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

2ª edição

CNT / SEST SENAT / ITL
Sistema Transporte

LGPD
TRANSPARÊNCIA E SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

Expediente

CNT – SEST SENAT – ITL
Presidente do Sistema Transporte
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: Luiz Gustavo Bueno Machado

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

Transporte Aéreo de Cargas e de Passageiros
Vice-Presidente da CNT: Eduardo Sanovicz
Presidente da Seção: Jurema Camargo Monteiro

Infraestrutura de Transporte e Logística
Vice-Presidente da CNT: Paulo Gaba Junior
Presidente da Seção: Murillo de 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
Dawidson Gomes Carneiro
Michelle Guimarães Carvalho Guedes

Transporte Rodoviário de Cargas
Ana Carolina Ferreira Jarrouge
Narciso Figueirôa Junior

Transporte Aquaviário de Cargas e Passageiros
Fernanda Mendes Azevedo
Thatiana Barros Percincula

Transporte Ferroviário de Cargas e de Passageiros
Fernanda Adjuto
Heider Gomes
João Costa

Transporte Aéreo de Cargas e de Passageiros
António Augusto do Poço Pereira
Bruna Gianezini
Giovanna Pires
Rafael Pinho Esnarriaga
Rebecca Buono

Infraestrutura de Transporte e Logística
Aline Borges
Ricardo Santoro Nogueira

Coordenação e elaboração
Laura Schertel
Mônica Tiemy Fujimoto
Giovanna Milanese
Eduarda Costa Almeida

Comitê de Governança de Dados do Sistema Transporte
Gabriel Filipi Araujo de Azevedo
João Frederico Chagas Maranhão
João Guilherme Vogado Abrahao
Kerem Rayssa Gonçalves Fernandes
Luiz Carlos Castello Branco
Rubens Peres Nogueira
Thais de Abreu Guimarães

Atualizada até
Junho/2024

Guia de boas práticas de proteção de dados no setor de transporte. – 2ª ed. – Brasília: CNT : SEST SENAT : ITL, 2024.
136 p.

1. Lei geral de proteção de dados – legislação - Brasil. 2. Segurança da informação. 3. Tratamento de dados. 4. Setor de transporte. I. Confederação Nacional do Transporte. II. Serviço Social do Transporte III. Serviço Nacional de Aprendizagem do Transporte. IV. Instituto de Transporte e Logística.

CDU 342.721:656(036)

Sumário

Seção 1 - Parte Geral

Seção 2 - LGPD aplicada ao setor de Transportes

>> Capítulo 1

Seção 1 - Parte Geral

1. CONSIDERAÇÕES INICIAIS

O presente Guia de Boas Práticas tem por objetivo orientar as empresas do setor de transportes na aplicação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD). Já na sua segunda edição, o Guia de Boas Práticas é um reflexo do compromisso contínuo do setor na garantia da privacidade e proteção de dados pessoais dos indivíduos. Fruto de um trabalho conjunto de especialistas no tema, membros do Sistema CNT e representantes dos modais, as orientações contidas neste Guia de Boas Práticas aplicam-se às empresas de transporte rodoviário, aquaviário, ferroviário, aéreo e de infraestrutura e logística.

O tratamento de dados pessoais no setor de transporte alcança todos os modais. Por exemplo, no transporte rodoviário de passageiros, empresas coletam dados pessoais durante a compra de passagens e check-in, utilizando-os para gerenciar embarques, para monitorar viagens e para oferecer promoções personalizadas. Já no transporte rodoviário de cargas, os dados dos motoristas e de localização dos veículos são continuamente monitorados para otimização de rotas, segurança viária e segurança da carga. No transporte aquaviário, por sua vez, companhias de cruzeiro coletam dados sobre passageiros, incluindo informações médicas e preferências, para proporcionar um serviço personalizado e seguro na viagem. Em relação ao modal ferroviário, de passageiros e de cargas, o uso de sistemas de monitoramento e de rastreamento é essencial para garantir a pontualidade e segurança das operações. No transporte aéreo, dados são coletados desde a reserva do bilhete até o desembarque, com múltiplas etapas de verificação de identidade e segurança. Por fim, no modal de infraestrutura e logística, empresas gerenciam grandes volumes de dados para uma coordenação eficiente de múltiplos modais e armazenamento de mercadorias.

Dadas as especificidades do setor de transporte, a sua regulação e dinâmica própria, é fundamental estabelecer diretrizes adaptadas à realidade dos modais. Esse é justamente o objetivo deste Guia de Boas Práticas, que cumpre o artigo 50 da LGPD ao propor regras de governança e boas práticas setoriais, para facilitar a implementação da Lei no setor.

A atualização deste Guia, que já se encontra na sua segunda edição, é impulsionada por diversos fatores. Em primeiro lugar, destacam-se as constantes evoluções tecnológicas, que alteraram diversas práticas do setor de transportes, criando novos cenários em que há a necessidade de tratar dados pessoais, como sistemas de inteligência artificial (IA). Ademais, a atualização legislativa e regulatória, incluindo as diretrizes mais recentes da Autoridade Nacional de Proteção de Dados (ANPD), exige que o setor de transportes ajuste as suas práticas, a fim de garantir a plena conformidade com a LGPD. Por fim, é fundamental

Seção 1 - Parte Geral

incorporar as lições aprendidas nos últimos anos, por meio das melhores práticas identificadas no setor, criando assim um ecossistema mais seguro e eficiente.

A segunda edição do Guia de Boas Práticas encontra-se organizada em duas seções. A primeira explora os principais conceitos da LGPD aplicáveis ao setor de transportes, os princípios, as bases legais, os agentes de tratamento, o encarregado, a ANPD e as sanções administrativas. A segunda, por sua vez, apresenta diretrizes concretas e específicas para o setor, como as principais atividades de tratamento, usos comuns de novas tecnologias que utilizam dados pessoais pelas empresas do setor, bem como boas práticas de accountability, de garantia dos direitos dos titulares, de segurança da informação, entre outros. Ao longo de todo o Guia de Boas Práticas, é possível encontrar casos concretos aplicados à realidade dos modais, checklists, quadros explicativos, fluxogramas e muito mais.

>> A LGPD para além do custo de compliance

Em um mundo cada vez mais digital, a proteção de dados é mais do que uma exigência legal. É uma oportunidade para as empresas demonstrarem o seu compromisso com a ética e a proteção dos clientes, colaboradores e terceiros prestadores de serviço, construindo um futuro mais seguro e confiável para todos.

A proteção de dados não deve ser enxergada apenas como uma questão de conformidade, mas também como pilar fundamental para a construção da credibilidade da marca e o fortalecimento das relações com os clientes. Por meio de um programa robusto de privacidade, a empresa passa a compreender o fluxo dos dados pessoais, entender onde esses dados são utilizados, identificar os riscos associados ao seu tratamento, e conhecer as suas obrigações e responsabilidades perante os titulares de dados. Ainda, programas de conformidade permitem integrar privacidade, proteção de dados e segurança da informação, além de unificar e automatizar fluxos de trabalho.[1]

Uma pesquisa da CISCO de 2024 destaca que 94% dos consumidores dizem não comprar mais com empresas que não protegem adequadamente os seus dados. Além disso, 95% das empresas afirmam que os benefícios de investir em proteção de dados superam os custos e a organização acaba alcançando um retorno de 1,6 vezes sobre o investimento realizado em privacidade.[2]

Ao adotar práticas eficazes de privacidade e proteção de dados, as empresas não apenas cumprem regulamentações, mas constroem confiança e diferenciam-se no mercado. Portanto, investir em proteção de dados, promover uma cultura de privacidade e adotar uma abordagem transparente e proativa acabam se tornando essenciais para garantir a segurança das informações e o sucesso a longo prazo.

1 https://www.ibm.com/security/digital-assets/data-privacy-matters/
2 https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html

Seção 1 - Parte Geral

2. FUNDAMENTOS DA LGPD APLICADOS AO SETOR DE TRANSPORTES

Este capítulo tem como objetivo introduzir os conceitos e os fundamentos da LGPD, destacando a sua importância e suas implicações específicas para o setor de transportes. O entendimento dos princípios e requisitos básicos da LGPD é crucial para que as empresas de transporte implementem medidas eficazes para proteger os dados pessoais de clientes, colaboradores, motoristas, passageiros, tripulação, fornecedores, parceiros, prestadores de serviços, entre outros.

O setor de transportes trata diversos tipos de dados para diferentes finalidades, envolvendo desde o registro dos passageiros, de destinatários de pacotes, até dados de colaboradores e parceiros. Esses dados pessoais são amplamente utilizados, por exemplo, em sistemas inteligentes de bilhetagem e check-in em locais como aeroportos e estações, visando aumentar a eficiência no fluxo de pessoas. Além disso, os dados são empregados para aprimorar o planejamento urbano, desenvolver sistemas autônomos de tráfego, e até melhorar os serviços prestados através do compartilhamento de informações com empresas terceirizadas, como agências de publicidade, entre outras.

Por um lado, o uso dos dados permite que as empresas se tornem mais produtivas, eficientes. Por outro, proporcionam aos usuários do sistema de transporte uma experiência mais segura, econômica e personalizada. Como a transformação tecnológica intensificou o uso e o compartilhamento de dados pessoais entre as empresas, é essencial que todo o setor de transporte se alinhe às diretrizes da LGPD, garantindo a conformidade plena de todas as suas atividades.

A utilização de novas tecnologias é fundamental para maior eficiência na prestação dos serviços de transporte, proporcionando mais agilidade, segurança e personalização no atendimento aos clientes. Por exemplo, sistemas de rastreamento em tempo real permitem que empresas de transporte monitorem suas frotas e cargas, otimizando rotas e reduzindo custos operacionais e garantindo segurança na condução dos veículos. Tecnologias, como inteligência artificial e big data, são utilizadas para analisar grandes volumes de dados, identificando os padrões e previsões de demanda que melhoram a gestão e alocação de recursos. Para os passageiros, aplicativos de mobilidade e check-in online agilizam o embarque e o desembarque, além de oferecerem uma experiência mais fluida e conveniente. No contexto de segurança, dados pessoais são essenciais para a autenticação de passageiros e a prevenção de fraudes.

Seção 1 - Parte Geral

Contudo, esses avanços exigem o tratamento de dados pessoais, como informações de localização, preferências de viagem, dados de identificação, entre outros, para funcionar de maneira eficaz. Assim, é crucial que as empresas implementem medidas de segurança e de conformidade com a LGPD para proteger a privacidade e os dados de clientes enquanto aproveitam os benefícios dessas inovações tecnológicas.

Para compreender melhor os impactos da LGPD nos diferentes processos e fluxos das empresas do setor de transporte, bem como os conceitos que serão abordados ao longo deste Guia de Boas Práticas, apresentamos alguns exemplos de fluxos de dados aplicados à realidade dos modais de transporte.

Seção I - Transporte Rodoviário de Passageiros

Uma pessoa residente em Belo Horizonte (Minas Gerais) precisa viajar de ônibus para Brasília (Distrito Federal) a trabalho. Ao acessar o site da empresa de transporte rodoviário para comprar a sua passagem, ela fornece uma série de dados pessoais, como o nome completo, a data de nascimento, o telefone, o e-mail, o CPF, endereço residencial e informações financeiras (como número do seu cartão de crédito). No dia da viagem, ao chegar à rodoviária, o passageiro utiliza o totem de autoatendimento para fazer o check-in, fornecendo novamente diversos dados pessoais, incluindo informações de terceiros, como um contato de emergência. Novos dados são processados se o passageiro decide despachar bagagens e também no momento do embarque no ônibus. Depois de chegar ao destino, os dados pessoais do passageiro continuam a ser utilizados para analisar hábitos de viagem e oferecer promoções personalizadas, além de solicitar feedback sobre a experiência. Se o passageiro se tornar um cliente frequente, ele receberá um cartão de fidelidade, o que exige o compartilhamento de dados com a gráfica responsável pela impressão e com a transportadora que entregará o cartão em sua residência.

Seção II - Transporte Rodoviário de Cargas

Uma empresa de São Paulo (SP) precisa enviar mercadorias para o Rio de Janeiro (RJ). Ao contratar a transportadora, a empresa fornece uma série de dados pessoais relacionados ao remetente e destinatário, como nome, endereço, telefone e e-mail. Além disso, são fornecidas informações sobre a carga, como o tipo, quantidade e valor das mercadorias. No dia do envio, a transportadora coleta dados do motorista e veículo que fará o transporte, incluindo nome, CPF, CNH e dados do veículo. Durante o trajeto, a transportadora utiliza os sistemas de rastreamento para monitorar a localização da carga em tempo real, coletando dados de localização (GPS). Ao chegar ao destino, dados são usados para confirmar a entrega e emitir recibos. Posteriormente, a transportadora pode utilizar esses dados para analisar rotas e otimizar futuras entregas.

>>

Seção 1 - Parte Geral

Uma pessoa perdeu objetos pessoais no sistema metroferroviário (metrô, trens, plataformas e estações). Para ser contatada, na hipótese de os objetos serem encontrados, ela fornece os seus dados pessoais (nome, telefone, endereço, e-mail). O fornecimento pode ser feito pessoalmente, através de formulário eletrônico ou durante contato telefônico. Os dados ficam armazenados em sistema pelo prazo necessário e são processados para a devolução do item. Os dados podem ser compartilhados com outras áreas da empresa, se necessária a apuração da localização do item.

Seção III - Transporte Aquaviário de Cargas e de Passageiros

Uma pessoa residente no Rio de Janeiro (RJ) decide fazer uma viagem de cruzeiro pelo litoral brasileiro. Para isso, ela acessa o site da companhia de cruzeiros para comprar o seu pacote de viagem, fornecendo vários dados pessoais, como nome completo, data de nascimento, telefone, e-mail, CPF, endereço residencial, CEP, e informações financeiras (como o número do cartão de crédito). Além disso, ela também pode vir a informar dados pessoais sensíveis, como alergias alimentares e condições médicas que requerem atenção especial. O site da companhia utiliza essas informações para processar o pagamento, verificar a identidade do passageiro e emitir a confirmação da reserva. No dia do embarque, ao chegar no porto, o passageiro realiza o check-in, fornecendo novamente dados pessoais, como número da reserva, CPF e informações de contato. A equipe de atendimento também coleta dados adicionais, como o nome e contato de emergência, e verifica seus documentos de identificação. Se o passageiro tiver bagagem, novos dados são processados para rastrear as bagagens até a sua cabine. No cruzeiro, são coletados dados pessoais do passageiro para diversos fins, como garantir a segurança a bordo, oferecer serviços personalizados (baseados em preferências alimentares e médicas) e facilitar transações financeiras a bordo (compras em lojas e pagamentos de serviços extras). A companhia também pode utilizar dados de localização por meio de pulseiras eletrônicas ou cartões de acesso para monitorar o fluxo de passageiros em áreas comuns e garantir a segurança. Após o término do cruzeiro, os dados continuam a ser utilizados pela companhia para analisar hábitos de viagem e oferecer promoções personalizadas para futuras viagens. Além disso, ela pode solicitar feedback sobre a experiência a bordo para melhorar os seus serviços. Se o passageiro se tornar um cliente frequente, ele pode ser convidado a participar de um programa de fidelidade.

Seção IV - Transporte Ferroviário de Cargas e de Passageiros

Uma pessoa precisa enviar uma carga de Guarujá (São Paulo) para Porto Alegre (Rio Grande do Sul) através de transporte ferroviário. Ao acessar o site da empresa para agendar o envio, ela fornece dados pessoais, como o nome completo, o telefone, o e-mail, CPF e endereço. Além disso, são fornecidas informações sobre as cargas, como o tipo, a quantidade e o valor das mercadorias. No dia do envio, ao chegar à estação ferroviária, o remetente entrega sua carga e fornece mais dados pessoais, se necessário, para seu despacho. Durante o transporte, a empresa utiliza sistemas de rastreamento para monitorar a localização da carga em tempo real. Ao chegar ao destino, os dados do destinatário são utilizados para confirmar a entrega e emitir recibos.

Seção 1 - Parte Geral

Seção V - Transporte Aéreo de Cargas e de Passageiros

Um morador de Curitiba (Paraná) precisa viajar a lazer para Salvador (Bahia). Ao acessar o site da companhia aérea para comprar sua passagem, ele fornece uma série de dados pessoais, como nome completo, data de nascimento, telefone, e-mail, CPF, endereço residencial, CEP, informações financeiras (como número do cartão de crédito) e, em alguns casos, até dados pessoais sensíveis, como condições de saúde que necessitam de atenção especial durante o voo. O site utiliza as informações para verificar a identidade do passageiro, processar o pagamento e emitir o bilhete eletrônico. Os dados financeiros são criptografados para garantir sua segurança durante a transação. No dia da viagem, ao chegar ao aeroporto, o passageiro consegue optar por usar o totem de autoatendimento ou fazer o check-in pelo aplicativo da companhia aérea. Nesse momento, ele fornece novamente alguns dados pessoais, como número do bilhete, informações de contato e CPF. Se houver bagagens para despachar, novos dados são tratados para identificar e rastrear as bagagens até o destino final. No embarque, os dados do passageiro são verificados novamente. A tripulação pode ter acesso a informações específicas, como preferências de assento e necessidades especiais, como restrições alimentares, para proporcionar a melhor experiência possível durante o voo. Após a chegada ao destino, os dados pessoais do passageiro continuam a ser utilizados pela companhia aérea para analisar seus hábitos de viagem e oferecer promoções personalizadas, além de solicitar feedback sobre a experiência. Se o passageiro vier a se tornar um cliente frequente, ele pode ser convidado a participar do programa de fidelidade, exigindo então o compartilhamento de dados pessoais com a gráfica responsável pela impressão dos cartões de fidelidade e com a transportadora que entregará o cartão em sua residência.

Seção VI - Infraestrutura de Transporte e Logística

Uma determinada empresa de logística foi contratada para gerenciar o transporte de mercadorias de um armazém em Santos (São Paulo) para uma fábrica em Curitiba (Paraná). A empresa de logística coleta dados pessoais dos remetentes e dos destinatários, como o nome, endereço, telefone e e-mail. Além disso, são coletadas informações sobre os motoristas e veículos que farão o transporte, incluindo nome, CPF, CNH e dados dos veículos. Durante o transporte, a empresa de logística utiliza sistemas de rastreamento para monitorar a localização dos veículos em tempo real. Ao chegar ao destino, os dados são utilizados para confirmar a entrega e emitir recibos. Posteriormente, a empresa de logística pode utilizar esses dados para analisar rotas e otimizar futuras operações.

Os exemplos apresentados acima mostram que o ciclo de vida do tratamento de dados no setor de transporte apresenta peculiaridades em cada modal, existindo riscos específicos para cada uma das operações.

Assim, garantir a conformidade com a LGPD deve ser acompanhada pelas empresas. Por isso, este Guia de Boas Práticas discutirá hipóteses comuns de tratamento dos dados pessoais no setor de transporte, apresentando as melhores práticas adotadas no mercado, a fim de ajudar as empresas na implementação facilitada e eficiente das regras da LGPD.

>> Capítulo 2

Seção 1 - Parte Geral

2.1 Conceitos

Compreender os conceitos da LGPD é essencial para a correta aplicação das práticas de proteção de dados pessoais. Este Guia visa esclarecer tais conceitos e oferecer uma base sólida para que as empresas do setor possam, aos poucos, familiarizar-se com eles.

O conceito central da LGPD é o de dados pessoais. Estes são conceituados em duas categorias: dados pessoais (art. 5º, I) e dados pessoais sensíveis (art. 5º, II). A distinção entre ambas se justifica pelo maior potencial discriminatório do tratamento de dados pessoais sensíveis, pois, caso eles sejam mal utilizados, podem causar discriminações e/ou danos significativos à pessoa.

O que é um dado pessoal?

O **dado pessoal** (art. 5º, I) é qualquer informação que identifique ou então possa identificar um indivíduo, independentemente de sua natureza ou atributos. Os elementos que constituem o conceito são:

- Informação de qualquer natureza: informação de qualquer tipo ou forma, seja texto, imagem, coordenadas geográficas, sinais, sons.
- Relacionada a uma pessoa natural: referentes a um indivíduo (o titular dos dados).
- Capacidade de identificação: que identifica ou têm o potencial de identificar o titular.

Exemplos: nome completo, endereço, telefone, CPF, data de nascimento, e-mail, comprovante de renda, currículos, dados bancários, entre outros.

Exemplos de dados pessoais utilizados no setor de transportes

Transporte Rodoviário de Passageiros: Nome completo e CPF dos passageiros são coletados na compra de passagens e no check-in para identificar e autenticar o passageiro. O telefone e e-mail são coletados para o envio de confirmações de viagem, notificações de mudanças no itinerário e ofertas promocionais. O endereço residencial é necessário para o envio de cartões de fidelidade e reembolsos de passagens, assim como os dados de localização (GPS) podem ser utilizados para monitorar a localização do ônibus e informar aos passageiros sobre a previsão de chegada.

Transporte Urbano de Passageiros: nome, identidade, data de nascimento, endereço, telefone, e-mail, histórico de viagens, saldo, recargas e, em alguns casos, fotografia e dados para benefícios sociais são dados normalmente coletados para a emissão de cartões de bilhete eletrônico para transporte público. Esses dados são usados para identificar e personalizar o serviço, processar pagamentos, comunicar atualizações.

Transporte Rodoviário de Cargas: Nome e CPF dos motoristas são coletados para verificar a sua identidade e habilitação. Já os dados do veículo são utilizados para registro e monitoramento no transporte.

>>

Seção 1 - Parte Geral

Informações de contato do remetente e destinatário são necessárias para coordenação da entrega e a comunicação sobre o status da carga, assim como dados de localização podem ser utilizados para monitorar a carga em tempo real e garantir a segurança e a eficiência da entrega.

Transporte Aquaviário de Passageiros: Nome completo e data de nascimento são utilizados na emissão de bilhetes e identificação dos passageiros a bordo. Informações médicas são coletadas a fim de atender as necessidades de saúde dos passageiros durante o cruzeiro, assim como as suas preferências alimentares, utilizadas para personalizar as refeições servidas a bordo. Já os dados de pagamento costumam ser utilizados para compra do pacote de viagem e despesas adicionais durante o cruzeiro.

Transporte Ferroviário de Cargas: Dados do remetente e do destinatário da carga são coletados para a coordenação e a confirmação da entrega de mercadorias. Por vezes, também são coletados dados de rastreamento para monitoramento da localização do trem e das mercadorias ao longo do trajeto. É possível que sejam coletadas as informações de contato para emergências, utilizadas para a comunicação rápida em caso de problemas durante o transporte.

Transporte Aéreo de Passageiros: O nome completo e documentos de identificação (como RG, CPF, Passaporte) são necessários para compra de passagens, check-in e controle de segurança no embarque. Informações de contato (telefone e e-mail) são utilizadas para o envio de informações sobre voos, alterações de itinerário e promoções. Ainda, dados de pagamento são coletados para processamento da compra de bilhetes e serviços adicionais. Quando necessário, as informações sobre necessidades especiais podem ser usadas para garantir assistência adequada no voo.

Infraestrutura de Transporte e Logística: Dados de identificação (como o nome completo e CPF) dos motoristas e colaboradores são coletados para a gestão e segurança das operações logísticas. É possível que sejam coletadas informações sobre veículos e dados de localização, utilizados para o monitoramento da frota, a otimização de rotas e garantia da segurança das mercadorias. Ainda, são coletadas informações de contato dos clientes para comunicação sobre o status das entregas e coordenação de serviços logísticos.

Atenção!

Informações que não se referem a uma pessoa identificada ou identificável não são considerados dados pessoais e, portanto, não estão sujeitos às regras da LGPD. Da mesma forma, dados anonimizados (art. 5º, III), isto é, que passaram por algum processo de anonimização, através do qual, mediante o uso de meios técnicos razoáveis e disponíveis no momento do tratamento, perdem a possibilidade de associação ao titular, também não são considerados dados pessoais.

Os dados pseudonimizados (art. 13, §4º), por sua vez, podem ser reconduzidos aos titulares através de uma chave de identificação armazenada separadamente. Por isso, eles são considerados dados pessoais e estão sujeitos à LGPD. Apesar de métodos de pseudonimização oferecerem grau adicional de segurança, como criptografia, isso não afasta a aplicação das regras da LGPD.

Seção 1 - Parte Geral

O que é um dado pessoal sensível?

O **dado pessoal sensível** (art. 5º, II) é qualquer informação sobre a origem racial ou étnica, a convicção religiosa, a 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.
Exemplos: biometria facial, registros médicos, registros em sindicatos, filiação partidária e entidades de classe etc.

Exemplos de dados pessoais sensíveis utilizados no setor de transportes

Transporte Rodoviário de Passageiros: Informações sobre condições de saúde, como mobilidade reduzida ou uso de cadeira de rodas, podem ser coletadas para garantir acomodações adequadas, assistência durante as viagens e emissão de cartões gratuidades. Ainda, podem ser coletados dados sobre alergias alimentares a fim de fornecer opções de refeição seguras durante viagens mais longas, bem como informações médicas de emergência, armazenadas para casos de necessidade de atendimento médico.

Transporte Rodoviário de Cargas: São coletados dados biométricos dos motoristas (a impressão digital e/ou o reconhecimento facial) para controle de acesso aos veículos e/ou acesso aos locais de carregamento e descarregamento e para autenticação de motoristas. Além disso, são coletadas informações sobre condições de saúde dos motoristas que possam afetar a sua capacidade de dirigir, como uso de entorpecentes, álcool, drogas e substâncias psicoativas, distúrbios do sono e/ou doenças crônicas.

Transporte Aquaviário de Passageiros: São coletados dados de saúde sobre condições médicas específicas, como diabetes ou necessidades de medicação, a fim de garantir assistência médica a bordo. É possível que sejam coletados dados de preferências religiosas para oferecer opções de refeições que atendam a restrições religiosas, assim como informações sobre alergias a alimentos ou medicamentos, para evitar reações adversas durante a viagem.

Transporte Ferroviário de Cargas: Comumente, é coletada a biometria (reconhecimento facial ou impressões digitais) para controlar o acesso a áreas restritas nas estações e nos trens. Além disso, são coletadas informações sobre condições médicas dos colaboradores que são responsáveis pelo transporte de cargas perigosas, garantindo que eles estejam aptos para o exercício dessa função.

Transporte Aéreo de Passageiros: Normalmente, são coletadas informações sobre saúde, como necessidades especiais de oxigênio suplementar ou assistência médica, para garantir a segurança e conforto dos passageiros durante o voo. É possível também a coleta de dados biométricos, por meio da utilização de reconhecimento facial, para agilizar o embarque e garantir a segurança dos passageiros. Caso necessário, são coletadas informações sobre preferências alimentares, devido a condições de saúde e/ou crenças religiosas.

Infraestrutura de Transporte e Logística: É comum a coleta de biometria para controle de acesso às instalações de armazenamento e de centros de distribuição. Informações de saúde ocupacional são coletadas para garantir a conformidade com as normas de segurança e de saúde ocupacional e implementar programas de prevenção de doenças ocupacionais para os trabalhadores expostos a riscos específicos

Seção 1 - Parte Geral

Quem é o titular dos dados?

O titular (art. 5º, V) é a pessoa natural (física) a quem se referem os dados pessoais que são objeto de um determinado tratamento. Abaixo, indicamos alguns exemplos de titulares que interagem com as empresas do setor de transportes.

- **Transporte Rodoviário de Passageiros:** passageiros e motoristas.
- **Transporte Rodoviário de Cargas:** motoristas, cliente remetente e o destinatário da carga.
- **Transporte Aquaviário de Passageiros:** passageiros de cruzeiros e membros da tripulação.
- **Transporte Ferroviário de Cargas:** empresário (empresário individual e/ou representante legal) que envia mercadorias e operadores dos trens.
- **Transporte Metroferroviário de Passageiros:** passageiros do sistema metroferroviário e colaboradores
- **Transporte Aéreo de Passageiros:** passageiros e tripulação (pilotos e comissários de bordo).
- **Infraestrutura de Transporte e Logística:** operadores e clientes de serviços logísticos.

Seção 1 - Parte Geral

2.2 Princípios

Os princípios previstos na LGPD (art. 6°) podem ser utilizados como parâmetro norteador ao longo de todo o tratamento de dados pessoais realizado. Eles se encontram listados na tabela abaixo, que explica o significado de cada princípio e o que as empresas devem fazer para garantir o seu cumprimento.

Boa-fé objetiva (art. 6°, caput)	O tratamento deve ser pautado nos ditames éticos e morais.
Finalidade (art. 6°, I)	O tratamento deve ter propósitos legítimos, específicos, explícitos e informados ao titular em toda a sua duração. Caso a finalidade se altere ao longo do processo, a nova finalidade deve ser compatível com as finalidades originais.
Adequação (art. 6°, II)	O tratamento deve ser compatível com as finalidades informadas ao titular.
Necessidade (art. 6°, III)	O tratamento deve ser limitado ao mínimo necessário para a realização das finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação a tais finalidades.
Livre Acesso (art. 6°, IV)	Os titulares dos dados devem poder consultar a forma e a duração do tratamento, e sobre a integralidade dos dados de forma gratuita.
Qualidade dos dados (art. 6°, V)	Os dados devem ser exatos, claros, relevantes e atualizados.
Transparência (art. 6°, VI)	As empresas devem disponibilizar informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do tratamento e os agentes, observados os segredos comercial e industrial.
Segurança (art. 6°, VII)	Os dados devem ser protegidos de acessos não autorizados e de situações acidentais e/ou ilícitas de destruição, de perda, alteração, comunicação ou difusão, com medidas técnicas e administrativas.

Seção 1 - Parte Geral

Prevenção (art. 6º, VIII)	É necessário prevenir a ocorrência de eventuais danos decorrentes do tratamento de dados pessoais.
Não discriminação (art. 6º, IX)	O tratamento não deverá ser realizado para fins discriminatórios, ilícitos ou abusivos.
Responsabilização e prestação de contas (art. 6º, X)	O agente deve adotar medidas eficazes e ser capaz de comprovar a observância e o cumprimento das normas de proteção de dados.

Para garantir a conformidade do tratamento de dados com a LGPD, é fundamental avaliar a aderência aos princípios acima. Na ausência de uma regra específica na LGPD, é indispensável que os princípios sejam usados como norte, orientando as decisões e ações das entidades. Abaixo, apresentamos um exemplo que ilustra a aplicação dos princípios na avaliação da legitimidade de uma atividade de tratamento de dados pessoais do setor.

Monitoramento de fadiga dos motoristas

Uma empresa de transporte intermunicipal implementou um sistema de monitoramento de fadiga para seus motoristas, utilizando as câmeras de vigilância e os sensores instalados nos veículos para detectar sinais de cansaço e sonolência durante a condução. As informações registradas incluem dados visuais dos motoristas, como piscadas frequentes e bocejos, e os dados comportamentais, como desvios de direção e velocidade irregular. Estes dados são integrados a um sistema central que emite alertas em tempo real e gera relatórios periódicos para o gestor de frotas. O objetivo declarado da coleta e tratamento de dados, conforme a legislação e comunicado aos motoristas, é garantir a segurança no trânsito, prevenindo acidentes causados por fadiga.

Os motoristas autenticam seu cartão de identificação ao iniciar o turno, e as câmeras e sensores começam a registrar os dados quando o veículo é ligado. Se o sistema detectar sinais de fadiga, um alerta sonoro é emitido no interior do veículo para avisar o motorista, recomendando uma pausa. Relatórios periódicos são gerados e enviados ao gestor de frotas, que analisa as condições de fadiga dos motoristas e toma medidas preventivas, como ajustes nos horários de trabalho ou pausas obrigatórias. Os dados são armazenados de forma segura, com acesso restrito a gestores autorizados, e são mantidos por um período definido, conforme a política de retenção de dados da empresa, sendo excluídos após esse período, exceto quando necessário para as investigações de incidentes específicos ou o cumprimento de obrigações legais. Ao avaliar a aplicação dos princípios da LGPD neste cenário, nota-se que alguns aspectos estão em conformidade, enquanto outros podem precisar de certos ajustes.

>>

Seção 1 - Parte Geral

Nesse contexto, o princípio da finalidade será cumprido, pois os dados são tratados para uma finalidade legítima e específica de monitorar a fadiga dos motoristas e de garantir a segurança no trânsito. Isso é assegurado desde que os motoristas sejam plenamente informados sobre as finalidades do tratamento, evitando qualquer uso não autorizado dos dados. O princípio da adequação também será respeitado, pois os dados são adequados para identificar os sinais de fadiga, alinhados ao objetivo de segurança. No entanto, a empresa deve garantir que apenas os dados estritamente necessários sejam coletados, respeitando o princípio da necessidade. Para isso, deve revisar regularmente os dados coletados para evitar qualquer excesso de informações.

Quanto ao princípio da transparência, embora a empresa informe os motoristas sobre a coleta e o uso dos dados, é essencial fornecer informações detalhadas, claras e acessíveis sobre todas as finalidades do tratamento, incluindo os possíveis usos secundários. A empresa deve garantir que os motoristas compreendam como seus dados serão utilizados. No que diz respeito ao princípio da segurança, a empresa implementa medidas como a criptografia e controle de acesso para proteger os dados dos motoristas. Contudo, é importante realizar auditorias regulares e testes de segurança para assegurar a eficácia das medidas e prevenir possíveis falhas.

O princípio da não discriminação também parece estar sendo respeitado, visto que os dados são utilizados exclusivamente para garantir a segurança e não para discriminar os motoristas. No entanto, a empresa deve monitorar continuamente suas práticas para garantir que nenhum viés ou discriminação inadvertida ocorra. Por fim, a empresa deve demonstrar a adoção de medidas eficazes para o cumprimento das normas de proteção de dados, o que inclui manter registros do tratamento de dados e adotar práticas de conformidade à LGPD, como a realização de avaliações de impacto à proteção de dados (RIPD), em observância ao princípio da prestação de contas.

Passe eletrônico no transporte público urbano

Um morador de São Paulo utiliza o transporte público todos os dias para ir ao trabalho. Ao adquirir seu passe eletrônico, ele fornece seus dados pessoais à empresa de transporte público urbano. A empresa coleta essas informações com a finalidade específica de emitir o cartão do bilhete eletrônico e gerenciar o bilhete do morador, garantindo que apenas os dados necessários sejam solicitados e utilizados. Por isso, a empresa solicita dados cadastrais, como nome, endereço, data de nascimento, e-mail, CPF e uma foto para a emissão do cartão. A foto não é utilizada para outros registros ou bases de dados, como a coleta de dados biométricos a partir da foto.

O morador tem acesso fácil a suas informações pessoais através do site da empresa, onde pode atualizar seus dados e consultar seu histórico de uso do transporte público. A empresa adota medidas rigorosas para proteger os dados dele, incluindo criptografia e políticas de acesso restrito. Em caso de qualquer incidente de segurança, o morador é prontamente notificado, e a empresa toma as medidas necessárias para mitigar quaisquer danos.

Quanto ao princípio da transparência, embora a empresa informe os motoristas sobre a coleta e o uso dos dados, é essencial fornecer informações detalhadas, claras e acessíveis sobre todas as finalidades do tratamento, incluindo os possíveis usos secundários. A empresa deve garantir que os motoristas compreendam como seus dados serão.

Seção 1 - Parte Geral

Questionário para avaliação da conformidade com os princípios da LGPD

- Todos os dados pessoais que estão sendo coletados são realmente necessários à atividade?
- Posso violar algum direito do titular com a minha atividade de tratamento de dados?
- O titular foi informado sobre os usos que eu vou fazer com os seus dados pessoais?
- Tenho condições de viabilizar o acesso do titular às informações sobre os seus dados?
- Onde e como eu vou guardar os dados pessoais? Só pessoas autorizadas terão acesso a eles?
- Os dados pessoais que estão sendo tratados estão seguros e protegidos contra ameaças?
- A finalidade estabelecida no início do tratamento foi finalizada? Ainda preciso dos dados?
- Precisei alterar a finalidade inicial em algum momento durante o tratamento?

2.3 Bases Legais

A LGPD reconhece a relevância jurídica dos dados pessoais e, por isso, estabelece as condições específicas para o seu tratamento, que são denominadas hipóteses autorizativas ou bases legais. As bases legais para tratamento de dados pessoais em geral encontram-se no artigo 7° da LGPD, enquanto as bases legais para o tratamento de dados sensíveis estão no artigo 11 da Lei. A LGPD não faz distinção hierárquica entre elas, assim, a confirmação da legitimidade de um tratamento deve ser feita a partir da existência de uma base legal adequada, garantindo ainda que o tratamento respeite os princípios e direitos do titular.

Isso é relevante porque, conforme será melhor explicado posteriormente, durante a etapa de mapeamento e no registro das atividades de tratamento de dados, o controlador deve indicar qual base legal possibilita cada uma das atividades, a fim de assegurar que nenhum tratamento ocorra sem a devida autorização da LGPD.

Um ponto importante a se destacar é a inexistência de hierarquia entre as bases legais dispostas na LGPD. Isto significa dizer que nenhuma delas é mais importante do que a outra e nenhuma se sobrepõe àquela escolhida, sendo igualmente importantes em peso e cabimento. A base legal pode ser a mais adequada ao tratamento, mas nunca a mais

Seção 1 - Parte Geral

importante dentre as hipóteses legais autorizativas, conforme Enunciado nº 689 aprovado na IX Jornada Direito Civil do Conselho da Justiça Federal ("Não há hierarquia entre as bases legais estabelecidas nos arts. 7º e 11 da LGPD").

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 PRE-LIMINARES RELACIONADOS A CONTRATO	Sim	Não
EXERCÍCIO REGULAR DE DIREIT-OS 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 ADMINIS-TRAÇÃO PÚBLICA	Sim	Sim

Seção 1 - Parte Geral

GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR EM PROCESSOS DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE CADASTRO*	**Não***	**Não**
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.

No setor de transporte, destacam-se principalmente as bases legais de **execução de contrato** (amplamente utilizada em razão da própria natureza dos serviços de transporte), de **cumprimento de obrigação legal e/ou regulatória** (aplicada devido à extensa legislação setorial vigente, como normas de agências reguladoras dos modais de transporte: ANAC, ANTT e ANTAQ e a extensa legislação trabalhista e de segurança do trabalho aplicável especialmente ao motorista profissional) e de **prevenção à fraude** (muito utilizada para fins de segurança).

Obrigação legal ou regulatória, prevenção à fraude e exercício de direitos em processos judiciais, administrativos e arbitrais

Caso as empresas necessitem compartilhar dados pessoais para cumprimento de obrigação legal ou regulatória, para prevenção à fraude ou para exercício regular de direitos em processo judicial, administrativo e/ou arbitral, é importante que elas:

- Garantam que as categorias e a quantidade de dados pessoais a serem compartilhados sejam aquelas necessárias para cumprir a finalidade, abstendo-se de compartilhar dados adicionais (para os quais não haveria base/fundamento legal na LGPD);
- Documentem o compartilhamento realizado para fins de auditoria (caso o compartilhamento ocorra para cumprimento de ordem judicial, armazenar a cópia da decisão e a comprovação do compartilhamento, por e-mail, pelo comprovante de protocolo e/ou outro documento);
- Manter registro do compartilhamento de dados pessoais que realizarem de forma contínua e permanente (por exemplo, com Receita Federal, ANTAQ, ANAC, ANTT e outras instituições públicas para cumprimento de obrigações legais e regulatórias);
- Quando utilizar a base legal de prevenção à fraude, analisar a proporcionalidade e finalidade do compartilhamento, de modo que ela seja compatível com a finalidade do tratamento; e
- Nos casos de requisições judiciais, verificar e confirmar a identidade da autoridade solicitante, fornecendo os dados pessoais tão somente se o requerimento for encaminhado por autoridade competente no formato legalmente exigido.

Seção 1 - Parte Geral

Ademais, abaixo detalhamos as outras bases legais amplamente utilizadas pelas empresas do setor de transportes e alguns exemplos para ilustrar os casos mais comuns de utilização.

Consentimento do titular dos dados (art. 7°, I, e art. 11, I)

É utilizada quando o titular dos dados autoriza, de forma livre e informada, o tratamento de seus dados pessoais. Para ser válido, o consentimento deve cumprir alguns requisitos: a manifestação deverá ser livre, informada e inequívoca, permitindo, ao titular, tomar uma decisão consciente sobre o uso de seus dados para determinada finalidade. Dessa forma, caso a finalidade mude ao longo do tratamento, o titular deve ser informado e ter a oportunidade de fornecer um novo consentimento.

Exemplo

Uma empresa de transportes deseja implementar um programa de fidelidade para os seus passageiros, oferecendo descontos e benefícios. Para isso, a empresa coleta dados pessoais como nome, endereço de e-mail e histórico de viagens. A empresa optou por, antes de iniciar este tratamento, obter o consentimento dos passageiros, explicando a eles como os dados pessoais serão usados e os benefícios que eles receberão.

Os desafios do consentimento (art. 8°) [3]

Coletar o consentimento do titular é um processo complexo e cabe ao controlador garantir e comprovar que ele foi obtido de forma adequada, em conformidade com a LGPD (art. 8°, § 2°). Por isso, quando for escolhido como base legal para justificar determinado tratamento, alguns cuidados devem ser tomados. Para ser considerado válido no âmbito da LGPD, o consentimento deve ser concedido por meio de uma manifestação livre, informada, inequívoca, e para uma finalidade específica. Isso significa que o consentimento deve ser livre, ou seja, não condicionado. Além disso, o titular deve receber informações sobre o tratamento e consentir por meio de um ato positivo, não sendo possível se falar em consentimento tácito. Ainda, o consentimento deve ser dado para finalidades específicas, não sendo permitidas autorizações amplas ou genéricas (art. 8°, § 4°).

Os agentes devem estar atentos a algumas questões para coletar o consentimento dos titulares:

- Quando oferecido por escrito, o consentimento deve constar em cláusula contratual separada e em destaque das demais (art. 8°, § 1°, da LGPD)
- Permitir que o titular revogue o consentimento a qualquer momento (art. 8°, § 5°, da LGPD)
- Para compartilhar dados pessoais com outros controladores, deve ser obtido o consentimento específico para essa finalidade, ressalvadas as hipóteses de dispensa do consentimento (art. 7°, § 5°, da LGPD).
- Assegurar que o titular tenha acesso à cópia completa de seus dados pessoais em um formato que permita sua utilização subsequente, respeitando os segredos comerciais e industriais (art. 19, § 3°, da LGPD).

3 https://static.portaldaindustria.com.br/media/filer_public/6c/a0/6ca07577-fbc6-4e9a-81cf-700e0570849b/id_1633_guia_de_boas_praticas_de_protecao_de_dados_para_a_industria_web.pdf

Seção 1 - Parte Geral

Cumprimento de obrigação legal ou regulatória (art. 7°, II, e art. 11, II, a)

Leis e regulamentos podem exigir a coleta e tratamento de dados pessoais, como a obrigação de armazenar documentos tributários (notas fiscais) por um período específico, ou a manutenção de dados de motoristas para o Código Identificador da Operação de Transporte (CIOT) e de exames toxicológicos periódicos.

Exemplo

Uma transportadora de cargas é obrigada a manter registros detalhados das viagens dos seus motoristas, incluindo registros de cumprimento do Código Identificador da Operação de Transporte (CIOT). Esses registros são exigidos pela legislação vigente e pelas normas estabelecidas pela Agência Nacional de Transportes Terrestres (ANTT), como as Resoluções ANTT n° 4.799/2015, n° 5.867/2020 e n° 5.833/2020.

Execução de contrato (art. 7°, V)

É utilizada quando o tratamento é necessário para cumprir um contrato do qual o titular é parte, a pedido dele. O tratamento deve ser limitado aos dados necessários à execução do contrato.

Exemplo

Uma empresa de logística celebra dois contratos com um cliente para o transporte de mercadorias. Para cumprir esses contratos, a empresa precisa coletar e tratar os dados pessoais dos motoristas, como o nome, número da carteira de motorista e informações de contato. Esses dados são essenciais para a execução do contrato, permitindo que a empresa organize e monitore as entregas.

Exercício regular de direitos em processos judiciais, administrativos ou arbitrais (art. 7°, VI, e art. 11, II, d)

Dados pessoais podem ser necessários em processos judiciais, administrativos e/ou arbitrais. Isso é muito comum em casos de produção de provas. Esta base legal assegura o uso de dados para o exercício de direitos dentro desses processos.

Exemplo

Um motorista de ônibus se envolve em um acidente de trânsito durante o trabalho. A empresa de transporte utiliza os dados pessoais do motorista, incluindo registros de condução e dados do bafômetro, como parte da defesa em um processo judicial para demonstrar que o motorista estava em conformidade com as políticas de segurança da empresa no momento do acidente.

Seção 1 - Parte Geral

Legítimo interesse do controlador e/ou de terceiros (art. 7°, IX)

É aplicada em situações nas quais o tratamento de dados é necessário para os interesses legítimos do controlador e/ou de terceiros, desde que esses interesses não prevaleçam sobre os direitos e as liberdades fundamentais dos titulares. Seguindo recomendações da ANPD, é importante que o tratamento de dados com respaldo no legítimo interesse seja precedido de um teste de balanceamento que considere, de um lado, os interesses do controlador ou de terceiro e, de outro, os direitos e liberdades fundamentais dos titulares. Cada caso precisa ser cuidadosamente analisado e documentado. Se o tratamento envolver alto risco, deve ser elaborado Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que pode incluir o teste de balanceamento, e conter uma análise detalhada dos riscos e das medidas de mitigação adotadas no caso. A ANPD publicou um Guia Orientativo específico para esta hipótese legal, indicando que as empresas devem conduzir processos de avaliação de necessidade e proporcionalidade do tratamento, comunicar claramente os titulares sobre o tratamento realizado com base no legítimo interesse e os motivos para isso, além de elaborar o teste de balanceamento para identificar e mitigar os riscos associados ao tratamento. [4]

Exemplo

Uma empresa de transporte utiliza câmeras de segurança (CCTV) em seus veículos para garantir a segurança dos passageiros e motoristas. As imagens são utilizadas para monitorar incidentes e proteger passageiros e colaboradores. A empresa decide realizar um teste de balanceamento para assegurar que o interesse de garantir a segurança não se sobrepõe aos direitos dos indivíduos filmados.

Proteção ao crédito (art. 7°, X)

É utilizada quando os dados pessoais são tratados para verificar a capacidade de pagamento do titular, especificamente em contextos de proteção ao crédito.

Exemplo

Uma locadora de veículos consulta dados de crédito dos clientes para verificar a sua capacidade de pagamento antes de aprovar a locação de um carro. Este procedimento é usado para minimizar os riscos financeiros e garantir que o cliente tenha condições de cumprir as obrigações financeiras do aluguel do veículo.

Garantia de prevenção à fraude (art. 11, II, g)

Costuma ser aplicada ao tratamento de dados pessoais sensíveis com o objetivo de segurança em processos de identificação e autenticação em sistemas eletrônicos, como o uso de dados biométricos para evitar fraudes.

Exemplo

Uma empresa de transporte de valores utiliza dados biométricos (impressões digitais) para autenticar os motoristas que transportam grandes quantidades de dinheiro. Esta medida é adotada para prevenir eventuais fraudes e garantir que apenas indivíduos autorizados possam acessar e transportar os valores.

4 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

Seção 1 - Parte Geral

A escolha da base legal mais adequada é crucial para cada atividade de tratamento de dados, garantindo a conformidade com a LGPD e a proteção dos direitos dos titulares. Os princípios previstos pelo art. 6° devem ser rigorosamente observados, independentemente da base legal escolhida. Por fim, ao implementar medidas de segurança, como a criptografia, as empresas conseguem aumentar significativamente a proteção dos dados pessoais sob sua responsabilidade.

2.4 Agentes de Tratamento

Os agentes de tratamento de dados (art. 6°, IX), como estabelecido pela LGPD, podem ser dois: controlador (art. 6°, VI) ou operador (art. 6°, VII) de dados. A identificação desses agentes depende das atividades concretas que eles realizam em relação ao tratamento dos dados pessoais. A partir dessa identificação, que deverá ser contextual e factual, pode-se delimitar as responsabilidades dos agentes em determinada atividade de tratamento.

A classificação enquanto controlador ou operador comumente é feita por meio dos instrumentos contratuais, mas também é possível que o arranjo seja estipulado por meio de ou- tras formas de interação empresarial. Importante ressaltar que mesmo nos casos em que as obrigações são estipuladas em um instrumento legal, a identificação da posição do controlador deve considerar realidade prática, uma vez que, em eventual violação e/ou descumprimento da legislação, é o contexto fático que será avaliado pela ANPD.

Na realidade, o mais importante para determinar se uma entidade é controladora é o poder de decisão sobre o tratamento, que se caracteriza pelo controle sobre os elementos essenciais do tratamento, como a definição da finalidade, da natureza dos dados pessoais tratados e a duração do processo. O operador pode ter poder decisório, mas somente em relação a elementos não essenciais do tratamento, por exemplo, a escolha de softwares e equipamentos utilizados para o tratamento, bem como medidas de segurança e prevenção adotadas.

Quem é o controlador dos dados?

O **controlador** é o responsável por tomar as decisões sobre o tratamento. Ele define a finalidade e principais características do tratamento, fornecendo instruções ao operador quando necessário. Além disso, ele assume a responsabilidade principal pelo tratamento e é geralmente a entidade que tem interesse direto no tratamento dos dados. As seguintes atividades são responsabilidades do controlador dos dados, entre outras:

- Estabelecer a natureza dos dados pessoais a serem coletados;
- Definir a finalidade do tratamento de dados;
- Estabelecer as principais características do tratamento;
- Fornecer instruções ao operador;
- Garantir a conformidade da coleta dos dados antes de compartilhá-los com o operador;
- Adotar medidas de segurança apropriadas;
- Assegurar o exercício dos direitos dos titulares.

Exemplo Uma empresa de transporte marítimo que coleta os dados pessoais dos passageiros para emitir bilhetes, gerenciar embarques/desembarques, e realizar serviços a bordo é controladora dos dados.

As pessoas subordinadas a um controlador, como colaboradores, servidores públicos ou equipes de trabalho da empresa, não são considerados controladores ou operadores, pois atuam sob o poder diretivo dos agentes de tratamento. No contexto de uma pessoa jurídica, o agente de tratamento, para fins da LGPD, é apenas a organização. Além disso, o agente de tratamento poderá ser definido para cada atividade de tratamento, ou seja, a mesma empresa pode ser controladora e operadora e, portanto, possuir uma atuação híbrida em diferentes contextos.

Ainda, há a possibilidade de um tratamento ser conduzido em controladoria conjunta. No entendimento da ANPD [5] a controladoria conjunta ocorre quando há uma determinação conjunta (comum ou convergente) de dois ou mais controladores diretamente envolvidos sobre as finalidades e os elementos essenciais do tratamento, formalizada por meio de acordo entre as partes, estabelecendo as respectivas responsabilidades no cumprimento da LGPD.

Destaca-se que a identificação da controladoria conjunta é contextual e depende do caso concreto para determinar se foi estabelecida. Quando configurada, a responsabilidade dos controladores será solidária, nos termos do art. 42, §1º, II da LGPD, o que reforça a necessidade de todos os envolvidos estarem em conformidade com a LGPD.

5 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleit oral.pdf

Seção 1 - Parte Geral

Quem é o operador dos dados?

O **operador** realiza o tratamento de dados conforme as instruções do controlador. Ele age dentro dos limites definidos pelo controlador, tornando-se responsável nos casos de descumprimento dessas instruções ou da LGPD, pois acaba sendo equiparado ao controlador de dados.

Exemplo

Uma empresa de tecnologia que gerencia o sistema de reserva e check-in online para a empresa de transporte marítimo mencionada acima é operadora dos dados. Ela trata os dados seguindo as diretrizes da empresa de transporte (controladora dos dados).

Quem é o suboperador dos dados?

O **suboperador** é uma entidade contratada pelo operador para realizar parte das atividades de tratamento de dados. Ele atua sob a supervisão do operador e deve seguir as instruções tanto do operador quanto do controlador, mas normalmente seu vínculo direto é apenas com o operador.

Exemplo

Uma empresa de hospedagem de dados que armazena as informações coletadas pelo sistema de reserva e check-in online gerenciado por um operador, é um suboperador.

Cadeia de tratamento para melhorar a eficiência operacional e garantir segurança às entregas

Uma empresa de transporte rodoviário de cargas implementa um sistema integrado de gestão de frotas e de monitoramento de motoristas para melhorar a eficiência operacional e garantir a segurança das entregas. Para isso, faz uma parceria com empresa especializada em soluções de telemetria e monitoramento. Elas atuam enquanto controladores conjuntos, pois determinam conjuntamente as finalidades e meios do tratamento dos dados pessoais. Decidem que os dados coletados serão usados para monitorar a performance de motoristas, otimizar rotas de entrega e garantir a segurança dos veículos e cargas. Elas firmam um contrato que define suas respectivas responsabilidades e obrigações no tratamento dos dados.

Para operacionalizar o sistema de gestão de frotas, elas contratam uma operadora de dados, que é responsável por processar os dados de telemetria, que incluem informações sobre a velocidade dos veículos, as frenagens bruscas, tempos de parada e desvios de rota, conforme as instruções fornecidas por elas. A operadora deverá seguir estritamente as diretrizes estabelecidas, sem a liberdade de utilizar os dados para outras finalidades não autorizadas.

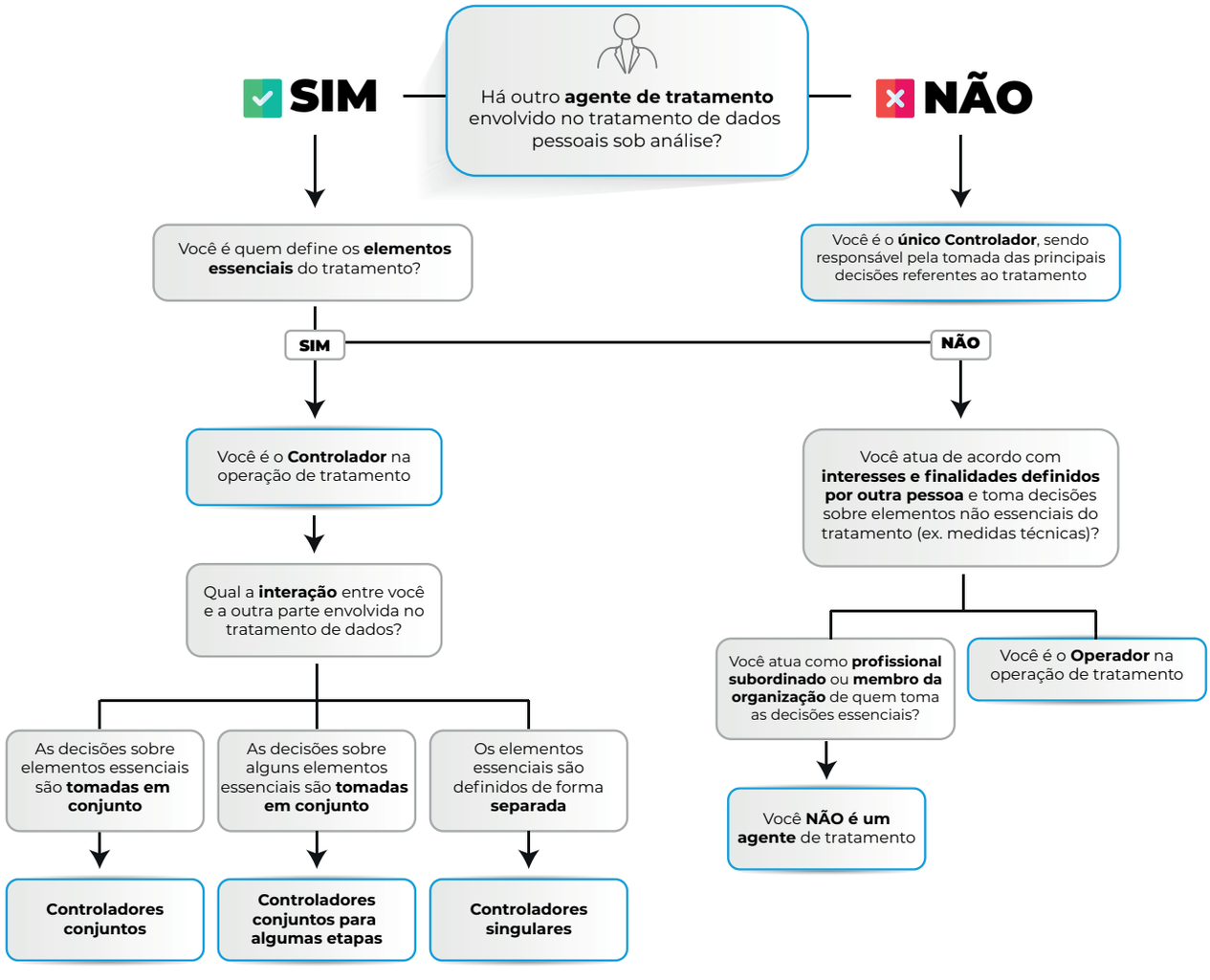
Para garantir a análise detalhada e segura dos dados coletados, a operadora contrata uma outra empresa especializada em serviços de armazenamento e processamento de dados em nuvem, a qual atua como suboperadora. A suboperadora armazena e processa os dados de telemetria sob as instruções da operadora, que, por sua vez, segue as instruções dos controladores conjuntos. A operadora obtém autorização formal dos controladores para subcontratar a suboperadora, a fim de garantir que todas as partes estejam cientes e de acordo com o arranjo de tratamento.

>>

Seção 1 - Parte Geral

Neste arranjo, os princípios da LGPD parecem ser cuidadosamente observados. A finalidade do tratamento é definida e comunicada aos motoristas: monitorar a performance, otimizar rotas e garantir a segurança das entregas. O tratamento ainda é adequado às finalidades estabelecidas, utilizando telemetria para monitorar a performance e segurança dos veículos. A coleta de dados é limitada ao mínimo necessário, evitando a coleta excessiva de informações. Os motoristas são informados de forma clara sobre a coleta e o uso de seus dados, incluindo os detalhes sobre os controladores conjuntos, a operadora e a suboperadora. Medidas rigorosas de segurança são implementadas, incluindo a criptografia dos dados armazenados e a adoção de protocolos de acesso seguros. Auditorias regulares e testes de segurança são realizados com a finalidade de prevenir incidentes de segurança e garantir a integridade dos dados. Os dados são utilizados exclusivamente para as finalidades declaradas, sem qualquer forma de discriminação contra os motoristas. Por fim, todas as empresas mantêm registros das operações de tratamento dos dados e estão preparadas para demonstrar sua conformidade com a LGPD, garantindo a proteção dos direitos dos motoristas e a eficiência das operações de transporte.

Para auxiliar na identificação do papel do agente de tratamento, a ANPD divulgou o fluxograma a seguir no Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD. [6]



6 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_reti ficada.pdf

Seção 1 - Parte Geral

A correta definição dos papeis do controlador (independente ou conjunto), operador e suboperador é essencial para garantir a conformidade com a LGPD. No setor de transportes, cada empresa envolvida no tratamento de dados deve compreender suas responsabilidades e adotar práticas que assegurem a proteção dos dados pessoais. É a partir da definição do agente de tratamento que as empresas conseguem mensurar as suas obrigações e responsabilidades na cadeia de tratamento.

O que fazer em relação às bases legadas?

Bases legadas são bases de dados e arquivos existentes na empresa antes da entrada em vigor da LGPD. Como elas foram construídas sem os parâmetros e requisitos definidos pela LGPD, elas devem receber um cuidado especial. A LGPD determina que a ANPD estabelecerá normas sobre a adequação progressiva das bases legadas (bancos de dados constituídos até a data de entrada em vigor da LGPD), consideradas a complexidade das operações de tratamento e a natureza dos dados (art. 63). Contudo, a ANPD ainda não se pronunciou sobre o tema. Independentemente disso, recomenda-se que a empresa inicie a adequação de tais bases considerando os princípios de finalidade, necessidade, adequação e qualidade dos dados.

2.5 Encarregado pelo tratamento de dados

O encarregado pelo tratamento de dados pessoais (o *Data Protection Officer* ou DPO, em inglês) é figura essencial para a implementação e a manutenção da conformidade com a LGPD. O encarregado é designado pelo controlador e pelo operador e atua como ponto focal nos temas relacionados à proteção de dados dentro de uma organização, além de ser canal de comunicação entre o controlador, os titulares e a ANPD (art. 6º, VIII, LGPD e art. 2º, V, do Regulamento do Encarregado).

A atuação do encarregado foi regulamentada pela Resolução CD/ANPD nº 18, de 16 de julho de 2024, que traz as características e obrigações do encarregado.

Quais são as obrigações do encarregado? (art. 41)

- **Canal de comunicação com os titulares:** O encarregado atua como ponto de contato entre o controlador e o titular de dados, sendo responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar as providências necessárias para resolver problemas e dúvidas.

>>

Seção 1 - Parte Geral

- **Recebimento de comunicações da ANPD para adoção de providências:** O encarregado atua também como ponto de contato entre o controlador e a Autoridade Nacional de Proteção de Dados (ANPD, sendo responsável por receber e responder as comunicações da ANPD, garantindo que, conforme necessário, sejam adotadas medidas corretivas e preventivas. Para isso, o encarregado por ter de encaminhar internamente a demanda para as unidades competentes, fornecer a orientação e a assistência necessárias ao agente de tratamento, e indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado (art. 15, Regulamento do Encarregado). Ainda, é sua função comunicar a ocorrência dos incidentes de segurança à ANPD por meio do formulário disponibilizado pela Autoridade.

- **Orientação interna:** Cabe, ao encarregado, orientar os colaboradores e contratados da entidade acerca das políticas e procedimentos adotados para proteção dos dados pessoais, promovendo treinamentos para criar uma cultura de privacidade e segurança dentro da organização e monitorando a conformidade organizacional. Entre as atribuições relacionadas ao programa de privacidade e proteção de dados, destacam-se: a manutenção do registro das operações de tratamento de dados pessoais (RoPA), a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a gestão das políticas internas e das requisições dos titulares, entre outros (art. 16, Regulamento do Encarregado ANPD). Além disso, há funções como avaliar a contratação de terceiros, gerenciar a maturidade da organização e oferecer suporte técnico-jurídico para novas iniciativas. Dentre as funções contínuas, algumas incluem a implementação do Comitê de Privacidade e o treinamento de colaboradores, já as funções contingentes abrangem atividades como a gestão do relacionamento com a ANPD, e o gerenciamento de incidentes de segurança.

- **Execução das demais atribuições:** O encarregado deve executar outras atribuições conforme determinado pelo controlador ou estabelecido em normas complementares da ANPD.

Apesar de o encarregado possuir várias atribuições, o desempenho de suas atividades não confere a ele a responsabilidade, perante a ANPD, pela conformidade do tratamento dos dados pessoais realizado pelo controlador (art. 17, Regulamento do Encarregado).

Toda empresa que realiza atividades de tratamento de dados pessoais deve indicar um encarregado, salvo exceções determinadas pela ANPD, como é o caso dos Agentes de Tratamento de Pequeno Porte (ATPPs), que não são obrigados a nomear um encarregado. Ainda assim, devem disponibilizar um canal de comunicação com o titular de dados para receber comunicações e, caso nomeiem um encarregado, essa indicação será considerada política de boas práticas e governança para fins da aplicação de sanções administrativas. [7]

A LGPD e a ANPD não estipulam critérios mínimos formais para ser um encarregado pelo tratamento de dados, no entanto, existem algumas exigências quanto a obtenção

de um conjunto de habilidades específicas pelo profissional. Nesse sentido, este deve possuir conhecimento jurídico em proteção de dados e privacidade, compreender normas e legislações pertinentes, além de entender a natureza e finalidades das operações de tratamento da organização. É recomendável ainda que o profissional tenha familiaridade com tecnologia da informação e segurança da informação, habilidades de comunicação para interagir com diversas áreas, bem como liderança, e autonomia para orientar corretamente sobre o tratamento de dados, minimizando conflitos de interesse.

Os agentes de tratamento obrigados a nomear um encarregado devem divulgar os seus dados de contato publicamente em local acessível. Contudo, esse contato não precisa ser necessariamente uma ponte direta com o encarregado. Basta a divulgação do contato da equipe do encarregado, por exemplo.

Além disso, também não é necessário divulgar informações sobre a identidade do encarregado, podendo ser disponibilizado um e-mail impessoal (dpo@empresa.com.br) ou uma plataforma para o envio de mensagens para a equipe designada. Por se tratar de dados que precisam ser divulgados publicamente, é possível que sejam enviadas comunicações sem qualquer relação com proteção de dados. Por isso, recomenda-se que as entidades usem mecanismos para filtrar as comunicações, garantindo que todas sejam endereçadas.

Exemplo

Uma empresa de transporte aquaviário coleta dados dos passageiros para emissão de bi-lhetes e gestão de embarque. Cabe, ao encarregado, orientar os colaboradores sobre a importância da proteção dos dados, garantindo que os passageiros sejam informados sobre como os dados serão usados e atuando como ponto de contato para responder dúvidas e reclamações dos passageiros.

A nomeação do encarregado é fundamental para assegurar a conformidade com a LGPD. Este processo pode ser realizado de diferentes formas, incluindo a designação de uma pessoa interna, a criação de uma área específica dentro da empresa, ou a contratação de um encarregado externo através de serviços especializados (*DPO as a Service*). Ainda, é possível a indicação de um único encarregado para o mesmo grupo econômico, desde que ele cumpra com todas as funções estabelecidas na LGPD. Não há também óbice da atuação de um mesmo encarregado em nome de diferentes organizações.

Independentemente do método escolhido, é importante formalizar a nomeação, como por meio de um contrato de prestação de serviços ou ato administrativo, detalhando as responsabilidades e estrutura de reporte dentro da organização. Recomenda-se que a nomeação e acompanhamento das atividades seja acompanhada pela alta administração da empresa ou órgão.

Seção 1 - Parte Geral

Quais são os caminhos possíveis para nomeação do encarregado?

- **Pessoa interna:** Nomear um encarregado interno envolve selecionar um colaborador da empresa, geralmente alguém contratado especificamente para o cargo ou um membro da equipe de jurídico, compliance ou segurança da informação com conhecimentos em proteção de dados. Segundo a LGPD, não há impedimento para que o encarregado desempenhe outras funções dentro da organização. No entanto, é aconselhável evitar que essas funções gerem conflitos de interesse com o papel esperado do encarregado. Esse conflito pode surgir, por exemplo, quando há acumulação de cargos que supervisionam atividades relacionadas ao tratamento de dados, as quais devem ser monitoradas de maneira imparcial pelo encarregado. Além disso, é essencial que as funções atribuídas ao colaborador permitam que ele atue como encarregado de dados sem sobrecarga, garantindo que todas as suas responsabilidades possam ser desempenhadas de maneira plena

- **Encarregado externo:** É possível ainda contratar um encarregado externo por meio do serviço especializado de DPO as a Service, prática comum para empresas que buscam otimizar os seus recursos e beneficiar-se da expertise necessária. O contrato com a empresa prestadora de serviços deve ser claro quanto às responsabilidades e às expectativas, e a nomeação poderá ser registrada em um documento formal, mencionando a empresa contratada e o profissional que atuará como encarregado.

Em qualquer cenário, o encarregado deve ter autonomia e independência funcional, podendo influenciar em decisões que afetem a política de dados pessoais da empresa, a administração da empresa, especialmente no que se refere ao desenvolvimento de novos produtos e na tomada de decisões estratégicas relacionadas ao tema.

Ainda, deve-se garantir que a atuação do encarregado não gere conflito de interesse com as suas atribuições legais. Por esse motivo, considera-se boa prática a delimitação das suas funções e a não indicação de colaboradores com atribuições comerciais para a função. Ainda, é indispensável que ele tenha conhecimentos técnicos e atualizados sobre proteção de dados. Por isso, deve-se incentivar e proporcionar meios para sua capacitação. Como o encarregado não tem um poder direto de decisão quanto às atividades de tratamento de dados, ele não assume qualquer responsabilidade pelas ações da entidade, salvo se agir comprovadamente de má-fé.

No setor de transporte, em que o tratamento de dados é intenso e diversificado, a presença de um encarregado é ainda mais importante, tendo em vista que as empresas de transporte costumam lidar com grandes volumes de dados de diferentes titulares. Assim, é o encarregado que ajuda a garantir que os dados sejam tratados conforme a LGPD e que sejam adotadas as melhores práticas de proteção de dados na empresa.

Seção 1 - Parte Geral

2.6 Encarregado pelo tratamento de dados

A LGPD impõe diferentes responsabilidades aos agentes de tratamento de dados, cujo descumprimento pode resultar em graves consequências financeiras, reputacionais e operacionais. As sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) exigem a tramitação de processo administrativo sancionador, em que a infração será apurada para determinar a sanção aplicável ao caso concreto. Por essa razão, os agentes de tratamento, ao exercerem as suas funções, devem evitar dar causa a danos patrimoniais, morais, individuais e/ou coletivos aos titulares dos dados.

As resoluções que foram editadas pela ANPD evidenciam o esforço em concretizar o disposto na LGPD, trazendo uma maior segurança jurídica aos agentes regulados. Até o momento foram editadas as seguintes resoluções: **Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador (Resolução CD/ANPD nº 01/202)**[8] e **Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD nº 04/2023)**[9].

Em caso de descumprimento com os dispositivos da legislação, as sanções administrativas previstas no art. 52 da LGPD variam de advertências a multas e outras penalidades mais severas, conforme descrito na tabela abaixo.

Sanção Administrativa	Descrição
Advertência	Aviso formal para corrigir irregularidades
Multa simples	Até 2% do faturamento, limitada a cinquenta milhões de reais por infração
Multa diária	Valor determinado até o limite de cinquenta milhões de reais
Publicização da infração	Divulgação da infração nos parâmetros e período determinado pela autoridade
Bloqueio dos dados pessoais	Interrupção do uso dos dados até regularização do tratamento
Eliminação dos dados pessoais	Exclusão definitiva dos dados tratados de forma inadequada
Suspensão parcial do funcionamento do banco de dados	Interrupção temporária de parte das operações do banco de dados

>>

8 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513
9 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077

Seção 1 - Parte Geral

Suspensão do tratamento dos dados pessoais	Interrupção temporária do tratamento de dados
Proibição parcial ou total do exercício de atividades	Proibição de realizar atividades relacionadas ao tratamento de dados

As sanções administrativas são aplicadas pela ANPD de acordo com a gravidade e a natureza da infração. Entre as penalidades já aplicadas, estão advertências formais, multas simples e publicização das infrações cometidas, que servem como um alerta público sobre as falhas de conformidade. O primeiro caso envolveu uma empresa de telecomunicações,[10] que recebeu multa e advertência respectivamente por realizar atividade de tratamento sem respaldo legal e por não nomear um encarregado pela proteção de dados.

Além desse caso, também foram julgados outros processos sancionadores, abrangendo atividades do setor público, com diferentes tipos de sanções, a depender da infração. No geral, os processos versavam sobreas consequências de incidentes de segurança, como o dever de comunicar e de empregar melhores esforços para garantir a segurança do tratamento realizado por entidades do Poder Público. As sanções variaram de acordo com a gravidade das infrações e o impacto para os titulares nos casos concretos.

É possível depreender destes primeiros casos julgados pela ANPD que configuram infrações à LGPD sancionáveis (i) a demora em notificar a ANPD e os titulares dos dados acerca de um incidente de segurança (art. 48, da LGPD), (ii) a ausência de políticas mínimas de segurança da informação (art. 49, da LGPD) e (iii) a ausência de mecanismos de controle e eventual resposta inadequada a um incidente de segurança confirmado (art. 48, da LGPD), ausência de resposta às requisições da ANPD (art. 5º, I, do Regulamento de Fiscalização), entre outros.

Ainda, em tais casos, a ANPD destacou a necessidade de treinamentos contínuos e do fortalecimento de uma cultura organizacional voltada à proteção de dados, pois a falta de conscientização dos colaboradores sobre melhores práticas de segurança contribui para a ocorrência e má gestão dos incidentes de segurança. Por isso, as empresas devem investir em capacitação constante, a fim de prevenir e mitigar os impactos de futuros incidentes.

10 https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf

Seção 1 - Parte Geral

Tellekall Infoservice [11]

O caso versa sobre a oferta aos candidatos às eleições municipais de uma listagem de contatos de WhatsApp de eleitores de Ubatuba/SP pela Telekall Infoservice para disseminação de material de campanha eleitoral. A empresa não comprovou a nomeação de encarregado de dados, obrigação prevista na LGPD, e não respondeu às requisições da ANPD ao longo do processo, infringindo o art. 5º, I, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. A ANPD entendeu que não foram identificadas hipóteses de tratamento que pudessem respaldar a atividade comercial da Telekall nos moldes em que era desenvolvida e, diante da ausência de base legal para o tratamento de dados, da não apresentação das informações solicitadas e ainda da falta de nomeação do encarregado, a empresa foi sancionada em advertências e obrigação de pagar uma multa no valor de R$ 14.400,00 (quatorze mil reais).

Instituto de Assistência ao Servidor Público Estadual de São Paulo (IAMSPE) [12]

O processo sancionador foi iniciado por conta da falha de segurança em um site sob controle do Governo do Estado de São Paulo. Por meio da exploração desta falha, foi possível acessar dados pessoais de titulares vinculados ao Instituto de Assistência ao Servidor Públicsagens SMS para um grupo menor de titulares e enviou e-mails para um grupo maior de titulares. Contudo, tais comunicações foram realizadas em prazo superior àquele determinado pela ANPD e com conteúdo supostamente em desconformidade com a LGPD. Além disso, o IAMSPE não adotava controles de acesso aos seus sistemas, configurando infração ao dever dos agentes de tratamento de utilizar sistemas seguros. Por isso, foi aplicada a sanção de advertência, com a indicação de medida corretiva.

Secretaria de Estado de Saúde de Santa Catarina (SES/SC) [13]

O caso versa sobre incidente de segurança sofrido pela SES/SC, em que dados de 48 mil titulares teriam sido exfiltrados. Diante do incidente, a SES/SC realizou a comunicação do o Estadual de São Paulo (IAMSPE). O IAMSPE realizou a comunicação do incidente por meio de men incidente para o público geral, não individualizado, mas em prazo irrazoável, segundo a ANPD. Em virtude do transcurso de tempo entre o incidente e a comunicação, a ANPD aplicou a sanção de advertência à SES/SC e medidas corretivas, determinando o envio de comunicado individualizado para os titulares afetados. A ANPD entendeu que o uso de sistema sem a devida segurança pela SES/SC pode afetar significativamente os direitos dos titulares. A falta de cuidado no desenvolvimento de um sistema seguro viabilizou a ocorrência de um incidente que pode ser causa para fraudes financeiras e uso indevido de identidade. Por isso, a ANPD aplicou a sanção de advertência. Ainda, como a SESC/SC não apresentou o relatório técnico do incidente, a ANPD concluiu que houve obstrução à atividade de fiscalização, já que a falta do documento impediu a avaliação das medidas técnicas adequadas e suficientes para prevenir e mitigar os efeitos do incidente. Como sanção, a ANPD novamente aplicou advertência.

11 https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf
12 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf
13 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-sesc-sc-00261001886202251-autos-publicos.pdf

Seção 1 - Parte Geral

Instituto Nacional do Seguro Social (INSS) [14]

Em 2022, o INSS apresentou uma comunicação de incidente de segurança preliminar à ANPD em virtude da identificação do aumento relevante no número de consultas a dados pessoais sem aparente justificativa operacional ou de negócios nos sistemas do INSS. A conduta foi analisada pela ANPD, que concluiu que o órgão não comunicou os titulares sobre o incidente de segurança e não atendeu às requisições da ANPD durante o processo. A falta de comunicação do incidente foi classificada como uma infração grave, por ter afetado significativamente interesses e direitos fundamentais dos titulares de dados. A sanção aplicada ao INSS foi de publicização da infração, considerando a relevância e o interesse público do caso. A ANPD inclusive apresentou sugestão de texto a ser publicado pelo INSS na primeira página do seu sítio eletrônico.

Secretaria de Estado de Educação do Distrito Federal (SEEDF) [15]

A ANPD apurou que a SEEDF expôs indevidamente dados pessoais de estudantes em razão de falha de segurança no formulário de inscrição do Programa Educação Precoce, construído com a ferramenta Google Forms. As respostas enviadas ficaram publicamente disponíveis, mostrando dados cadastrais e de saúde de 3.030 crianças e adolescentes, bem como de seus responsáveis. A SEEDF esclareceu que, diante desse problema, alterou a configuração do link de inscrição para não permitir a visualização das respostas, além de passar a realizar o download e a exclusão das respostas diariamente. Contudo, a ANPD seguiu investigando o caso sob o prisma da ocorrência de um incidente de segurança, solicitando diversos documentos à SEEDF. No fim das contas, a ANPD sancionou a SEEDF pela ausência de um registro de operações de tratamento (RoPA) e do relatório de impacto à proteção de dados (RIPD), quando solicitados pela Autoridade, em razão das obrigações previstas nos art. 37 e 38 da LGPD. Além disso, a SEEDF foi sancionada pela falta de comunicação do incidente aos titulares em prazo razoável após a determinação pela ANPD, o que foi feito por meio da aplicação de advertência.

Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS) de Pernambuco [16]

O caso versa sobre um incidente de segurança comunicado pela Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS) de Pernambuco, no qual dados pessoais de 413 cadastrados no Programa PE Livre Acesso Intermunicipal, iniciativa que concede gratuidade a pessoas com deficiência em transportes intermunicipais, teriam sido expostos. A ANPD analisou se este fato violou os arts. 48 e 49 da LGPD, em razão da falta de comunicação aos afetados pelo incidente em prazo razoável após a determinação pela ANPD e a ausência de sistemas seguros para o acesso aos dados dos beneficiários do programa. A ANPD concluiu que a não adoção de sistemas estruturados conforme requisitos de segurança, padrões de boas práticas e governança e princípios gerais da LGPD configura violação ao art. 49 da LGPD. Assim, a ANPD sancionou a SAS por meio da aplicação de uma advertência, além de medidas corretivas.

14 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-de-instrucao-1_2024.pdf.
15 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-instrucao-2-2024_sec-educacao-gdf.pdf.
16 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf.

Seção 1 - Parte Geral

Como consequência de uma regulação responsiva, a ANPD, no seu Mapa de Temas Prioritários,[17] indicou que os temas prioritários para atividades de fiscalização entre 2024 e 2025: os direitos dos titulares, o tratamento de dados pessoais de crianças e adolescentes, a inteligência artificial e tratamento de dados pessoais, e a raspagem de dados e agregadores de dados. A definição desses temas visa justamente definir as prioridades para os estudos e atividades de fiscalização da ANPD. No entanto, isso não quer dizer que a ANPD apenas fiscalizará a aplicação desses temas. Quanto aos setores prioritários, no Relatório de Ciclo de Monitoramento,[18] a ANPD indica que acompanhará alguns setores mais de perto, como de agregadores de dados, o setor público, de plataformas digitais, de telecomunicações, e os bancos, financeiras e administradoras de cartão.

Por fim, a fiscalização da LGPD não se restringe à ANPD, podendo envolver outras autoridades, como o Ministério Público e a Secretaria Nacional do Consumidor (Senacon). Os titulares dos dados também têm o direito de exigir indenizações por danos morais e materiais resultantes do tratamento inadequado dos seus dados pessoais. A ANPD criou, inclusive, um fluxo para petições dos titulares, de modo a incentivar que o titular entre em contato com o controlador antes de enviar sua petição à ANPD.

O compromisso com a governança e a segurança dos dados pessoais, portanto, não apenas previne sanções, mas fortalece a confiança nas entidades do setor de transportes.

17 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-19 -2023-fis-cgf-anpd.pdf.
18 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatori o-do-ciclo-de-monitoramento-2023-versao-final.pdf.

Seção 2 - LGPD aplicada ao setor de Transportes

3. *ACCOUNTABILITY* NA PROTEÇÃO DE DADOS NO SETOR DE TRANSPORTES

Accountability (art. 6º, X, LGPD) é um princípio fundamental na proteção de dados, especialmente no âmbito da LGPD. Ele exige que empresas demonstrem responsabilidade e transparência em suas práticas de tratamento de dados pessoais. No setor de transportes, onde grandes volumes de dados são constantemente usados, a accountability é crucial para garantir a confiança dos usuários e a conformidade com a legislação.

A adoção de medidas robustas de governança de dados, segurança da informação, treinamentos contínuos e políticas claras são essenciais para criar uma cultura de proteção de dados. Essas práticas não só ajudam a prevenir incidentes de segurança, mas também asseguram que a empresa possa responder de forma eficaz quando eles ocorrem.

A implementação de Programas de Governança em Privacidade e Proteção de Dados Pessoais, bem como a designação de responsáveis pela implementação deste, são passos importantes para garantir que todas as atividades de tratamento de dados sejam conduzidas de forma ética e segura pela organização. Ainda, a accountability promove a transparência, permitindo que os usuários compreendam como seus dados são tratados e quais são as medidas adotadas para protegê-los. Assim, as empresas não apenas cumprem as suas obrigações legais, mas fortalecem a sua reputação e confiança junto aos clientes e parceiros.

Exemplo

Uma empresa de transporte ferroviário de pessoas implementou um sistema robusto para responder aos direitos de titulares de dados. Nesse sistema, a empresa consegue gerir, de forma facilitada, o banco de dados de passageiros por meio da compilação de dados e das finalidades associadas, como o envio de campanhas de marketing, a emissão de bilhete, e o envio de pesquisa NPS (Net Promoter Score). Assim, a empresa consegue responder pedidos de acesso e retificação de titulares imediatamente.

Esse sistema foi desenvolvido para atender o requisito de accountability, assegurando eficiência, transparência e conformidade com a LGPD. Primeiro, registra e documenta todas as etapas do processo, garantindo que cada ação seja rastreável e auditável. Isso permite verificar se as medidas necessárias foram tomadas para localizar e revisar os dados. Por outro lado, a verificação de identidade e a validação dos dados garantem que as informações sejam tratadas de forma precisa e segura. Essa verificação é feita a partir dos dados que o passageiro informou para a empresa. Ainda, a documentação detalhada ajuda a empresa a demonstrar a sua conformidade legal às autoridades reguladoras, caso necessário. Já a avaliação interna pós-processo identifica possíveis pontos de melhoria, aumentando a eficiência e qualidade de um atendimento futuro. Portanto, a accountability não só assegura o cumprimento das obrigações legais, mas reforça a confiança dos passageiros na proteção dos seus dados pessoais, mostrando um compromisso contínuo com a transparência e a melhoria dos processos internos.

>> Capítulo 3

Seção 2 - LGPD aplicada ao setor de Transportes

3.1 Sensibilização e criação de uma cultura de proteção de dados

Conforme destacado anteriormente neste Guia de Boas Práticas, a responsabilidade pelo tratamento de dados pessoais recai sobre os agentes de tratamento, inclusive quando realizadas por seus colaboradores (art. 42, LGPD).

Dada a frequência com que as atividades empresariais envolvem o tratamento de dados, é crucial que o conhecimento sobre a proteção de dados pessoais seja amplamente disseminado entre todos os membros de uma organização.

Para tanto, as seguintes práticas podem auxiliar na sensibilização dos envolvidos e na criação da cultura interna de proteção de dados.

- **Adoção de ferramentas de sensibilização eficazes.** É importante integrar a proteção de dados no dia a dia dos colaboradores. Isso demanda a implementação de estratégias de sensibilização e ferramentas educativas eficazes para uma conscientização contínua da importância da privacidade e segurança dos dados, garantindo que o tema se torne uma responsabilidade compartilhada por todos na organização.

- **Difusão de conhecimento e realização de treinamentos contínuos.** A criação da cultura de proteção de dados dentro das organizações vai além do mero cumprimento das leis. Envolve a disseminação de noções básicas sobre proteção de dados por meio de ações de sensibilização, fortalecimento da cultura organizacional e treinamentos específicos.

É essencial realizar ações de conscientização periódicas para setores estratégicos das empresas que lidam diretamente com o tratamento de dados pessoais. Isso pode ser feito através de diversas ferramentas, como:

- Guias e cartilhas informativas
- Materiais educativos em formato de “pílulas de conhecimento”
- Palestras e campanhas de endomarketing
- Divulgação de informações em sites, intranet e redes sociais da empresa
- Criação de vídeos institucionais e campanhas temáticas s de maneira plena
- Realização de treinamentos regulares

Seção 2 - LGPD aplicada ao setor de Transportes

Os programas de conscientização devem abranger colaboradores, terceirizados, parceiros, fornecedores, prestadores de serviço, entre outros. Além disso, é importante que áreas críticas, como de Segurança da Informação, Recursos Humanos, Atendimento ao cliente, Marketing e a própria Direção recebam treinamentos específicos.

Treinamentos regulares são muito importantes para garantir que todos os colaboradores compreendam as práticas de proteção de dados das empresas. Preferencialmente, estes treinamentos devem ser conduzidos por especialistas, incluindo o próprio encarregado de proteção de dados da empresa. É necessário monitorar a participação e compreensão do conteúdo pelos colaboradores, oferecendo treinamentos adicionais, caso necessário.

Os materiais dos treinamentos devem estar permanentemente disponíveis, além de ser atualizados periodicamente. De preferência, mensagens de conscientização sobre temas de proteção de dados devem ser publicadas nos portais da empresa, como a intranet. Recomenda-se a realização frequente de treinamentos e a promoção de eventos sobre o tema, incentivando a participação de todos os colaboradores.

- **Condução de simulações, inclusive sobre incidentes de segurança** (art. 50, § 2º, I, "g", LGPD). A condução de simulações de incidentes de segurança é uma prática essencial para preparar a equipe de uma empresa para responder de maneira eficaz a possíveis ameaças à segurança da informação. Essas simulações, conhecidas como exercícios de tabletop, permitem que a organização avalie a eficácia do seu plano de resposta a incidentes, além de identificar, de forma preventiva, possíveis vulnerabilidades em seus sistemas e procedimentos.

Durante as simulações, cenários realistas de incidentes devem ser criados, incluindo cenários como ataques cibernéticos e vazamentos de dados até falhas operacionais. A equipe envolvida na simulação deve endereçar o caso fictício seguindo as diretrizes estabelecidas no plano de resposta a incidentes da organização, permitindo uma avaliação prática e detalhada da prontidão e capacidade de resposta dos colaboradores.

Além de testar a eficácia dos procedimentos da empresa, as simulações de incidentes de segurança servem como uma ferramenta de treinamento valiosa aos colaboradores. Elas ajudam a fortalecer a comunicação e coordenação entre diferentes áreas, promovendo uma compreensão clara das responsabilidades de cada uma nos casos de ocorrência de um incidente de segurança real.

Através dessas práticas, os colaboradores ganham confiança e experiência na gestão de crises, o que é crucial para minimizar o impacto de um incidente verdadeiro. Após cada simulação, deve-se realizar uma análise detalhada dos resultados, identificando pontos de melhoria e atualizando os planos e políticas de segurança, conforme necessário. Isso aumenta as chances da organização estar preparada para enfrentar e mitigar ameaças à segurança de seus dados e operações.

Seção 2 - LGPD aplicada ao setor de Transportes

Exemplo

Uma empresa de transporte aquaviário realiza regularmente simulações de incidentes de segurança como parte de suas medidas de accountability e de conformidade com a LGPD. Em uma dessas simulações, a empresa testa um cenário onde um colaborador inadvertidamente compartilha credenciais de acesso a um sistema de dados pessoais com um fornecedor externo. Durante a simulação, os procedimentos de resposta são acionados imediatamente. A equipe de TI identifica a brecha de segurança e isola o acesso comprometido. Simultaneamente, a equipe de comunicação interna começa a elaborar notificações para os titulares dos dados e a ANPD, detalhando o incidente e as medidas tomadas. Os exercícios de simulação destacam pontos fracos no processo de resposta a incidentes de segurança, como a necessidade de treinamentos adicionais sobre o manuseio seguro de credenciais. Por isso, a empresa reforça suas políticas de segurança cibernética, garantindo que os fornecedores compreendam e sigam os seus protocolos de segurança. Quando um incidente real ocorre, a empresa aplica as lições aprendidas nas simulações.

Portanto, simulações permitem que a empresa melhore continuamente suas respostas a incidentes e a resiliência de seus sistemas de segurança. Sua prática constante e a avaliação crítica dos resultados asseguram que, em situações reais, a empresa esteja bem preparada para proteger os dados pessoais dos passageiros, minimizar impactos e manter a confiança do público.

- **Designação de "embaixadores da privacidade".** Os embaixadores da privacidade (*privacy champions*) são colaboradores de diferentes departamentos que são escolhidos para auxiliarem na disseminação de boas práticas e conscientização de seus colegas sobre a importância de temas de privacidade e proteção de dados na sua organização. Eles atuam como pontos de referência nas suas respectivas áreas e facilitam a comunicação e a implementação de políticas de proteção de dados, além de oferecer suporte e orientação sobre questões relacionadas ao tema. Ainda, eles participam de treinamentos avançados e têm o dever de se manterem atualizados sobre matérias legais, regulatórias e técnicas em matéria de proteção de dados. Essa abordagem descentralizada não apenas fortalece a adesão de colaboradores às políticas internas, como também cria um ambiente de trabalho onde a privacidade é valorizada e respeitada por todos.

- **Implementação de programa contínuo de governança em proteção de dados** (art. 50, § 2º, I, "h", LGPD). Essa medida é fundamental para garantir a conformidade com a LGPD. O princípio da accountability, presente na LGPD, exige que organizações demonstrem a adoção de medidas eficazes de proteção de dados, incluindo a criação de políticas e salvaguardas baseadas em risco. A implementação de um programa de governança robusto requer a fixação de controles internos flexíveis e alinhados às especificidades do negócio e do tratamento de dados, além de sua contínua atualização.

Seção 2 - LGPD aplicada ao setor de Transportes

- **Desenvolvimento de estrutura de governança** (art. 50, § 2º, I, "f", LGPD). Essa medida é essencial para assegurar que as empresas adotem práticas eficazes de proteção de dados. Essa estrutura envolve a criação de políticas e processos claros, a designação de responsabilidades específicas e o estabelecimento de mecanismos de monitoramento e de controle robustos, de forma a garantir a conformidade contínua com a LGPD. A governança eficaz inclui a formação de comitês de privacidade e a designação de um encarregado de proteção de dados para supervisionar as atividades relacionadas ao tema.

A implementação de auditorias regulares e a realização de avaliações de risco contínuas (art. 50, § 2º, I, "d", LGPD) podem ajudar a identificar e mitigar potenciais ameaças à segurança preventivamente. Esta abordagem assegura que todas as ações relacionadas à proteção de dados sejam coordenadas, transparentes e ainda alinhadas com os objetivos estratégicos da empresa, promovendo uma cultura organizacional comprometida com a segurança e privacidade.

- **Engajamento da liderança.** O engajamento dos líderes das empresas é indispensável para o sucesso dos programas de proteção de dados. Os líderes devem ser capazes de dar o exemplo no cumprimento das diretrizes institucionais e incentivar uma cultura de proteção de dados na organização. A adoção de uma norma interna de boas práticas pode ser uma estratégia eficaz para envolver lideranças e colaboradores na temática.

Checklist das medidas de sensibilização e criação de cultura em proteção de dados

- [ ] Adoção de ferramentas de sensibilização eficazes
- [ ] Difusão de conhecimento e realização de treinamentos contínuos.
- [ ] Condução de simulações, inclusive de incidentes de segurança
- [ ] Designação de embaixadores da privacidade (privacy champions)
- [ ] Implementação de um programa contínuo de governança e accountability
- [ ] Desenvolvimento de uma estrutura de governança
- [ ] Engajamento da liderança

Seção 2 - LGPD aplicada ao setor de Transportes

A criação de uma cultura interna de proteção de dados é um desafio contínuo que requer o comprometimento de toda a organização. Através dos treinamentos específicos, de programas eficazes e do engajamento das lideranças, as empresas podem promover a conformidade legal e fortalecer a confiança de clientes e parceiros estratégicos.

3.2 Principais medidas práticas para adequação à LGPD

Para garantir a sua conformidade com a LGPD, as empresas do setor de transportes devem adotar uma série de medidas práticas. Este tópico detalha seis medidas essenciais, proporcionando um guia prático e detalhado para implementação de cada medida.

MEDIDA 1

Mapeamento das Atividades de Tratamento de Dados Pessoais

O mapeamento das atividades de tratamento de dados pessoais é o primeiro passo para uma empresa se adequar à LGPD. Esse processo envolve a identificação e a documentação de todas as operações que envolvem dados pessoais (art. 37, LGPD). É essencial entender como os dados pessoais são coletados, processados, armazenados e compartilhados, entre outros, para que sejam adotadas medidas de proteção eficazes e adequadas à realidade da empresa (operacional e financeira).

Exemplo

Uma empresa de transporte rodoviário deve mapear o fluxo dos dados desde a coleta de informações de motoristas (como habilitação, exames toxicológicos e resultados de bafôme-tro) até o armazenamento seguro das informações em sistemas internos e a posterior eli- minação dos dados após o término da relação contratual e vencimento de eventuais prazos legais aplicáveis. Além disso, deve mapear os dados dos passageiros que foram coletados para prestação dos serviços de transporte, a exemplo dos dados de reserva e de pagamento, garantindo que todas as etapas estejam documentadas.

Passo 1: Identificação de Dados Pessoais. Liste todos os tipos de dados coletados por cada departamento separadamente, incluindo dados de identificação (nome, CPF, endereço), dados financeiros (número de conta bancária, cartão de crédito), dados de localização (GPS, endereço do IP) e dados sensíveis (saúde, biometria), ou quaisquer outros capazes de identificar um indivíduo, direta ou indiretamente.

Seção 2 - LGPD aplicada ao setor de Transportes

Passo 2: Mapeamento de Fluxos. Documente como os dados são coletados, utilizados, armazenados, compartilhados, descartados ou retidos. Identifique os pontos de entrada (onde os dados são coletados) e saída (para onde os dados são transferidos ou como são destruídos). Sempre que possível, é relevante armazenar evidências de que estes procedimentos são implementados e seguidos.

Atenção!

O produto do mapeamento dos fluxos de dados é o Registro das Operações de Tratamento de Dados Pessoais (ROT ou RoPA, na sigla em inglês), exigido pela LGPD no art. 37 para controladores e operadores de dados.

Passo 3: Ferramentas. Se possível, utilize ferramentas de mapeamento de processos para visualizar os fluxos de dados e identificar pontos críticos, como, por exemplo, planilhas e/ou sistemas próprios desenvolvidos para essa função.

MEDIDA 2

Análise de Risco do Tratamento

A análise de risco (*gap analysis*) avalia os riscos associados ao tratamento de dados pessoais e identifica as lacunas nas práticas de proteção de dados da empresa (art. 50, § 2º, I, "d", LGPD). Essa etapa é fundamental para antecipar e prevenir problemas, bem como implementar medidas preventivas (art. 38, parágrafo único, LGPD).

Exemplo

Para uma empresa ferroviária, a análise de riscos poderá identificar a necessidade de utilizar métodos de criptografia para dados de passageiros armazenados nos sistemas de reserva, a fim de evitar acessos não autorizados. Ainda, pode incluir a avaliação de sistemas de controle de acesso nas estações, de forma a garantir que apenas o pessoal autorizado tenha acesso a áreas restritas.

Seção 2 - LGPD aplicada ao setor de Transportes

Passo 1: Identificação de Riscos. Liste os possíveis riscos associados ao tratamento de dados pessoais, como acesso não autorizado, vazamento ou perda de dados, falhas nos sistemas de segurança, entre outros.

Passo 2: Avaliação de Impacto. Avalie qual é o impacto e a probabilidade de cada risco identificado. Considere o potencial dano aos titulares e a gravidade das consequências para a empresa.

Passo 3: Medidas de Mitigação. Proponha medidas para mitigar os riscos identificados, como a implementação de controles de segurança adicionais, políticas de acesso restrito, e treinamentos específicos para colaboradores.

MEDIDA 3

Estruturação da Governança em Privacidade

A estruturação da governança em privacidade envolve a criação de um framework de governança que assegure a conformidade contínua com a LGPD. Isso inclui a definição de políticas e responsabilidades claras para que todas as áreas estejam alinhadas com os princípios de proteção de dados.

Exemplo

Uma empresa de transporte aéreo pode criar um comitê de privacidade composto por membros das áreas de TI, jurídico, operações e atendimento ao cliente. Esse comitê se reunirá regularmente para revisar as políticas de privacidade, avaliar a conformidade e discutir quaisquer incidentes ou problemas relacionados à proteção de dados.

Sugestão 1: Nomeação de Encarregado (art. 41, LGPD). Nomeie um encarregado de proteção de dados (Data Protection Officer ou DPO, em inglês) que ficará responsável pela conformidade da empresa com a LGPD. O encarregado deve ter conhecimento especializado em proteção de dados, se possível, e estar capacitado para lidar com a ANPD e os titulares de dados.

Sugestão 2: Políticas e Procedimentos (arts. 46, 49, e 50, § 2º, I, “a” e “b”, LGPD). Desenvolva políticas e procedimentos para o tratamento de dados pessoais na empresa, abordando questões relativas à coleta, uso, compartilhamento, retenção e descarte de dados. Ademais, inclua diretrizes específicas para diferentes departamentos, como Recursos Humanos, Marketing e TI.

Sugestão 3: Comitê de Privacidade Estabeleça um comitê interno de privacidade que supervisione a conformidade e a implementação das políticas de proteção de dados. O comitê deve incluir representantes de diferentes áreas da empresa para garantir uma abordagem integrada.

Seção 2 - LGPD aplicada ao setor de Transportes

MEDIDA 4

Revisão de Documentos e Contratos

A revisão de documentos e contratos é essencial para garantir que todas as relações contratuais estejam em conformidade com a LGPD, incluindo as cláusulas contratuais de proteção de dados. Isso assegura que todas as partes envolvidas estejam cientes de suas responsabilidades e obrigações em relação ao tratamento de dados (art. 42, LGPD).

Exemplo

Uma empresa de logística rodoviária deve revisar os contratos com seus fornecedores de tecnologia para garantir que existam obrigações específicas de conformidade com a LGPD, como a proteção adequada dos dados de clientes e colaboradores. Além disso, deve incluir cláusulas específicas sobre o processamento de dados de rastreamento de carga, garantindo que os dados sejam tratados de forma segura e conforme a LGPD.

Sugestão 1: Revisão de Contratos. Revise os contratos com fornecedores, parceiros e clientes para incluir cláusulas específicas de proteção de dados pessoais. Essas cláusulas devem abordar questões como responsabilidades de cada parte, medidas de segurança e procedimentos para lidar com solicitações dos titulares e notificações de incidentes.

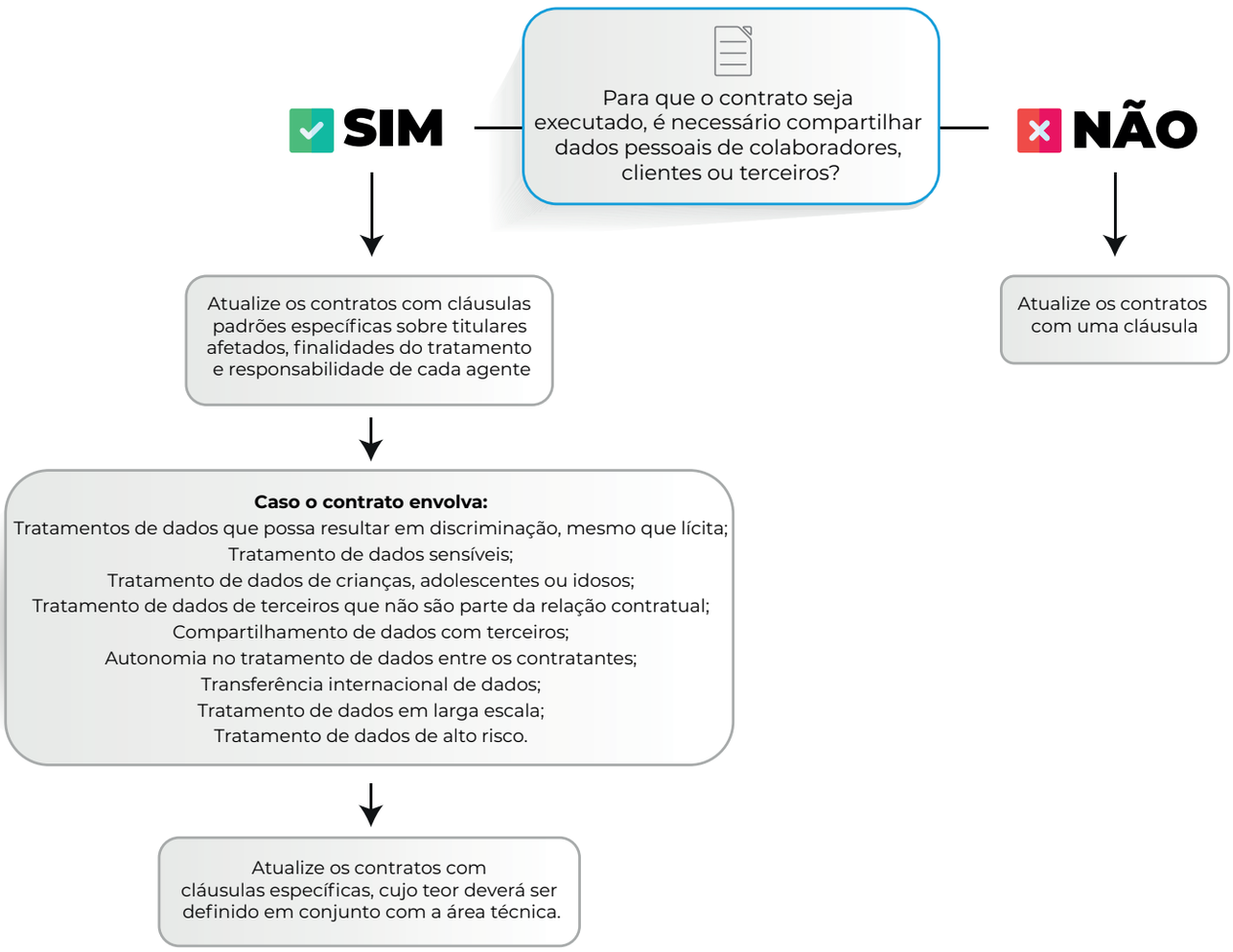
Boas práticas para contratos com terceiros

Sempre que as empresas firmarem contratos com terceiros que envolvam o tratamento de dados pessoais, recomenda-se:

- A inclusão de cláusulas específicas de proteção de dados e/ou a assinatura de um acordo de compartilhamento de dados específico que garantam que os dados pessoais serão protegidos pelo terceiro ao menos na mesma medida que originariamente, a depender da complexidade do contrato e do nível de compartilhamento de dados necessário para a sua execução;
- A condução de diligência prévia e contínua do terceiro (caso seja contratado como fornecedor ou prestador de serviço), para atestar o cumprimento das obrigações contratuais assumidas quanto ao tratamento de dados e aquelas relacionadas ao cumprimento da LGPD;
- A definição clara, inclusive por via contratual, dos papeis de cada agente envolvido (como controlador, operador ou suboperador), e das obrigações e responsabilidades de cada agente;
- A definição detalhada, no contrato ou em documento a ele anexo, de obrigações específicas de compartilhamentos de dados necessários à execução do contrato principal (como de dados pessoais previdenciários e trabalhistas, quando aplicável); e
- Quando a empresa contratada subcontratar terceiros para realizar uma ou mais operações de tratamento de dados, recomenda-se que seja firmado contrato com a empresa subcontratada, contendo as mesmas obrigações previstas na cláusula de proteção de dados ou no acordo de compartilhamento de dados firmado entre a organização e a empresa contratada.

Seção 2 - LGPD aplicada ao setor de Transportes

Para a revisão dos contratos, o seguinte fluxograma pode ser seguido:



Sugestão 2: Documentos Internos. Atualize os documentos internos, como políticas de privacidade, termos de uso e manuais de procedimentos, a fim de refletir as práticas de proteção de dados da empresa e garantir a conformidade com a LGPD.

MEDIDA 5

5 Atendimento aos Titulares de Dados

O atendimento aos titulares de dados envolve estabelecer canais eficazes para que os titulares possam exercer os seus direitos sob a LGPD, como acesso, correção, exclusão e portabilidade de dados (arts. 9°, VII, 18, e 50, § 2°, I, “e”, LGPD). Esse processo deve ser eficiente e transparente, a fim de garantir a confiança dos titulares de dados.

Seção 2 - LGPD aplicada ao setor de Transportes

Direitos dos titulares (arts. 18, 19 e 20 da LGPD)

- Saber se a empresa trata algum dado pessoal (art. 18, I, LGPD);
- Saber quais dados pessoais são tratados pela empresa (art. 18, II, LGPD);
- Corrigir dados incompletos, inexatos ou desatualizados (art. 18, III, LGPD);
- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou que, porventura, tenham sido tratados em desconformidade com a lei (art. 18, IV, LGPD);
- Solicitar a portabilidade dos dados a outro fornecedor de serviço ou produto (art. 18, V, LGPD);
- Solicitar a eliminação dos dados tratados com o consentimento (art. 18, VI, LGPD);
- Obter informações sobre as entidades públicas ou privadas com as quais a empresa compartilha os dados (art. 18, VII, LGPD);
- Quando a atividade de tratamento necessitar do consentimento, o titular pode se negar a consentir. Nesse caso, a empresa deve informar sobre as consequências da não realização de tal atividade. Caso o titular consinta, a qualquer momento poderá revogá-lo (art. 18, VIII e IX, LGPD);
- Pedir a revisão de decisões unicamente automatizadas que afetem seus interesses (art. 20, LGPD).

Exemplo

Uma empresa de transporte aquaviário pode criar um portal online no seu site onde os passageiros podem solicitar o acesso/correção de dados pessoais, com respostas automatizadas e eficientes. Além disso, a empresa pode estabelecer um atendimento telefônico para resolver dúvidas e solicitações dos titulares de forma rápida e eficaz.

Sugestão 1: Canais de Comunicação. Estabeleça canais claros e acessíveis para que os titulares possam enviar suas solicitações, como e-mail, formulários online ou telefone. Certifique-se de que esses canais sejam divulgados de forma ampla e acessível.

Seção 2 - LGPD aplicada ao setor de Transportes

Sugestão 2: Procedimentos Internos. Desenvolva procedimentos internos para atender prontamente às solicitações de titulares, documentando o passo a passo desse processo. Estabeleça prazos claros, de acordo com os prazos estabelecidos na LGPD, e assegure-se de que a equipe esteja treinada para responder de forma adequada e eficaz.

Sugestão 3: Treinamento de Equipe. Treine a equipe responsável pelo atendimento ao cliente sobre os direitos dos titulares e os procedimentos de resposta. Garanta que todos conheçam as obrigações legais e saibam como proceder em cada tipo de solicitação.

MEDIDA 6

6 Treinamento dos Colaboradores

O treinamento dos colaboradores é crucial para garantir que todos compreendam as suas responsabilidades e estejam capacitados para cumprir com a LGPD no dia a dia. O treinamento contínuo é essencial para manter a conformidade e a segurança dos dados.

Exemplo

Uma empresa de transporte público pode implementar treinamentos trimestrais para seus motoristas e sua equipe administrativa, focando na importância da proteção dos dados pessoais dos passageiros e práticas recomendadas para evitar violações. Além disso, pode realizar sessões para capacitação sobre como lidar com as solicitações dos titulares e como responder a incidentes de segurança.

Passo 1: Programas de Treinamento. Promova programas regulares de treinamento sobre proteção de dados e privacidade, adaptados às diferentes funções dentro da sua empresa. Inclua módulos específicos para as áreas que lidam diretamente com dados pessoais, como RH, TI e atendimento ao cliente.

Passo 2: Capacitação Contínua. Promova sessões de reciclagem e atualização sobre novos regulamentos, melhores práticas e incidentes recentes de segurança envolvendo dados pessoais. Utilize exemplos práticos e casos reais para ilustrar os pontos-chave.

Passo 3: Avaliação de Conhecimento. Realize avaliações periódicas a fim de medir a compreensão dos colaboradores sobre a LGPD e as políticas de privacidade da empresa. Utilize questionários, testes e simulações para avaliar a eficácia do treinamento.

Seção 2 - LGPD aplicada ao setor de Transportes

Checklist de ações para adequação à LGPD

1) Mapeamento das Atividades de Tratamento de Dados:

- [ ] Identificar e documentar todos os dados pessoais coletados.
- [ ] Mapear os fluxos de dados desde a coleta até o descarte.
- [ ] Utilizar ferramentas de mapeamento de processos, quando possível.

2) Análise de Risco do Tratamento:

- [ ] Identificar todos os riscos associados ao tratamento de dados.
- [ ] Avaliar o impacto e a probabilidade de cada risco.
- [ ] Propor e implementar medidas de mitigação para os riscos identificados.

3) Estruturação da Governança em Privacidade:

- [ ] Nomear um encarregado de proteção de dados (DPO).
- [ ] Desenvolver políticas e procedimentos internos para tratamento de dados.
- [ ] Estabelecer um comitê de privacidade.

4) Revisão de Documentos e Contratos:

- [ ] Revisar contratos para incluir cláusulas específicas de proteção de dados.
- [ ] Atualizar documentos internos para refletir as práticas de proteção de dados.
- [ ] Garantir que parceiros e fornecedores estejam em conformidade com a LGPD.

5) Atendimento aos Titulares de Dados:

- [ ] Estabelecer canais de comunicação claros e acessíveis.
- [ ] Desenvolver procedimentos para atender às solicitações dos titulares.
- [ ] Treinar a equipe sobre os direitos dos titulares e os procedimentos de resposta.

6) Treinamento dos Colaboradores:

- [ ] Desenvolver programas de treinamento sobre proteção de dados.
- [ ] Promover sessões de reciclagem e atualização.
- [ ] Realizar avaliações periódicas de conhecimento.

Seção 2 - LGPD aplicada ao setor de Transportes

A adoção dessas medidas práticas é fundamental para que as empresas do setor de transportes estejam em conformidade com a LGPD. Implementar essas ações não só ajuda a proteger os dados pessoais dos titulares, mas também fortalece a confiança dos clientes e parceiros, contribuindo para o sucesso e a reputação da empresa.

Medidas Contínuas

Recomenda-se que as empresas adotem medidas de conformidade e de governança contínuas:

- Atualizar os Registros de Operação de Tratamento de Dados Pessoais (RoPA) ao menos uma vez ao ano e, sempre que possível, a cada seis meses;
- Elaborar um novo RoPA sempre que um novo processo, produto ou serviço que trate dados pessoais de alguma forma for criado/instituído; e
- Dedicar maior atenção e adotar salvaguardas e precauções adicionais para os tratamentos de dados de alto risco, ou seja, aqueles que envolvam tratamento em larga escala, que possam afetar significativamente interesses e direitos fundamentais dos titulares de dados, que usem tecnologias emergentes ou inovadoras, que sejam focadas em vigilância ou controle de zonas acessíveis ao público, se baseiam em decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil do titular, ou que utilizem dados sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

3.3 Documentos relevantes para um Programa de Proteção de Dados

Além das ações práticas mencionadas, a conformidade com a LGPD também requer a criação e a manutenção de uma série de documentos essenciais. Esses documentos são fundamentais para demonstrar a conformidade com a LGPD e para proteger os dados pessoais tratados. Abaixo, serão apresentados os documentos mais relevantes da LGPD e as suas principais características.

Registro das Operações de Tratamento de Dados Pessoais (ROT ou RoPA)

O **Registro das Operações de Tratamento de Dados Pessoais (ROT ou RoPA)** é um documento que detalha todas as atividades de tratamento de dados pessoais conduzidas por uma empresa (art. 37, LGPD). Este documento serve para mapear e monitorar como os dados pessoais são coletados, utilizados, compartilhados, armazenados, descartados, ou seja, desenhar o fluxo dos dados, identificando pontos de entrada (onde os dados são coletados) e de saída (onde os dados são transferidos ou destruídos).

Seção 2 - LGPD aplicada ao setor de Transportes

Quais são os principais elementos deste documento?

- Identificação das categorias de dados pessoais tratados.
- Descrição do propósito para o qual os dados são coletados e tratados.
- Identificação da base legal que justifica o tratamento, conforme as hipóteses da LGPD.
- Detalhamento das medidas de segurança implementadas para proteger os dados.
- Indicação do período durante o qual os dados pessoais serão armazenados e critérios usados para definir esse período.
- Informações sobre compartilhamento com terceiros, incluindo identificação dos parceiros e a finalidade do compartilhamento.

Exemplo

Uma empresa de transporte rodoviário deve registrar as operações de tratamento de dados pessoais dos motoristas, incluindo a coleta de dados para controle de jornada e para manutenção de veículos e segurança. No documento, deverá constar a base legal (como cumprimento de obrigação legal), medidas de segurança (como a criptografia e os controles de acesso) e o período de armazenamento (por exemplo, cinco anos após a rescisão do contrato, conforme aplicável). Ainda, a empresa deve detalhar como os dados dos passageiros são coletados durante a compra de bilhetes, armazenados em sistemas seguros e utilizados para melhorar os serviços oferecidos, caso aplicável.

1. Liste todos os tipos de dados pessoais que a empresa coleta e trata, como dados de clientes, colaboradores e fornecedores.
2. Documente o ciclo de vida dos dados, desde a coleta até o descarte ou transferência. Se possível, use diagramas de fluxo para visualizar melhor os processos.
3. Revise e atualize o registro regularmente para refletir as eventuais mudanças no tratamento de dados ao longo do tempo.

Seção 2 - LGPD aplicada ao setor de Transportes

Relatório de Impacto à Proteção de Dados (RIPD ou DPIA)

O **Relatório de Impacto à Proteção de Dados (RIPD ou DPIA)** é um documento que avalia os riscos associados às operações de tratamento de dados pessoais que podem gerar riscos aos direitos e liberdades fundamentais dos titulares (arts. 5º, XVII, e 38, LGPD). Ele é essencial para identificar e mitigar possíveis impactos negativos.

Quais são os principais elementos deste documento?

- Detalhamento das atividades de tratamento, desde a coleta até o descarte ou transferência.
- Identificação dos tipos de dados pessoais e dados sensíveis tratados.
- Avaliação dos riscos aos direitos e liberdades dos titulares e possíveis consequências de uma violação de dados.
- Descrição das medidas e salvaguardas implementadas para mitigar os riscos.
- Explicação dos critérios e métodos utilizados para realizar a avaliação de risco.

Exemplo

Uma empresa de transporte aéreo pode elaborar o RIPD para o tratamento de dados sensíveis dos passageiros para fins de prevenção à fraudes. O relatório deve avaliar, por exemplo, riscos de eventual vazamento de dados (como o impacto na privacidade dos passageiros) e descrever as medidas de mitigação (como a adoção de criptografia e de controles de acesso restrito). Ainda, o RIPD deve abordar os riscos associados ao compartilhamento dos dados com parceiros comerciais, se existente, e as medidas de segurança implementadas para proteger esses dados.

1. Detalhe a operação de tratamento, incluindo coleta, armazenamento, uso, compartilhamento e descarte, caso ocorram durante o fluxo daquela atividade.
2. Avalie os riscos associados à operação de tratamento de dados, considerando a natureza dos dados e o contexto do tratamento.
3. Analise o impacto potencial dos riscos e estabeleça medidas de mitigação apropriadas para cada um dos riscos identificados.
4. Documente todas as etapas da análise de risco, incluindo qual foi a metodologia utilizada e quais medidas de mitigação foram e ainda serão adotadas.
5. Revise o relatório regularmente para garantir que ele reflita as práticas atuais de tratamento de dados e que as medidas de mitigação estejam atualizadas.

Seção 2 - LGPD aplicada ao setor de Transportes

Política de Privacidade

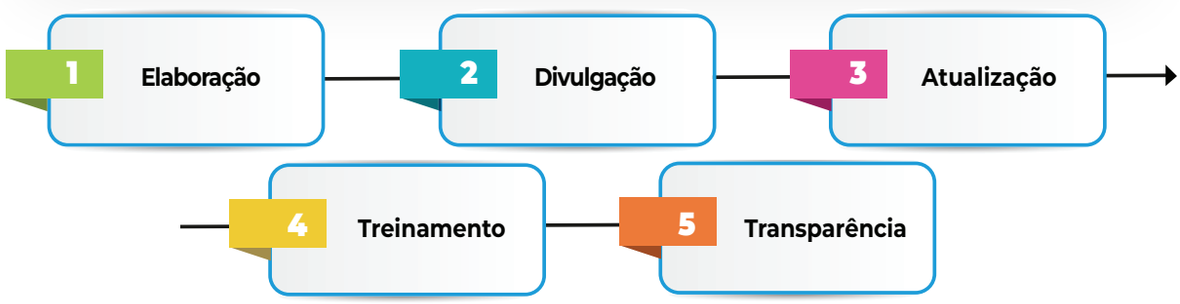
A **Política de Privacidade** é um documento público que informa aos titulares como seus dados pessoais são coletados, utilizados, compartilhados e protegidos pela empresa. Ela é fundamental para garantir a transparência e a confiança dos clientes.

Quais são os principais elementos deste documento? (art. 9º, LGPD)

- Descrição dos tipos de dados pessoais coletados e tratados.
- Explicação clara das finalidades para as quais os dados são utilizados.
- Informações sobre com quem os dados são compartilhados e por quê. No geral, não são identificadas as empresas com quem é realizado o compartilhamento, mas apenas a categoria de terceiro com quem são compartilhados: parceiros, prestadores de serviço, fornecedores, autoridades, agências reguladoras, entre outros.
- Detalhamento dos direitos dos titulares e como eles podem exercê-los.
- Descrição das medidas adotadas para proteger os dados pessoais.
- Informações de contato do encarregado e/ou do canal de comunicação para questões relacionadas à privacidade e proteção de dados.

Exemplo

Uma empresa de transporte ferroviário deve publicar uma política de privacidade no seu site, explicando como os dados dos passageiros são coletados durante a compra de bilhetes online, utilizados para melhorar serviços e compartilhados com parceiros comerciais. A política deve detalhar quais são os direitos dos passageiros, a exemplo da confirmação, acesso e correção dos dados, e fornecer informações de contato para dúvidas e solicitações. A política também deve explicar as medidas de segurança implementadas para proteger os dados, como criptografia e controle de acesso.



1. Crie uma política clara e acessível que descreva como os dados pessoais são tratados na sua empresa.
2. Publique essa política de privacidade no site da sua empresa e em outros pontos de contato com os titulares de dados.
3. Revise e atualize a política de privacidade regularmente a fim de refletir eventuais mudanças nas práticas de tratamento de dados e nas exigências legais.
4. Garanta que todos seus colaboradores compreendam adequadamente a política de privacidade e saibam como aplicá-la no dia a dia.
5. Certifique-se de que a política seja escrita em língua portuguesa, com uma linguagem clara e acessível, para que os titulares possam entender facilmente as práticas de tratamento de dados da sua empresa.

Seção 2 - LGPD aplicada ao setor de Transportes

Teste de Balanceamento

O **Teste de Balanceamento** é uma avaliação realizada para determinar se o tratamento de dados pessoais poderá ser justificado com base no legítimo interesse do controlador ou de terceiros, conforme art. 7º, IX, da LGPD. O objetivo é identificar se direitos e liberdades fundamentais do titular podem ser colocados em risco(art. 10, LGPD). Segundo a ANPD[19], este teste também deve ser aplicado em situações que envolvam o uso da base legal de prevenção à fraude e à segurança do titular (art. 11, II, "g", LGPD).

Quais são os principais elementos deste documento?

- Indicação da finalidade do tratamento e interesse legítimo que o justifica.
- Avaliação da real necessidade do tratamento para atingir a finalidade.
- Balanceamento entre o interesse legítimo do controlador ou terceiro e os direitos e liberdades dos titulares, garantindo que os últimos não sejam desrespeitados.
- Medidas adicionais implementadas para proteger os dados e mitigar riscos do tratamento.

Exemplo

Uma empresa de logística pode realizar um teste de legítimo interesse para justificar o monitoramento dos motoristas via GPS, argumentando que é necessário para garantir a segurança das entregas e a eficiência operacional. O teste deve incluir a análise dos benefícios à empresa, necessidade do monitoramento e salvaguardas implementadas, como a limitação do acesso aos dados de localização e a anonimização dos relatórios. Ainda, a empresa deverá documentar a análise e revisar periodicamente a justificativa para garantir que ela continue sendo válida ao longo do tempo.

Para identificar se o legítimo interesse é a melhor base legal, pode ser utilizado um teste de três etapas, que deve verificar a finalidade, a necessidade e a proporcionalidade do tratamento. A ANPD, em seu Guia Orientativo[20], preconiza os parâmetros a seguir para a realização do Teste de Balanceamento. Importante notar que eles não são de adoção obrigatória, mas fornecem um claro cenário do que a ANPD considera como requisitos adequados de análise para fundamentar a base legal.

Fase 1: **Identificar o legítimo interesse**	**Natureza dos dados pessoais** • Qual a natureza dos dados pessoais? • Existe tratamento de dados pessoais sensíveis? Em caso afirmativo, o tratamento não pode ser realizado com base na hipótese legal do legítimo interesse. **>>**

20 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf.

Seção 2 - LGPD aplicada ao setor de Transportes

Fase 1: **Identificar o legítimo interesse**	**Dados de crianças e adolescentes** • Serão tratados dados de crianças e adolescentes? • Em caso positivo, o que foi considerado como melhor interesse dos titulares? • Quais os critérios utilizados para a ponderação entre os interesses do controlador ou de terceiro e os direitos dos titulares? • O tratamento gera riscos ou impactos desproporcionais e excessivos, considerando a condição da criança e do adolescente como sujeito de direitos? • O controlador possui uma relação prévia e direta com os titulares crianças e adolescentes? • O tratamento visa assegurar a proteção de direitos e interesses dos titulares ou viabilizar a prestação de serviços que os beneficiem? **Interesse e finalidades legítimas** • Qual benefício ou proveito resulta do tratamento de dados pessoais para o controlador ou terceiro? • O interesse é compatível com o ordenamento jurídico? Ou seja, o tratamento é compatível com princípios, normas jurídicas e direitos fundamentais? • Aplicam-se ao caso hipóteses legais que vedam ou impeçam a realização do tratamento? • O tratamento contraria, direta ou indiretamente, disposições legais ou princípios aplicáveis ao caso? • Qual a finalidade do tratamento? A finalidade é legítima, específica e explícita? **Situação concreta** • O interesse é baseado em uma situação clara, concreta e não especulativa? • Qual é essa situação concreta, de forma detalhada? • Qual o contexto em que é realizado o tratamento?
Fase 2: **Testar a necessidade do tratamento**	**Tratamento e finalidade pretendida** • O tratamento é necessário para atingir os interesses -analisados no passo anterior? • É possível usar outros meios razoáveis para atingir a mesma finalidade de forma menos intrusiva para o titular? **>>**

Seção 2 - LGPD aplicada ao setor de Transportes

Fase 2: **Testar a necessidade do tratamento**	**Minimização** • Estão sendo utilizados apenas os dados estritamente necessários para atingir a finalidade pretendida? • Existem formas menos intrusivas, menos onerosas ou com menores riscos ao titular que poderiam ser utilizadas para atingir a mesma finalidade?
Fase 3: **Testar a proporcionalidade do tratamento**	**Legítima expectativa** • O tratamento dos dados pessoais para a finalidade pretendida é razoavelmente esperado pelos titulares, considerando o contexto em que é realizado? A avaliação quanto à legítima expectativa deve levar em consideração, entre outros, os seguintes fatores relevantes: • Existe uma relação prévia do controlador com o titular? • Qual a fonte e a forma por meio das quais os dados foram coletados? Isto é, foram coletados diretamente do titular, de fontes públicas ou foram obtidos por meio de compartilhamento realizado por terceiros? • Qual o contexto e o período da coleta dos dados pessoais? • A finalidade original da coleta é compatível com o tratamento baseado no legítimo interesse? Há expectativa do titular de que esses dados sejam tratados? **Riscos e impactos aos direitos e liberdades fundamentais** • De que forma os titulares de dados pessoais serão impactados pelo tratamento? • Direitos e garantias fundamentais como liberdade de expressão, locomoção, não discriminação, intimidade, integridade física e moral podem ser afetados com o tratamento? • Quais são os riscos em potencial sobre os titulares? • Os direitos e liberdades fundamentais dos titulares prevalecem sobre os interesses do controlador ou de terceiro? **Salvaguardas e mecanismos de opt-out e de oposição** • Quais medidas são adotadas para mitigar os riscos identificados? • Quais medidas de transparência são adotadas? Serão disponibilizadas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e respectivos agentes de tratamento? • Será disponibilizado canal de fácil acesso, por meio do qual os titulares podem exercer os direitos previstos na LGPD, em especial os de se descadastrar, de opor ao tratamento e de solicitar o término da operação e a eliminação de seus dados pessoais?

Seção 2 - LGPD aplicada ao setor de Transportes

1. Determine a finalidade específica do tratamento de dados e justifique a necessidade desse tratamento para atingir tal finalidade.
2. Avalie se o interesse legítimo do controlador ou de terceiro prevalece sobre os direitos e liberdades dos titulares após o balanceamento.
3. Implemente medidas adicionais para proteger os dados pessoais e mitigar quaisquer riscos identificados.
4. Documente o processo de avaliação, incluindo o balanceamento e as medidas de proteção implementadas.
5. Revise regularmente a justificativa do legítimo interesse para garantir que ela continue sendo válida e apropriada.

Termo de Consentimento

O **Termo de Consentimento** é um documento que obtém a autorização explícita dos titulares para tratamento de dados pessoais para finalidades específicas (art. 8º, LGPD). Ele deve ser claro e informar todas as condições do tratamento para que o consentimento fornecido seja de e se refira a finalidades determinadas.

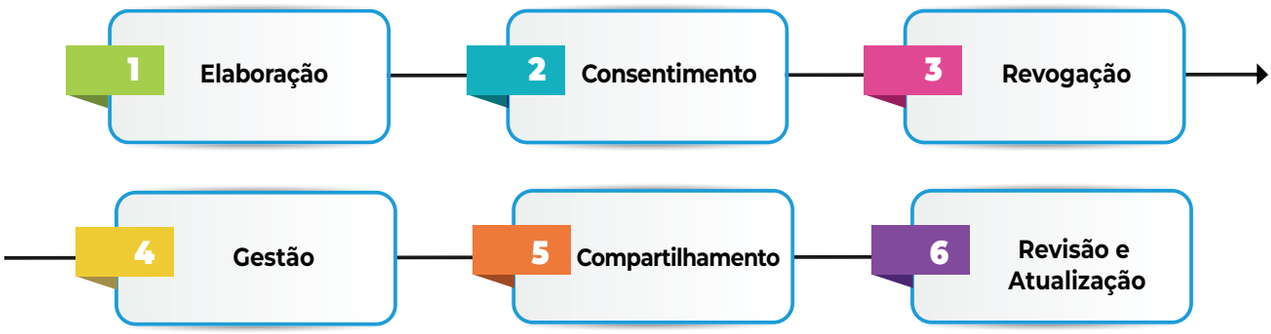
Quais são os principais elementos deste documento?

- Explicação detalhada das finalidades do tratamento de dados.
- Descrição dos tipos de dados pessoais que serão tratados.
- Informações sobre os direitos dos titulares e como eles podem ser exercidos.
- Explicação de como o titular pode revogar o consentimento.
- Informações de contato para o titular esclarecer dúvidas e exercer direitos.
- Forma adequada para registrar o consentimento inequívoco do titular (por exemplo, caixa de seleção para ser preenchida em formulários eletrônicos ou assinalada com “X” em formulários impressos).

Exemplo

Uma empresa de transporte rodoviário de carga poderá solicitar o consentimento dos colaboradores para uma campanha interna de diversidade envolvendo coleta de dados sensíveis relativos à orientação sexual, à raça, à etnia e à condição de saúde. O termo de consentimento deverá explicar claramente a finalidade, os dados coletados, os direitos dos colaboradores e como podem revogar seu consentimento, se desejarem. Se possível, recomenda-se que a empresa adote procedimentos de anonimização ou pseudonimização dos dados e documente os consentimentos obtidos, garantindo que os colaboradores consigam facilmente revogá-lo a qualquer momento. Ainda, para registrar o consentimento dos colaboradores sobre o tratamento dos dados, a empresa poderá usar um formulário eletrônico que conte com ferramentas como caixas de seleção (checkboxes), desde que elas não venham pré-preenchidas, para não invalidar a escolha livre do colaborador em dar o seu consentimento.

Seção 2 - LGPD aplicada ao setor de Transportes



1. Crie termos de consentimento claros e detalhados para cada finalidade específica de tratamento.
2. Garanta que o consentimento seja obtido de forma livre, informada e explícita. Utilize formulários ou interfaces digitais para facilitar o processo.
3. Inclua informações sobre como o titular pode revogar o consentimento a qualquer momento, e garanta que esse processo seja fácil e acessível.
4. Documente todos os consentimentos obtidos, incluindo a data, a finalidade e os dados coletados. Se houver mudanças da finalidade do tratamento de dados não compatíveis com o consentimento original, deve-se informar previamente o titular sobre tais mudanças e ele poderá revogar o consentimento, caso discorde delas.
5. Caso seja necessário comunicar e/ou compartilhar os dados com outros agentes de tratamento, deve-se obter consentimento específico do titular para essa finalidade, ressalvadas as hipóteses de dispensa previstas na LGPD.
6. Revise e atualize os termos de consentimento regularmente a fim de garantir que eles reflitam as práticas atuais de tratamento de dados e as exigências legais.

Checklist para elaboração dos documentos relevantes da LGPD

1) Registro das Operações de Tratamento de Dados Pessoais (ROT ou RoPA)

- ☐ Identificar e documentar todos os dados pessoais tratados.
- ☐ Descrever as finalidades do tratamento e as bases legais respectivas.
- ☐ Listar as medidas de segurança e o período de armazenamento.
- ☐ Registrar informações sobre o compartilhamento de dados.

2) Relatório de Impacto à Proteção de Dados (RIPD ou DPIA)

- ☐ Detalhar as operações de tratamento e os tipos de dados tratados.
- ☐ Avaliar os riscos e as consequências de uma violação de dados.
- ☐ Descrever as medidas de mitigação e a metodologia utilizada.
- ☐ Revisar e atualizar o relatório periodicamente, inclusive monitorando o nível de risco frente a novas circunstâncias de cada operação.

Seção 2 - LGPD aplicada ao setor de Transportes

Checklist para elaboração dos documentos relevantes da LGPD

3) Política de Privacidade

- ☐ Publicar uma política clara e acessível sobre o tratamento de dados pessoais.
- ☐ Usar técnicas de publicação que facilitem a leitura e a navegação pelo documento (como índices, informações em camadas, elementos visuais pertinentes).
- ☐ Incluir informações sobre os dados coletados, finalidades, compartilhamento e medidas de segurança adotadas.
- ☐ Explicar os direitos dos titulares e fornecer informações de contato.
- ☐ Manter o documento atualizado à luz das mudanças legais e práticas da empresa.

4)Teste de Balanceamento

- ☐ Realizar uma avaliação detalhada da finalidade, necessidade e balanceamento.
- ☐ Documentar as salvaguardas implementadas para proteger os dados.
- ☐ Revisar e justificar periodicamente o uso das bases legais de legítimo interesse e de prevenção à fraude e à segurança do titular nas respectivas atividades.

5) Termo de Consentimento

- ☐ Elaborar termos claros e detalhados para finalidades específicas.
- ☐ Incluir informações sobre finalidades, dados coletados, direitos dos titulares e revogação do consentimento.
- ☐ Garantir que o consentimento seja obtido de forma livre, informada e explícita.
- ☐ Facilitar o processo de revogação do consentimento pelos titulares.
- ☐ Estruturar procedimento de gestão do consentimento dos titulares, mantendo-o atualizado conforme as manifestações dos titulares.

Manter esses documentos atualizados e completos é muito importante para garantir a conformidade com a LGPD e uma prática essencial para qualquer programa de proteção de dados eficaz.

Seção 2 - LGPD aplicada ao setor de Transportes

4. DIREITOS DOS TITULARES

A LGPD concede, aos titulares de dados, diversos direitos que podem ser exercidos perante os controladores. Tais direitos estão previstos nos arts. 18 a 22 da LGPD e podem ser exercidos a qualquer momento, mediante a requisição expressa do titular dos dados ou representante legalmente constituído, sem custos. É possível subdividi-los conforme o seu contexto de aplicação.

Direitos aplicáveis em qualquer contexto

- **Confirmação da existência de tratamento (art. 18, I):** O titular pode solicitar a confirmação de que seus dados pessoais estão sendo tratados por determinada empresa.
- **Acesso aos dados (art. 18, II):** Confirmada a existência do tratamento de dados, o titular terá o direito de acessar os dados pessoais que são tratados por determinada empresa.
- **Correção dos dados (art. 18, III):** O titular pode solicitar a correção dos dados incompletos, incorretos e/ou desatualizados.
- **Informações sobre compartilhamento (art. 18, VII):** O titular pode solicitar informações sobre as entidades públicas e privadas com as quais a empresa realiza uso compartilhado de dados.
- **Portabilidade (art. 18, V e § 7º):** O titular pode solicitar a portabilidade dos seus dados para outro fornecedor de serviço ou produto, observados os segredos comercial e industrial. Essa portabilidade não inclui dados que já tenham sido anonimizados pelo controlador.

Direitos aplicáveis quando houver tratamento em desconformidade com a LGPD

- **Anonimização, bloqueio ou eliminação (art. 18, IV):** O titular pode solicitar a anonimização, bloqueio e eliminação de dados desnecessários, excessivos e/ou tratados em desconformidade com a LGPD.
- **Oposição (art. 18, § 2º):** O titular pode opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento à LGPD.

Seção 2 - LGPD aplicada ao setor de Transportes

Direitos aplicáveis quando a base legal for consentimento

- **Eliminação de dados (art. 18, VI):** O titular pode solicitar a eliminação de dados tratados com base no consentimento, exceto nas hipóteses de conservação dos dados após o término do seu tratamento previstas no art. 16 da LGPD, quais sejam: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida a anonimização dos dados; (iii) transferência a terceiro; ou (iv) uso exclusivo do controlador, vedado o acesso por terceiro, e desde que anonimizados os dados.

- **Possibilidade de não fornecer o consentimento (art. 18, VIII):** O titular deverá ser informado sobre a possibilidade de não fornecer consentimento e as consequências dessa negativa.

- **Revogação do consentimento (art. 8º, § 5º e art. 18, IX):** O titular tem o direito de revogar o consentimento a qualquer momento por meio de procedimento gratuito e simplificado. Caso isso ocorra, ficam ratificados eventuais tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 18, VI).

Direitos aplicáveis em face de decisões automatizadas

- **Revisão da decisão (art. 20, caput):** O titular tem o direito de solicitar revisão das decisões tomadas exclusivamente com base em tratamento automatizado de dados que afetem os seus interesses, como decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

- **Informações sobre os critérios da decisão (art. 20, § 1º):** O titular pode obter informações claras e adequadas sobre os critérios e procedimentos utilizados para as decisões automatizadas, sempre observado os segredos comercial e industrial.

Apesar de os direitos previstos na LGPD serem uma obrigação dos controladores de dados, é possível que os titulares encaminhem seus requerimentos para os operadores. Se isso ocorrer, e a empresa for uma operadora, é importante que a solicitação seja enviada, o quanto antes, para o respectivo controlador para dar encaminhamento ao pedido. Por isso, recomenda-se a inclusão de cláusulas contratuais específicas para cooperação em acordos entre controladores e operadores (C2P) para melhor atendimento dos direitos de titulares.

Dessa forma, os controladores têm a obrigação de garantir que os titulares consigam exercer os direitos da LGPD, implementando os procedimentos e os sistemas necessários

Seção 2 - LGPD aplicada ao setor de Transportes

para tanto. Quanto mais claros e fáceis esses procedimentos, maior a relação de confiança com os titulares e menor a quantidade de atritos e demandas administrativas e judiciais.

É importante que os requerimentos dos titulares sejam atendidos no menor tempo operacionalmente possível, observando os prazos legais aplicáveis, como o de 15 dias para a declaração completa dos dados (art. 19, II). Normalmente, as empresas direcionam os requerimentos de titulares para o contato do encarregado. O canal de comunicação pode ser exclusivo para questões de proteção de dados ou integrar a estrutura de outros canais de comunicação já existentes, como serviços de atendimento ao consumidor (SAC) e ouvidorias. Além disso, as empresas devem estar preparadas para receber solicitações de titulares estrangeiros (residentes ou não no Brasil), a quem a LGPD pode se aplicar.

Independentemente do canal de comunicação escolhido, é essencial definir o passo a passo interno para endereçar as solicitações dos titulares de dados.

1. O requerimento pode ser recebido por email, formulário, portal ou outro canal de comunicação disponível. É importante que todos os canais sejam monitorados para que seja possível cumprir os prazos legais de resposta.
2. Terceiros não devem acessar as informações de outro titular sem autorização. Por isso, é importante que o controlador confirme que a pessoa que está exercendo os direitos é o titular daqueles dados. A confirmação de identidade pode ser feita de várias formas: envio de documentos oficiais, duplo fator de autenticação, ligação telefônica, entre outros.
3. Nem sempre o titular será preciso no seu requerimento. Por isso, é importante que o controlador tenha uma equipe treinada para analisar os requerimentos recebidos e identificar qual é o direito da LGPD que o titular busca concretizar.
4. Para atender o requerimento, pode ser necessário realizar um levantamento interno de informações. Caso o direito seja de acesso a dados, deve-se identificar informações como a origem dos dados, os critérios utilizados e a finalidade do tratamento. Caso o direito seja a confirmação de existência do tratamento, deve-se identificar se há ou não registro de tratamento nos sistemas da empresa.
5. Após o levantamento de informações pertinentes, o controlador deve fornecer as informações solicitadas ou concretizar o pedido do titular, conforme aplicável. Quando o pedido for de confirmação de existência do tratamento ou acesso a dados, a resposta deve ser fornecida em formato simplificado, imediatamente, ou por meio de declaração completa, em até 15 dias (art. 19).
6. Caso o pedido seja de correção, eliminação, anonimização ou bloqueio dos dados, e for possível adotar as providências solicitadas, o controlador deverá, de maneira imediata, informar os agentes de tratamento com quem tenha realizado uso compartilhado dos dados para que eles repitam o procedimento idêntico, exceto se esta comunicação for comprovadamente impossível ou implicar em esforço desproporcional (art. 18, § 6º).

Seção 2 - LGPD aplicada ao setor de Transportes

A depender do pedido do titular, é possível que o seu direito encontre limitações, especialmente se a informação solicitada puder prejudicar a privacidade ou a proteção de dados de outros titulares, se a empresa não for o agente de tratamento dos dados ou se a informação for protegida por segredo comercial.

Quando isso ocorrer, a empresa deve responder o titular (i) comunicando que não é o agente de tratamento dos dados e indicar, sempre que possível, tal agente; ou (ii) indicar as razões de fato ou de direito que impedem a adoção da providência solicitada (art. 18, § 4º). Além disso, recomenda-se que a empresa mantenha registro detalhado da razão pela qual não pode fornecer as informações ou adotar a providência solicitada. Isso será útil se o titular questionar essa decisão ou se houver uma auditoria. Mesmo que não seja possível atender o requerimento, é recomendado que a empresa ofereça alternativas ao titular. Por exemplo, se as informações não puderem ser divulgadas na sua integralidade, confirme se há uma forma de fornecer um resumo ou uma versão reduzida das informações.

Em caso de não atendimento de uma requisição do titular e, ou caso a resposta não seja adequada, o titular pode recorrer à ANPD (por meio da petição de titular), aos órgãos de defesa do consumidor ou ao Poder Judiciário, para obter a satisfação da sua demanda.

E quando não houver um prazo para resposta previsto na LGPD?

As empresas devem ter uma estrutura interna, mecanismos e instrumentos para garantir o exercício dos direitos previstos na LGPD pelo titular de dados. Para fins operacionais, recomenda-se que o prazo de resposta aos pedidos seja sempre o menor possível, ainda que a LGPD indique um prazo apenas para confirmação de existência do tratamento ou acesso a dados pessoais. Nos demais casos, deve-se levar em consideração:

- A complexidade e a abrangência do pedido;
- A capacidade do controlador de cumprir a solicitação do titular (em alguns casos, não será possível, por exemplo, realizar a exclusão de alguns dados pessoais diante de uma obrigação legal ou regulatória vigente);
- Eventual justificativa de urgência do titular; e
- A legitimidade do titular em exercer o direito objeto do requerimento (o titular não pode solicitar a revogação do consentimento, por exemplo, se os seus dados pessoais são tratados para fins de execução de contrato).

Seção 2 - LGPD aplicada ao setor de Transportes

Para além dos direitos que podem ser exercidos mediante requerimentos do titular, a empresa deve ser proativamente transparente sobre algumas informações. Esse dever de informar o titular sobre o tratamento está previsto no art. 9° da LGPD.

A quais informações do tratamento o titular deve ter acesso facilitado?

Para atender o princípio do livre acesso, o titular deve ter acesso facilitado às informações sobre o tratamento, disponibilizadas de forma clara, adequada e ostensiva. Essas informações incluem:

- Finalidade específica do tratamento.
- Forma e duração do tratamento (observados os segredos comercial e industrial).
- Identificação do controlador e suas informações de contato.
- Informações sobre o uso compartilhado de dados pelo controlador e sua finalidade.
- Responsabilidades dos agentes de tratamento envolvidos na cadeia de tratamento.
- Menção explícita aos direitos dos titulares do art. 18, da LGPD (mencionados acima).

Normalmente, as informações costumam ser fornecidas pelas empresas por meio das políticas de privacidade em sítios eletrônicos, quando os titulares são agentes externos (clientes, usuários e candidatos de emprego), ou na forma de políticas na intranet, quando são agentes integrados à estrutura da empresa (colaboradores, prestadores de serviço e fornecedores).

LGPD e Lei de Acesso à Informação (LAI)

A Lei de Acesso à Informação (Lei n° 12.527/2011) e a LGPD estabelecem sistemas compatíveis de gestão e de proteção de dados, tratando-se de direitos complementares. A LGPD não afasta a publicidade e o acesso à informação nos termos da LAI, amparando-se nas bases legais do art. 7°, inc. II ou III, e art. 11, inc. II, alíneas “a” ou “b”, da LGPD. Por isso, as empresas devem cumprir com as obrigações da LAI e da LGPD quando ambas forem aplicáveis. Por exemplo, o procedimento de pedido de acesso à informação da LAI é diferente do procedimento de exercício de direito de titular da LGPD e ambos devem ser cumpridos nos termos de cada legislação.

Garantir maior clareza sobre o tratamento de dados ao titular é essencial, ainda que as informações não se limitem às previstas na LGPD. Por isso, quando possível, recomenda-se que as empresas avaliem se há outras informações relevantes que possam ser repassadas aos titulares sobre o tratamento dos seus dados, além daquelas do art. 9°.

Seção 2 - LGPD aplicada ao setor de Transportes

Quanto à forma, as informações fornecidas aos titulares devem ser claras, precisas, apresentadas em língua portuguesa e por meio de linguagem simples e acessível, evitando termos genéricos e ambíguos. Eventuais restrições fundamentadas na proteção do segredo comercial e/ou industrial devem ser justificadas e limitadas às informações indispensáveis para a sua manutenção.

Como garantir que as informações fornecidas aos titulares sejam claras e adequadas?

Um titular está navegando pelo site de uma empresa de transporte aquaviário a fim de adquirir passagens para suas próximas férias em cruzeiro. Intrigado com o pop-up que apareceu na sua tela sobre o tratamento de dados pessoais que a empresa realiza, ele acessa a Política de Privacidade da empresa, onde consta que são observados e coletados dados pessoais a partir do uso do site. A política informa que o histórico de navegação e buscas feitas no site são coletados para atender a finalidade de "melhorar a experiência do usuário", e que as informações são compartilhadas com parceiros para "fornecer conteúdos personalizados".

O titular não fica satisfeito com as informações e envia um requerimento à empresa solicitando informações mais precisas sobre a finalidade da coleta dos dados e o seu compartilhamento. Para atender o pedido, a empresa detalha de que forma, com quais dados e quais modalidades de tratamentos a experiência do titular poderá melhorar a partir do tratamento. Ainda, a empresa passa a especificar, com o detalhamento necessário, a finalidade do compartilhamento com parceiros. Por fim, a empresa atualiza a sua Política de Privacidade para que todos os titulares conheçam o tratamento, para evitar novos requerimentos individuais. Portanto, a observância do art. 9º da LGPD pode auxiliar as empresas a evitarem questionamentos e reclamações de titulares a respeito da falta de transparência sobre o tratamento, além de novos pedidos de informação.

Boas práticas de transparência

Para garantir maior transparência aos titulares quanto ao tratamento de dados, recomenda-se que as empresas adotem, no mínimo, os seguintes instrumentos:

- Disponibilização de Política de Privacidade para os titulares, no sítio eletrônico para clientes e em portais internos para colaboradores;
- Envio de Avisos de Privacidade para situações específicas, a exemplo da notificação acerca do compartilhamento de dados diante de operações societárias;
- Fornecimento de informações completas e detalhadas em pedidos de exercício de direitos do titular, observados o segredo industrial e comercial; e
- Sempre que possível, a fixação de Avisos de Privacidade em locais de fácil visibilidade.

Seção 2 - LGPD aplicada ao setor de Transportes

5. PRINCIPAIS ATIVIDADES DE TRATAMENTO DE DADOS NO SETOR DE TRANSPORTES

O setor de transportes realiza diversas atividades de tratamento de dados pessoais e de dados sensíveis no dia a dia, mas algumas são comuns entre os modais de transportes. Abaixo, seguem alguns exemplos de atividades de tratamento de dados conduzidas pelas empresas do setor de transporte.

Tratamento de dados de passageiros na prestação de serviços de transporte

- **Reservas de Bilhetes:** São coletados dados para processar a reserva do bilhete e a emissão da passagem, além de enviar comunicados aos passageiros sobre eventuais alterações.
- **Entretenimento a Bordo:** São coletados dados para personalização da experiência do usuário, melhoria do serviço e oferta de conteúdos relevantes (filmes e músicas). Os dados podem ser compartilhados com empresas parceiras de entretenimento.
- **Acesso ao Wi-Fi em Embarcações:** São coletados dados para oferecer o acesso à internet aos passageiros. Os dados podem ser compartilhados com os provedores de serviços de internet e empresas parceiras que oferecem conteúdo ou serviços através do Wi-Fi.
- **Programas de Fidelidade:** São coletados dados para oferecer benefícios e personalizar ofertas. Os dados podem ser compartilhados com empresas parceiras (como hotéis e locadoras de veículos).
- **Câmeras de Vigilância:** São coletados dados a fim de garantir a segurança dos passageiros, prevenir e investigar incidentes e cumprir obrigações legais e regulatórias. Os dados podem ser compartilhados com as autoridades policiais e de segurança, além das empresas parceiras responsáveis pela segurança de portos, aeroportos e estações ferroviárias e rodoviárias.
- **Procedimentos Migratórios:** São coletados dados para garantir a segurança dos passageiros, cumprir obrigações legais e regulatórias e realizar controle de fronteiras. Os dados podem ser compartilhados com autoridades governamentais responsáveis pela segurança e imigração.

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados de colaboradores na gestão de pessoas

- **Admissão de Pessoal:** São coletados dados durante o processo de análise de currículos para a seleção de novos colaboradores. Se a pessoa é selecionada, são coletados dados relacionados ao exame admissional, entre outros.
- **Obrigações Trabalhistas e Previdenciárias:** São coletados e compartilhados dados no eSocial, um sistema que centraliza informações fiscais, previdenciárias e trabalhistas das empresas.
- **Histórico do Colaborador:** São coletados dados para acompanhamento do desenvolvimento das atividades do colaborador. Eles podem ser usados em políticas afirmativas ou defesa em processos judiciais e administrativos.
- **Controles de Acesso e jornada de trabalho:** São coletados dados biométricos para controle de ponto, por meio de impressão digital ou reconhecimento facial. Também são utilizados meios menos invasivos, como folha de ponto escrita e crachá.
- **Exames Toxicológicos:** São coletados dados de saúde dos motoristas para fins de prevenção e preservação da vida, além do cumprimento de obrigações regulatórias. Esses dados podem ser compartilhados com laboratórios credenciados pelo Denatran, por exemplo.
- **Acompanhamento das Entregas:** São coletados dados de rastreamento do veículo conduzido pelos motoristas para garantir a segurança da carga e monitorar o progresso da sua entrega. Podem ser coletados inclusive dados registrados em sensores de fadiga. Esses dados podem ser compartilhados com o remetente e o destinatário da carga, com as gerenciadoras de risco e seguradoras, além de autoridades competentes, em caso de incidentes, por exemplo.
- **Benefícios e convênios:** são coletados dados pessoais para que os colaboradores usufruam de alguns benefícios e /ou convênios (médico, farmácia, academia, entre outros)

5.1 Tratamento de dados de passageiros para prestação de serviços de transporte

A prestação de serviços de transporte de passageiros exige o uso de dados pessoais a todo momento. Há várias situações em que dados pessoais de passageiros são utilizados para viabilizar o transporte, independentemente da modalidade no qual ele é realizado.

Seção 2 - LGPD aplicada ao setor de Transportes

- **Identificação:** Garantir que a pessoa que utiliza o transporte é a mesma que adquiriu o bilhete, inclusive de beneficiários de cartões de transporte, crianças e/ou adolescentes.

- **Pagamento:** Cobrança e pagamento do bilhete, feito pelo passageiro ou por um terceiro.

- **Segurança:** Garantir que a pessoa transportada é quem diz ser, inclusive com o uso de biometria e/ou reconhecimento facial, a fim de prevenir fraudes.

- **Melhorias:** Melhorar o atendimento por meio do envio de pesquisas de satisfação após a prestação dos serviços de transporte.

A identificação adequada do passageiro é necessária para formalização do contrato de transporte e exige o uso de dados pessoais. Além disso, dados pessoais utilizados para fins de cobrança, de passageiros ou outros terceiros, são imprescindíveis para execução do contrato. Em todos os casos, apenas os dados essenciais para a prestação segura do serviço de transporte devem ser coletados. Existem também situações nas quais as empresas precisam tratar dados pessoais de passageiros para atender obrigações regulatórias, como nos casos abaixo.

Norma	Obrigação Regulatória
Portaria nº 143 da Receita Federal do Brasil	Administradoras do local ou recinto alfandegado devem implementar sistema de monitoramento e vigilância, ininterruptos, nas dependências, com acesso remoto para fiscalização da Receita Federal do Brasil, dotado de câmeras que captam imagens com nitidez, inclusive à noite, nas áreas de movimentação de viajantes, veículos de cargas e armazenagem de bens e mercadorias, e pontos de acesso à entrada e saída autorizados e outras áreas definidas pela RFB de jurisdição do local ou recinto. Os dados devem ser armazenados por 180 dias.
Lei nº 16.758, do Estado de São Paulo (art. 1º)	No Estado de São Paulo, é obrigatório que todos os cadastros, os bancos de dados e registros de informações assemelhados, públicos e privados, tenham informações autodeclaradas sobre cor ou identificação racional.
Resolução nº 255/2012 da ANAC (art. 3º)	Empresas brasileiras e estrangeiras que exploram serviços de transporte aéreo público devem disponibilizar dados antecipados dos passageiros e tripulantes a bordo de suas aeronaves em voos internacionais com destino, origem, escala ou conexão em território brasileiro à ANAC.
Resolução nº 4308/2014 da ANTT (art. 10)	O controle de passageiros será realizado no embarque por meio da verificação entre as informações contidas nos documentos de identificação do passageiro. Constatada divergência, a falha deve ser sanada, sob pena de o passageiro ser impedido de embarcar.

Seção 2 - LGPD aplicada ao setor de Transportes

Os sistemas de venda de passagens também devem ser projetados para maximizar a funcionalidade com a coleta mínima de dados, isto é, aqueles estritamente necessários para a prestação dos serviços. Qualquer tratamento de dados para fins de melhoria do processo de venda, para fornecimento de serviços personalizados ou para programas de fidelidade deve ser claramente informado ao titular.

Procedimentos que envolvem o uso de dados pessoais comuns para a detecção e prevenção de fraudes devem ser precedidos de uma análise de risco e impacto à proteção dos dados. A transparência sobre o uso das informações para essa finalidade é essencial, e elas devem ser tratadas exclusivamente para tal propósito, exceto em situações permitidas por lei.

Para finalidades de realização de estatísticas, monitoramento do uso para melhoria do serviço e outras similares, deve-se utilizar, sempre que possível, dados anonimizados. Caso não seja possível, recomenda-se que se utilizem técnicas de pseudonimização e que o tratamento de dados ocorra em conformidade com a LGPD.

A utilização de dados sensíveis deve ocorrer somente nas situações em que seja indispensável ou em casos previstos por lei. Quando possível, deve-se evitar o tratamento de dados sensíveis, preferindo dados não sensíveis para alcançar a mesma finalidade. Devido à natureza dos dados sensíveis, as empresas devem priorizar sua proteção, pois incidentes com estes dados podem impactar significativamente os titulares. Portanto, recomenda-se a implementação de procedimentos reforçados de segurança, como restrição de acesso, pseudonimização, criptografia e outras medidas técnicas, além de precauções para evitar o compartilhamento não autorizado.

O tratamento de dados sensíveis deve ser precedido por uma análise de risco. Caso haja riscos relevantes, é recomendável a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD), descrevendo o tratamento de dados que pode gerar riscos aos titulares, junto com as medidas adotadas para mitigá-los. Quando o tratamento envolver situações de verificação ou autenticação biométrica, é altamente recomendado a empresa realize um Teste de Balanceamento específico para esta finalidade, que pode ou não estar integrado ao RIPD.

Seção 2 - LGPD aplicada ao setor de Transportes

Boas práticas para tratamento de dados sensíveis

Em relação aos dados pessoais sensíveis, as empresas devem observar algumas práticas:

- Tratar somente os dados que sejam estritamente necessárias e cujo tratamento fundamente-se em uma das bases legais do art. 11 da LGPD;
- Fornecer informações claras e detalhadas sobre o tratamento de dados ao titular, por meio, por exemplo, da Política de Privacidade da empresa;
- Redobrar o cuidado com segurança da informação, adotando medidas de segurança, técnicas e organizacionais adequadas, a exemplo de controle de acesso lógico e limitação do número de colaboradores que acessam a base de dados;
- Limitar o tratamento à finalidade original informada ao titular, abstendo-se de utilizar dados em outras circunstâncias ou para outras finalidades;
- Para tratamentos relacionados à verificação biométrica para prevenção à fraude e para segurança do titular, realizar um Teste de Balanceamento; e
- Caso o tratamento possa gerar riscos aos direitos fundamentais do titular, elaborar Relatório de Impacto à Proteção de Dados (RIPD) com a descrição do processo e medidas, salvaguardas e mecanismos de mitigação de risco.

A proteção dos dados de crianças e de adolescentes também deve ser especialmente rigorosa, considerando seu estágio de desenvolvimento cognitivo, social e intelectual. Este cuidado é fundamental para assegurar o seu melhor interesse, obtendo o consentimento de pais e/ou responsáveis sempre que necessário. O tra- tamento de dados de crianças deve ser realizado somente quando ele for absolutamente necessário para a prestação do serviço de transporte ou se exigido por lei. Os dados dos pais ou responsáveis legais, que fornecem e autorizam o uso dos dados das crianças, também devem ser tratados com máxima cautela.

Documentos exigidos por lei ou outras normas que contenham dados pessoais de crianças e de adolescentes devem ser utilizados somente para a finalidade prevista na regra. Ainda, devem receber proteção rigorosa e ser compartilhados apenas quando estritamente necessário, como por exemplo, para cumprir exigências legais ou regulatórias.

Seção 2 - LGPD aplicada ao setor de Transportes

Boas práticas para tratamento de crianças e adolescentes

Dados pessoais de crianças e adolescentes devem ser tratados pelas empresas somente quando forem realmente necessários para a prestação do serviço de transporte ou em razão de exigência legal e/ou regulatória, e sempre observar o seu melhor interesse. Toda documentação necessária pela exigência legal e/ou regulatória para a prestação do serviço de transporte de crianças ou de adolescentes que inclua seus dados pessoais deve ser utilizada unicamente para esta finalidade e disponibilizada às autoridades competentes, se necessário, devendo ser compartilhada somente em situações decorrentes da exigência legal e/ou regulatória. É indispensável que as empresas forneçam informações sobre o tratamento de tais dados, a exemplo dos tipos de dados coletados, a forma de utilização e os procedimentos para exercício de direitos, de maneira simples, clara e acessível, à luz das características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais, se adequado, para proporcionar a informação necessária aos pais/responsável legal e adequada ao entendimento da criança/adolescente.

Conforme entendimento consolidado no Enunciado CD/ANPD nº 1/2023, o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da LGPD. Especialmente nos casos em que a base legal for o legítimo interesse, será necessário elaborar um Teste de Balanceamento específico, delimitando as características do relacionamento do controlador com a criança ou adolescente e as medidas adotadas para garantir o seu melhor interesse, bem como mitigar riscos associados ao tratamento.

Tratamento de dados pessoais em cartões de transporte

Sistemas de bilhetagem eletrônica tratam diversos tipos de dados, incluindo dados sensíveis, como biometria, e dados de crianças, adolescentes e idosos. Tais sistemas podem também identificar os hábitos de deslocamento de usuários frequentes. Por isso, é essencial que todos esses processos estejam em conformidade com a LGPD.

Os sistemas de bilhetagem eletrônica funcionam como um cartão pré-pago, em que o usuário carrega determinado valor que é descontado à medida que utiliza os serviços de transporte. O melhor exemplo é o **Bilhete Único,** que é utilizado em diversas modalidades de transporte público. Durante a emissão, a recarga e utilização dos cartões, são coletados dados pessoais e financeiros. Em todo caso, sistemas de bilhetagem devem ser projetados para coletar apenas os dados essenciais para prestação do serviço.

Os dados de localização utilizados para controle de tráfego e fins estatísticos devem ser anonimizados e/ou pseudonimizados, sempre que possível. Ainda, o uso desses dados deve ser previamente comunicado aos titulares e incluído na Política de Privacidade. Além disso, o titular deve conhecer informações sobre as categorias de dados coletados, o tempo de

>>

Seção 2 - LGPD aplicada ao setor de Transportes

duração do tratamento, o prazo de retenção, a base legal, e a finalidade do tratamento.

As empresas devem garantir que todos os fornecedores envolvidos no sistema de bilhetagem estejam em conformidade com a LGPD. Instruções claras sobre o tratamento de dados pessoais devem ser fornecidas, assegurando que os dados não sejam usados para outras finalidades e/ou compartilhados sem autorização, (quando for necessário). Caso a recarga do cartão exija coleta de dados adicionais, os titulares devem ser informados sobre essa necessidade e os meios para exercer os seus direitos previstos na LGPD.

Políticas de descontos e isenções de tarifas podem requerer o tratamento de dados pessoais para autenticar usuários beneficiados e prevenir fraudes. É fundamental seguir o princípio da minimização e garantir a transparência no tratamento dos dados, observando as disposições específicas da LGPD para dados sensíveis e categorias especiais de titulares.

1. Quem são os titulares de dados?

São os usuários dos serviços de transporte, inclusive crianças ou adolescentes. Nessa hipótese, é indispensável a observância do art. 14 da LGPD, especialmente no que se refere à realização do tratamento de dados no seu melhor interesse, observando-se a necessidade de transparência e a observância das regras do consentimento ou assistência de pais ou responsáveis. É possível que idosos tenham um cartão de transporte específico. Nessas situações, costumam ser solicitadas informações para elegibilidade a benefícios e autenticação (biometria, por exemplo). Quanto às pessoas com necessidades especiais, o seu cadastramento contempla a coleta de dados básicos de identificação e de dados sensíveis, que devem ser tratados com procedimentos específicos. Quanto às outras gratuidades, a depender das especificidades definidas em lei para cada sistema de transporte, é possível que existam outras categorias de usuários do sistema de transporte enquanto titulares de dados.

2. Qual a finalidade do tratamento?

Os dados costumam ser tratados para emissão e recarga do cartão de transporte (tanto cartões de gratuidade quanto cartões de comercialização) para utilização do serviço de transporte.

3. Quem são os agentes de tratamento?

A depender do caso concreto, as prestadoras de serviços de transporte podem ser controladoras ou operadoras. Isso porque, em alguns casos, o controle é realizado pelo Governo ou Município e as prestadoras de serviços de transporte realizam o tratamento apenas para operacionalizar e viabilizar o uso da bilhetagem eletrônica, como ocorre no caso dos contemplados com benefícios tarifários específicos.

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados pessoais para emissão e recarga de cartões de transporte

4. Qual a base legal para o tratamento?

Quando as prestadoras de serviço de transporte atuam como controlador, podem fundamentar o tratamento de dados na execução de contrato ou no cumprimento de obrigações legais ou regulatórias, a depender do caso. Quando atuam como operadores, não cabe a elas definir uma base legal para o tratamento.

5. Quais cuidados devem ser adotados?

É importante que os dados coletados para a emissão e a recarga do cartão sejam apenas aqueles necessários para alcançar tal finalidade, sob pena da coleta estar excedendo o necessário.

A proteção dos dados em sistemas de bilhetagem eletrônica deve ser priorizada, garantindo transparência, segurança e uso restrito às finalidades declaradas. As empresas de transporte devem implementar políticas robustas para assegurar a proteção dos dados dos passageiros em todas as etapas do processo de bilhetagem eletrônica.

Tratamento de dados biométricos, imagem e reconhecimento facial

No setor de transporte, o uso de dados biométricos para a validação de identidade tem se tornado prática comum, visando aumentar a eficiência e efetividade operacional em políticas de controle de acesso, de prevenção a fraudes e segurança. No entanto, isso exige precauções rigorosas para garantir a legitimidade do tratamento. Isso porque, dependendo de como esses dados são tratados, eles podem conferir, aos controladores, uma capacidade significativa de monitoramento das atividades dos titulares. Por isso, seu uso deve ser feito de forma proporcional, adequada e transparente.

Os dados biométricos são identificados como dados sensíveis pelo art. 5º, inc. II, da LGPD, exigindo que o seu tratamento seja baseado em uma das bases legais do art. 11. Embora a LGPD não forneça uma definição explícita de dados biométricos, entende-se que a biometria inclui mais do que apenas impressões digitais e imagens faciais. Também pode incluir dados extraídos da retina ou da íris dos olhos, voz, DNA, padrão das veias e até a forma de andar. A tabela abaixo sintetiza exemplos de técnicas de identificação biométrica física, fisiológica e comportamental.

Seção 2 - LGPD aplicada ao setor de Transportes

Tipo de Biometria	Exemplo
Técnicas de identificação biométrica física ou fisiológica	• Reconhecimento facial • Verificação de impressão digital • Varredura da íris • Análise da retina • Reconhecimento de voz • Reconhecimento de formato de orelha
Técnicas de identificação biométrica comportamental	• Análise de pressionamento de tecla • Análise de assinaturas manuscritas • Análise de marcha • Análise do olhar (rastreamento ocular)

Uma das principais características dos dados biométricos é a sua ligação única com indivíduos específicos, o que aumenta o seu potencial de identificação precisa. Em muitos casos, esses dados não só tornam uma pessoa identificável, mas a identificam diretamente, sem a necessidade de cruzamento com outros tipos de dados. Diferentemente dos sistemas que utilizam identificadores externos (como números de identidade), os dados biométricos refletem características físicas inatas e imutáveis da pessoa, exigindo tratamento cauteloso.

Por exemplo, enquanto uma senha de cartão de crédito pode ser alterada em casos de fraude, a íris ou impressão digital de alguém não podem ser modificadas. É importante notar que, embora algumas características biométricas (como o modo de andar) não sejam exclusivas, elas podem ser usadas para excluir pessoas de um processo de classificação e, quando combinadas com outros dados, levar à identificação de um indivíduo.

Ainda, a consideração de um dado como biométrico pode depender do contexto de seu tratamento, e não apenas das características do dado em si. O Conselho Europeu de Proteção de Dados (European Data Protection Board - EDPB) entende que imagens de vídeo de uma pessoa não são automaticamente consideradas dados biométricos, a menos que o processamento técnico dessas imagens tenha sido especificamente projetado para produzir a identificação do indivíduo.[21] Assim, a definição prática de dado biométrico inclui tanto o processamento técnico específico quanto a intenção em identificar uma pessoa específica.

Esse entendimento é refletido no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, no Considerando 51, que esclarece que o tratamento de fotografias não

Seção 2 - LGPD aplicada ao setor de Transportes

deve ser sistematicamente considerado como tratamento de categorias especiais de dados (dados sensíveis da LGPD). As fotografias são incluídas na definição de dados biométricos somente quando processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa. Esse entendimento é reforçado pela ANPD, que reconhece que a foto da face do cidadão deve ser entendida como dado biométrico se passar por um sistema de reconhecimento automatizado que viabilize a sua identificação.[22]

Para cada atividade de tratamento de dados biométricos, independentemente da finalidade, recomenda-se que as empresas elaborem o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), para avaliar os riscos associados ao tratamento. Essa avaliação é especialmente importante para tratamentos em larga escala, que podem afetar um número significativo de titulares de dados, e deve incluir medidas, garantias e procedimentos para mitigar riscos, assegurar a proteção dos dados e comprovar a conformidade com a LGPD.

O uso de autenticação biométrica baseada em amostras biológicas, como a saliva e o sangue, deve ser evitado. Além disso, as empresas devem justificar a escolha do método biométrico, como verificação de íris, impressão digital, rede venosa da mão ou formato da face, em vez de métodos menos invasivos. Para controle de acesso, deve-se questionar se a proteção desejada realmente demanda a coleta de dados biométricos e se o mesmo nível de segurança não pode ser alcançado com a coleta de dados não sensíveis.

Atenção!

A instalação de câmeras na cabine do veículo de transporte rodoviário de cargas

A utilização de câmeras na cabine do veículo de transporte rodoviário de cargas, especialmente para aquelas de maior risco ou valor, e a utilização das filmagens assim obtidas pode ser muito importante para a proteção do motorista e a segurança da operação, de terceiros e da carga. No entanto, para que esta prática seja legítima, alguns requisitos devem ser observados:

- As empresas devem utilizar as filmagens apenas para finalidade específica de monitoramento do trabalho, para fins de segurança, controle de fadiga e sono do motorista e relacionados diretamente à segurança;
- Recomenda-se que as empresas limitem a filmagem do interior da cabine do motorista ao período da jornada de trabalho (por exemplo, com implementação de sistemas que desligue a câmera se o motorista desligar a ignição do veículo) para preservar a intimidade do motorista e limitar o monitoramento ao horário de trabalho;
- Recomenda-se que as empresas limitem o tempo de armazenamento das filmagens ao tempo estritamente necessário para que as demandas de segurança sejam atendidas, observando os eventuais prazos legais ou regulatórios aplicáveis; e
- As empresas devem fornecer informações claras e detalhadas sobre o tratamento dos dados por meio das filmagens, que pode ser feito a partir da Política de Privacidade da empresa, por avisos específicos afixados no interior do veículo e/ou pelo envio de informações ao motorista por meio de documento com as informações relevantes.

Seção 2 - LGPD aplicada ao setor de Transportes

Quando o tratamento de dados biométricos for necessário para a prestação de um serviço de transporte, como recarga na bilhetagem eletrônica, o titular deve ser informado claramente e de forma destacada, em linguagem simples, sobre tal necessidade e os meios para exercer os direitos previstos na LGPD (art. 9°, § 3°). As políticas de privacidade devem especificar claramente os motivos da coleta e tratamento de dados biométricos, medidas de segurança adotadas e as hipóteses de eliminação dos dados.

A tabela abaixo contém informações relevantes para a conformidade do tratamento à LGPD, quando tratados dados biométricos de usuários dos serviços de transporte para a garantia da prevenção à fraude e à segurança do titular no uso de cartões de transporte.

Tratamento de dados biométricos para garantia de prevenção à fraude e à segurança

1. Quem são os titulares de dados?

São os usuários dos serviços de transporte, normalmente de categorias especiais. Nos casos de passe estudantil, o titular de dados será menor de idade, ou seja, criança ou adolescente. Nessa hipótese, deve-se observar o art. 14 da LGPD, para realizar o tratamento no seu melhor interesse.

2. Qual a finalidade do tratamento?

Identificar os usuários e impedir fraudes no uso dos cartões de transporte, coibir o uso indevido por quem não é titular do cartão e/ou não faz jus ao benefício de uma modalidade específica da bilhetagem eletrônica (estudante, idoso, passe livre para estudantes de escolas públicas, etc.).

3. Quem são os agentes de tratamento?

Comumente, são as prestadoras de serviços de transporte e o poder concedente.

4. Qual a base legal para o tratamento?

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. Ainda, é importante que os agentes de tratamento verifiquem se não há alguma obrigação legal ou regulatória vinculada ao tratamento de dados biométricos para prevenção à fraude no caso concreto.

5. Quais cuidados devem ser adotados?

Os titulares devem ser informados sobre o tratamento ao qual estão sujeitos, especialmente em relação à verificação de identidade em casos de benefícios. Recomenda-se que as câmeras usadas para coleta dos dados biométricos estejam próximas a avisos específicos sobre essa tecnologia.

Seção 2 - LGPD aplicada ao setor de Transportes

É crucial que as empresas adotem medidas especiais de proteção, como criptografia e controle de acesso físico e lógico às bases de dados. O tratamento de dados biométricos deve ser ponderado à luz (i) dos princípios da necessidade, da adequação e da finalidade, (ii) da sensibilidade dos dados, (iii) do volume necessário e (iv) do potencial dano em caso de incidentes de segurança.

Boas práticas para tratamento de dados biométricos

Para tratar dados biométricos, as empresas devem considerar alguns aspectos relevantes:

- A coleta de dados biométricos para controle de acesso deve ser realizada se for estritamente necessária. Se possível, deve-se optar por outros sistemas de identificação, como senhas.
- Recomenda- se a realização de um Teste de Balanceamento para verificar se, no caso concreto, não devem prevalecer os direitos e as liberdades fundamentais dos titulares, nos moldes divulgados pela ANPD. Também é recomendada a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para cada atividade de tratamento, com a descrição do processo e de medidas, salvaguardas e mecanismos de mitigação de risco.
- Empresas devem conferir especial atenção à transparência, assegurando que todas as políticas internas e externas indiquem expressamente os motivos da coleta, e disponibilizando, quando possível, mecanismos adicionais de transparência, como uma aba específica de FAQ no site.
- Em razão da sensibilidade de dados biométricos, devem ser adotadas medidas especiais para sua proteção, como criptografia e controle de acesso físico e lógico às bases de dados.

Tratamento de dados para fins de marketing

As atividades de publicidade que fazem uso de dados pessoais, como o marketing direto para envio de publicidade segmentada, pesquisas de mercado e outras ações, para promover e ofertar produtos ou serviços, devem seguir os parâmetros da LGPD.

O marketing busca conectar o mercado aos consumidores, fortalecendo as relações econômicas, o que se alinha aos fundamentos da LGPD de desenvolvimento econômico e livre iniciativa. Assim, o tratamento de dados pessoais deve ocorrer dentro de um contexto de legitimidade, respeitando os direitos e garantias dos titulares e adotando medidas para promover a transparência.

É recomendável que as comunicações de marketing possuam um mecanismo que permita, ao destinatário, retirar o consentimento dado para recebimento da comunicação, caso essa seja a base legal utilizada. Alternativamente, deve-se oferecer a opção de não receber futuras comunicações

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados para fins de marketing

quando outra base legal estiver em uso. Em ambos os casos, o mecanismo deve proporcionar a interrupção das comunicações de maneira fácil e eficaz.

É essencial assegurar a ampla divulgação e a transparência no tratamento de dados, utilizando instrumentos adequados e de fácil visualização, como avisos de cookies, avisos de privacidade destacados em sites e aplicativos, e a inclusão das informações necessárias nos diversos meios de contato e comunicação com os titulares.

Nos processos de marketing, como nas outras atividades de tratamentos, devem ser utilizados apenas os dados estritamente necessários, inclusive na caracterização do público em pesquisas de mercado. Para concretizar o princípio da necessidade, recomenda-se que a base de dados utilizada para marketing não seja integrada à base de dados cadastrais ou outras bases da empresa. Contudo, se a integração for pertinente, seja por interesses da empresa, dos titulares ou de terceiros, recomenda-se realizar um Teste de Balanceamento ou o Relatório de Impacto à Proteção de Dados para mitigar riscos, especialmente quando informações de marketing são integradas a dados identificáveis dos titulares.

No compartilhamento de dados com parceiros, como agências de publicidade para atividades de marketing digital, mídia programática, campanhas, pesquisas e elaboração de materiais, é necessário garantir que esses parceiros estejam em conformidade com a LGPD. Em geral, essa garantia é estabelecida por meio de ajustes nos contratos firmados, que devem prever responsabilidades de cada parte, padrões de conduta e procedimentos a serem adotados, especialmente em caso de incidentes de segurança.

Em atividades de endomarketing e marketing institucional que envolvem o uso de imagens ou voz de colaboradores, dependentes e clientes, recomenda-se que seja coletado o consentimento específico para o uso e compartilhamento desses dados. Quando se trata de dados de crianças e adolescentes em campanhas específicas, deve-se obter a autorização destacada de pelo menos um dos pais ou responsável legal, sempre observando o melhor interesse da criança. Caso as imagens ou vozes dos colaboradores sejam utilizadas para iniciativas de divulgação externa e com cunho comercial, deve ser celebrado um termo de licença de uso de voz e imagem com o colaborador, seguindo o disposto no art. 20, CC.

Seção 2 - LGPD aplicada ao setor de Transportes

5.2 Tratamento de dados na gestão de pessoas

Os colaboradores de uma empresa são uma categoria altamente relevante de titulares de dados, devido à natureza dos dados que são tratados durante a relação de trabalho.

Desde a fase pré-contratual até o momento após a rescisão do contrato de trabalho, o empregador atua enquanto controlador dos dados pessoais dos empregados, tomando decisões sobre o tratamento desses dados. Exemplos de dados pessoais tratados incluem: documentação de identificação, imagens capturadas no ambiente de trabalho, registros de videoconferências e registros biométricos de jornada de trabalho.

Dado o desequilíbrio de poder nas relações de trabalho, entende-se que os colaboradores raramente fornecem um consentimento verdadeiramente livre para o tratamento de seus dados. No entanto, existem situações excepcionais em que os colaboradores podem oferecer seu consentimento de forma livre, especialmente quando a concessão ou a recusa do consentimento não resultar em consequências negativas para eles. Nesses casos, é essencial garantir que os elementos necessários para essa liberdade estejam presentes e sejam demonstráveis.

Ademais, tratando-se de relações trabalhistas existem muitos casos em que as empresas são obrigadas a tratar dados pessoais de colaboradores para atender obrigações regulatórias, como nos casos abaixo.

Norma	Obrigação Regulatória
Decreto nº 10.854/2021 (art. 112)	O empregador é obrigado a fornecer o benefício de vale-transporte aos empregados. Para tanto, precisa coletar o endereço residencial do empregado e informações sobre serviços e meios de transporte mais adequados ao seu deslocamento residência-trabalho.
Decreto nº 11.795/2023 (art. 2º)	O empregador é obrigado a elaborar um Relatório de Transparência Salarial e de Critérios Remuneratórios. Para isso, trata alguns dados pessoais, que devem ser anonimizados e enviados pela ferramenta disponibilizada pelo Ministério do Trabalho e Emprego.
Lei nº 8.036/1990 (art. 17-A)	O empregador é obrigado a declarar dados relacionados aos valores do FGTS e outras informações de interesse do Poder Público pelo sistema de escrituração digital, na forma, no prazo e nas condições estabelecidas pelo Ministério do Trabalho e Previdência. A obrigação cria um dever do empregador de compartilhar dados relacionados ao FGTS de seus empregados.

Seção 2 - LGPD aplicada ao setor de Transportes

Resolução do Comitê Gestor do eSocial nº 1 (art. 1º)	O empregado é obrigado a preencher o eSocial em seus campos sobre os dados do empregador. A Resolução cita especificamente os dados cadastrais dos empregadores, inclusive domésticos, da empresa e a eles equiparados em legislação específica e dos segurados especiais; dados cadastrais e contratuais, incluídos os relacionados ao registro de empregados; dados cadastrais dos dependentes dos empregados, inclusive domésticos, dos trabalhadores avulsos e dos segurados dos regimes geral e próprios de previdência social; entre outros. Desde agosto de 2024, os empregadores também são obrigados a transmitir informações ao eSocial sobre os exames toxicológicos dos motoristas profissionais empregados (Portaria MTE nº 612/2024).

Em algumas situações, a empresa pode decidir terceirizar atividades que envolvem o tratamento de dados de empregados, como a gestão de folha de pagamento ou processos de recursos humanos. Nesses casos, é fundamental garantir que as regras de privacidade e proteção de dados sejam rigorosamente observadas por todos os envolvidos, seguindo as recomendações descritas na seção 7.3 deste Guia.

Implementar políticas e práticas adequadas são ferramentas úteis para a garantia de conformidade à LGPD. Além de assegurar a conformidade com a LGPD, promovem um ambiente de confiança e segurança. Dessas políticas, destacam-se os seguintes documentos essenciais que desempenham um papel fundamental nesse processo.

Política de Privacidade para Colaboradores
A Política de Privacidade para Colaboradores é o documento que define como a empresa coleta, usa, armazena e protege os dados pessoais dos seus colaboradores. Ela deve incluir informações sobre os tipos de dados coletados, as finalidades do tratamento, os direitos dos empregados em relação aos seus dados, e as medidas de segurança implementadas para proteger esses dados. A transparência e comunicação clara são fundamentais para assegurar que os empregados estejam cientes de como seus dados são gerenciados e protegidos.

Seção 2 - LGPD aplicada ao setor de Transportes

Política de Tratamento de Dados para Colaboradores

Esta política fornece diretrizes detalhadas sobre as melhores práticas que os empregados sobre a coleta, armazenamento, acesso e compartilhamento de dados pessoais, enfatizando a importância da conformidade com a LGPD. A política deve abordar procedimentos para relatar incidentes de segurança e violações de dados, promovendo uma cultura de responsabilidade e conscientização sobre a proteção de dados dentro da organização.

Cláusulas Contratuais de Proteção de Dados em Contratos de Trabalho

Incorporar cláusulas específicas de proteção de dados nos contratos de trabalho é uma prática importante para assegurar a conformidade legal e proteger interesses da empresa e empregados. Essas cláusulas devem esclarecer as responsabilidades do empregado em relação ao tratamento de dados pessoais, bem como os direitos do empregado sobre seus próprios dados. Elas também devem incluir disposições sobre confidencialidade, medidas de segurança, e as consequências de violações das políticas internas de proteção de dados.

Cada um desses documentos tem uma função específica na proteção e na gestão adequada dos dados pessoais dos empregados. Ao estabelecer diretrizes claras e robustas, a empresa reforça seu compromisso com a privacidade e segurança dos dados, protegendo os direitos dos empregados e a integridade da organização. Abaixo, serão apresentadas as boas práticas de proteção de dados recomendáveis para cada etapa da relação de trabalho.

Fase 1 - Pré Contrato

Durante a fase pré-contratual, é necessário informar claramente os candidatos sobre a coleta e o uso de seus dados pessoais. Isso inclui especificar a finalidade do tratamento e obter consentimento, quando apropriado. Durante processos seletivos e de recrutamento, é essencial limitar a coleta de dados àqueles estritamente necessários à seleção, solicitando a menor quantidade possível de dados, com cautela para informações do passado.

Seção 2 - LGPD aplicada ao setor de Transportes

Atenção!

O tratamento de dados pessoais obtidos por meio de gerenciadoras de risco

- **Contratação de Autônomos**

O art. 13-A da Lei nº 11.442/2007 veda expressamente a utilização de informações de bancos de dados de proteção ao crédito como mecanismo de vedação de contrato com o Transportador Autônomo de Cargas (TAC) e Empresa de Transporte Rodoviário de Cargas (ETC) devidamente regulares para exercício da atividade de transporte rodoviário de cargas. Diante disso, orienta-se que as empresas se abstenham de contratar ou utilizar, ainda que de forma esporádica, qualquer gerenciadora de riscos que use, em seu banco de dados, dados relativos a restrições de crédito.

- **Contratação de Empregados**

As empresas devem, ao longo do processo seletivo, utilizar apenas as informações estritamente necessárias à seleção dos candidatos, evitando coletar dados sensíveis sempre que possível, e abstenham-se de usar quaisquer informações do candidato de forma ilícita, inadequada, abusiva ou discriminatória (por exemplo, utilizar informações de crédito para calcular eventual risco à segurança da carga transportada, que é proibido por lei e pela jurisprudência trabalhista).

- **Cuidados na relação contratual com a Gerenciadora de Risco**

Caso as empresas contratem gerenciadoras de risco, devem adotar as seguintes boas práticas:

  - Assinar um acordo de compartilhamento de dados específico, em que conste a definição clara dos papeis de cada agente de tratamento envolvido (controlador, operador ou suboperador) e as obrigações e responsabilidades de cada agente;

  - Realizar uma diligência prévia e contínua das gerenciadoras de risco, a partir de critérios de seleção à luz das exigências da própria LGPD quanto a medidas e mecanismos de proteção de dados e segurança da informação; e

  - Garantir que as gerenciadoras de risco, caso usem sistemas automatizados de verificação de risco, consigam proporcionar, ao titular, o direito de solicitar a revisão das decisões finais de análise de perfil de risco caso a empresa seja questionada, bem como de fornecer os critérios principais utilizados pelo seu sistema conforme previsto no art. 20 da LGPD.

Para armazenar currículos de candidatos não selecionados, preferencialmente, deve ser obtido o consentimento, especificando o período de retenção do currículo. Com relação aos dados sensíveis, como informações sobre condições de saúde, o consentimento deve ser utilizado como base legal para a coleta e armazenamento, como regra, resguardadas as obrigações legais e regulatórias que possam se aplicar.

Se um candidato se opuser ao tratamento de dados, as empresas devem descartar os dados obtidos com consentimento de forma segura, gerando evidências que comprovem

Seção 2 - LGPD aplicada ao setor de Transportes

a eliminação através de procedimentos técnicos apropriados. Para dados pessoais que não foram obtidos por consentimento, a retenção é permitida enquanto houver uma finalidade específica e uma base legal que a justifique.

Qualquer anotação feita durante entrevistas de seleção e de recrutamento deve ser descartada imediatamente após o encerramento do processo seletivo, a menos que exista alguma razão legal específica para a sua retenção. Nesse sentido, o fluxo abaixo ilustra o tratamento de dados pessoais que toda empresa comumente realiza na fase pré-contratual.

Boas práticas para tratamento de dados durante processos seletivos

Ao realizar processos seletivos para contratação de novos colaboradores, as empresas devem:

- Coletar apenas as informações que sejam estritamente necessárias à seleção dos candidatos, evitando coletar dados sensíveis e somente utilizá-los se devidamente fundamentado;
- Quando a coleta de dados sensíveis for necessária, fornecer informações claras e detalhadas sobre o tratamento ao titular, por exemplo, na Política de Privacidade e em outros momentos quando houver interação com o titular;
- Abster-se de utilizar dados do candidato de forma discriminatória, inadequada, abusiva ou ilícita durante o processo seletivo;
- Limitar a coleta de certidões de candidatos (a exemplo da certidão de antecedentes criminais) para quando for necessário, para que seja utilizado estritamente quando houver previsão em lei, em virtude da natureza do ofício ou do grau especial de fidúcia exigido, de acordo com o entendimento consolidado do Tribunal Superior do Trabalho (TST); e
- Após o processo seletivo, quanto aos candidatos não selecionados, armazenar as informações apenas pelo prazo prescricional que se faça necessário e utilizá-los somente para a finalidade estritamente relacionada ao respectivo prazo prescricional; e
- Se houver intenção de armazenar o currículo do candidato não selecionado em um banco de dados da empresa, obter o devido consentimento do titular.

Somado a isso, há que se considerar ainda dois aspectos adicionais:

- Caso a filtragem e seleção de currículos seja feita com base em ferramentas automatizadas, a empresa deve fornecer, ao titular, informações sobre os critérios utilizados para esta filtragem e seleção, e lhe garantir o direito de solicitar a revisão da decisão final (art. 20 da LGPD); e
- Recomenda-se que as empresas evitem a utilização da base legal do consentimento, tendo em vista que a assimetria de poder entre o candidato/colaborador e a empresa pode gerar questionamentos sobre a liberdade de escolha do titular e inviabilizar a caracterização do consentimento livre.

Seção 2 - LGPD aplicada ao setor de Transportes

Fase 2 - Execução do contrato de trabalho

Para formalizar o contrato de trabalho, é necessário coletar diversos dados pessoais e dados sensíveis do colaborador, como cópias de documentos de identificação, imagens e vídeos capturados no ambiente de trabalho e em videoconferências, registro biométrico da jornada de trabalho, entre outros.

As empresas devem tomar as precauções necessárias para evitar a coleta excessiva de dados e garantir que o colaborador entenda claramente a finalidade de cada informação coletada e informá-lo sobre possíveis compartilhamentos que possam ser necessários em virtude de obrigações legais ou regulatórias.

É essencial que as empresas informem suas políticas de tratamento de dados para os colaboradores, incluindo a finalidade e a base legal para a coleta de dados. Sempre que possível, deve-se solicitar que o colaborador assine um termo de compromisso, por meio do qual confirma que está ciente dessas políticas.

A manutenção do contrato de trabalho exige também atualizações periódicas dos dados pessoais do colaborador, que incluem o seu histórico dentro da empresa, atestados médicos, licenças e registros de processos disciplinares internos. Dada a sensibilidade e a confidencialidade dos dados, é fundamental que o seu acesso seja estritamente limitado às pessoas autorizadas.

Tratamento de dados para concessão do benefício de vale-transporte aos colaboradores

1. Quem são os titulares de dados?

São os colaboradores das prestadoras de serviços de transporte.

2. Qual a finalidade do tratamento?

Concessão mensal do benefício de vale-transporte ao colaborador celetista.

3. Qual a base legal aplicável?

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.

- Nos casos de concessão do benefício sem uso de dados sensíveis: Art. 7º, VI, IX, da LGPD.
- Nos casos de gratuidade: Art. 11, II, “a”, da LGPD.

Seção 2 - LGPD aplicada ao setor de Transportes

Ainda, deve-se informar o colaborador de todo o processo de tratamento de dados e garantir meios que ele possa exercer seus direitos. Além disso, para assegurar a proteção de dados, a empresa deve implementar políticas claras e fornecer treinamento regular aos colaboradores. As políticas devem cobrir aspectos como segurança da informação (medidas para proteger os dados contra acessos não autorizados), gerenciamento de consentimento (procedimentos para obter e registrar o consentimento, quando aplicável) e auditorias e revisões (realização de auditorias periódicas para garantir conformidade com normas de proteção de dados).

Com o aumento do trabalho remoto, é fundamental adotar medidas adicionais para proteger os dados pessoais dos empregados. Isso inclui medidas para segurança de rede (uso de redes seguras e criptografia para proteger os dados transmitidos) e políticas para o trabalho remoto (diretrizes claras sobre o uso de dispositivos pessoais e corporativos, bem como a segurança das informações).

A coleta e o tratamento de dados pessoais para a formalização e a manutenção de contratos de trabalho devem ser conduzidos com extremo cuidado. As empresas devem garantir a transparência na coleta de dados, proteger a confidencialidade e a segurança das informações, e manter os dados atualizados.

No contexto corporativo, o uso de dados biométricos de colaboradores tornou-se uma prática comum para melhorar a eficiência e a segurança. Especificamente, a coleta e o tratamento desses dados são fundamentais para o registro preciso da jornada de trabalho e o controle de acesso às instalações físicas. Nesses casos, as empresas devem demonstrar a necessidade do tratamento, explicando as razões específicas para preferir essa abordagem em vez de outros sistemas de identificação, como senhas ou medidas organizacionais de segurança. É recomendável restringir a coleta de dados biométricos ao controle de acesso a áreas de tráfego restrito e a dispositivos e aplicativos computacionais de acesso limitado. Também neste caso, será necessário realizar um Teste de Balanceamento para respaldar o uso da base legal da prevenção à fraude e segurança do titular (art. 11, II, “g”, LGPD), seguindo as recomendações da ANPD.

Exemplo

O prédio de uma companhia aérea possui um sistema eletrônico de digitalização de impressões digitais. Seguranças escaneiam impressões digitais dos colaboradores para que eles possam passar pelas catracas de entrada nas áreas restritas do prédio. O sistema processa dados biométricos para identificar os colaboradores e confirmar se eles têm autorização para acesso às áreas restritas. Portanto, a empresa de transporte deve observar as disposições da LGPD no tratamento desses dados.

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados biométricos para registro eletrônico de ponto

1. Quem são os titulares de dados?

São os colaboradores das prestadoras de serviços de transporte.

2. Qual a finalidade do tratamento?

Registro biométrico de ponto dos colaboradores (anotação do horário de entrada e saída dos colaboradores, a fim de contabilizar a jornada de trabalho).

3. Qual a base legal aplicável?

Art. 11, II, "a", da LGPD - Cumprimento de obrigação legal ou regulatória pelo controlador.
O art. 74 da CLT estipula a necessidade de registro de ponto (anotação do horário de entrada e de saída do trabalho dos empregados), admitindo que ele seja feito por meio manual, mecânico ou eletrônico. A Portaria nº. 1.510/2009 do Ministério do Trabalho autoriza o registro de ponto biométrico dos empregados.

Fase 3 - Rescisão do Contrato de Trabalho e Pós-Contrato

Após a rescisão do contrato, o empregador deve continuar a observar as normas de proteção de dados. Isso inclui o descarte seguro dos dados que não são mais necessários e a retenção dos dados conforme exigido por leis e regulamentos.

Como é comum que os titulares de dados, ou seja, os empregados, recorram ao judiciário após o fim da relação contratual entre o empregado e o empregador, é importante que, até o término dos prazos prescricionais, os documentos relacionados ao empregado sejam arquivados. No caso de aposentadoria, é comum que empresas sejam chamadas a comprovar o tempo de serviço do empregado e, para que a demanda seja atendida, informações pessoais do empregado podem ser armazenadas inclusive após o prazo prescricional da reclamação trabalhista. Ainda, documentos como a guia recolhimento do FGTS e informações à previdência social e a guia de recolhimento rescisório do FGTS e contribuição social devem ser armazenados em lugar seguro para cumprimento de normas no Código Tributário Nacional e na CLT.

Seção 2 - LGPD aplicada ao setor de Transportes

Quando necessária a retenção de dados após o término de um contrato de trabalho, é crucial que as empresas observem estritamente os prazos legais e regulatórios para isso. Os dados devem ser mantidos apenas enquanto houver uma finalidade e base legal para seu armazenamento, como o exercício de direitos em processos judiciais e administrativos.

Após esse prazo, as empresas devem promover o descarte seguro e efetivo desses dados. Para facilitar a gestão dos dados, recomenda-se a manutenção de um inventário dos dados pessoais tratados pela empresa. Esse documento ajuda a controlar os períodos de retenção e a garantir que os dados sejam descartados adequadamente quando não forem mais necessários.

Boas práticas para retenção de dados pessoais

Após o término do tratamento, as empresas devem eliminar os dados tratados. No entanto, há hipóteses em que a conservação dos dados pessoais após o término do tratamento é autorizada pela LGPD e até mesmo necessária para fins de cumprimento de obrigação legal ou regulatória pelo controlador. Nesses casos, deve-se observar os prazos legais e regulatórios específicos para definir o período de retenção dos dados pessoais. Por exemplo:

- Prazo de 5 anos para armazenamento da folha de pagamento do colaborador contado a partir do término da relação de emprego (art. 7º, XXIX, da Constituição e art. 11 da CLT); e

- Prazo de 30 anos para armazenamento de comprovantes de depósito do FGTS (art. 23, § 5º, da Lei nº 8.036/90).

No momento de eliminação definitiva dos dados, deve-se formalizar referida exclusão para fins de auditoria e prestação de contas posterior. É fundamental que a empresa elabore uma política de retenção dos dados para determinar quais dados pessoais serão armazenados após o término do tratamento (por exemplo, término do contrato de trabalho), a partir de qual fundamento legal (art. 16 da LGPD) e por quanto tempo (observando prazos legais e regulatórios aplicáveis). Ademais, podem ser utilizadas técnicas de pseudonimização para auxiliar na proteção das informações pessoais.

Tratamento de dados sensíveis relacionados à saúde e segurança do trabalho

Os dados pessoais relacionados à saúde e segurança do trabalho devem ser tratados pelas empresas com finalidades específicas, de forma proporcional e conforme o princípio da não discriminação. Eles podem incluir informações sobre estado de saúde, como lesões, doenças, incapacidades, histórico médico, diagnósticos, tratamentos, exames médicos, dados de dispositivos médicos ou rastreadores de aptidão, além de dados fornecidos por operadoras de saúde e referentes a tratamentos contínuos, consultas e faturas.

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados sensíveis relacionados à saúde e segurança do trabalho

Dada a sensibilidade dos atestados médicos, recomenda-se que as empresas adotem uma política específica para tratamento, retenção e acesso a essas informações. Eles devem ser armazenados em ambientes separados com controles de acesso rigorosos, autorizando somente pessoas específicas.

Para o oferecimento de planos de saúde e odontológicos corporativos, as empresas devem se atentar para o tratamento de dados pessoais de dependentes, especialmente as crianças, os adolescentes e os idosos, conforme regras específicas da LGPD que protegem o melhor interesse desses grupos. Além disso, ao realizar pesquisas internas para avaliar a produtividade e bem-estar dos colaboradores, é crucial proteger a sua privacidade. Para isso, recomenda-se o uso de técnicas de anonimização ou pseudonimização para garantir a confidencialidade dos dados enquanto se obtêm os resultados desejados.

Para exames admissionais, controle de jornada (registros de ponto) e atividades de segurança do trabalho (exames toxicológicos e teste do bafômetro), é indispensável que as empresas observem todas as obrigações legais e regulatórias aplicáveis. O tratamento deve se restringir ao mínimo necessário para cumpri-las, evitando dados desnecessários.

No tratamento de dados relacionados à saúde e à segurança do trabalho, é comum contratar parceiros, como clínicas médicas e outros prestadores de serviços. Nesses casos, é necessário assegurar que tais parceiros estejam em conformidade com a LGPD e que os contratos definam claramente os direitos, as obrigações e responsabilidades de cada parte, especialmente em relação a medidas de segurança da informação e gestão de incidentes.

Os exames periódicos devem ser limitados a casos que sejam estritamente necessários para o desempenho de funções específicas. Por exemplo, exames toxicológicos para motoristas profissionais são justificados, enquanto os exames de gravidez na admissão de empregados administrativos não são. Os resultados desses exames devem ser acessíveis apenas ao titular e às pessoas autorizadas dentro da empresa.

Os motoristas profissionais em regime celetista devem realizar exames toxicológicos de largo espectro, para detectar substâncias psicoativas em períodos de 90 a 180 dias. Este exame é obrigatório para categorias específicas de motoristas profissionais, como aqueles de furgões, ambulâncias, ônibus e caminhões, e deve ser realizado conforme a legislação.

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados para condução de exames toxicológicos

1. Quem são os titulares de dados?

Motoristas profissionais dos veículos de transporte.

2. Qual a finalidade do tratamento?

Verificar o consumo de substâncias psicoativas (lícitas e/ou ilícitas) pelos motoristas profissionais contratados sob o regime celetista.

3. Quem são os agentes de tratamento?

Prestadoras de serviços de transporte e o Ministério do Trabalho e Emprego. O art. 2º da Portaria nº. 945/2017 do Ministério do Trabalho e Previdência Social exige, das empresas contratantes de motoristas profissionais contratados sob o regime celetista, a inserção dos dados do resultado do exame toxicológico no eSocial sempre que for admitido ou desligado. Os resultados detalhados dos exames devem ficar armazenados em formato eletrônico pelo laboratório executor por, no mínimo, 5 (cinco) anos.

4. Qual a base legal para o tratamento?

Art. 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. 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, somados à Portaria MTE nº 612/2024 e a Resolução nº 1009/2024 do Contran . Por fim, o Código de Trânsito Brasileiro normatiza em seu art. 165-A penalidade de multa por se recusar a soprar o bafômetro.

5. Quais cuidados devem ser adotados?

Por se tratar de dados sensíveis, a segurança da informação no tratamento de dados de saúde é elemento de destaque. Qualquer incidente de segurança pode colocar os direitos dos titulares em um risco mais elevado, quando comparado com dados meramente cadastrais, por exemplo. Por isso, os resultados dos exames devem ser armazenados em local controlado e seguro, a fim de se evitar acessos por terceiros não autorizados.

O teste de bafômetro é uma ferramenta de controle prevista no art. 235-B da CLT, que pode ser usada para monitorar o uso de álcool entre os motoristas profissionais. As empresas devem criar um regulamento específico que detalhe os procedimentos do teste, incluindo a periodicidade, local de realização, possibilidade de contraprova e medidas em caso de resultado positivo. Os empregados devem ser informados claramente sobre esses procedimentos e a recusa em realizar o teste pode ser considerada infração disciplinar.

Seção 2 - LGPD aplicada ao setor de Transportes

Tratamento de dados para realização de teste de bafômetro

1. Quem são os titulares de dados?

Motoristas profissionais dos veículos de transporte

2. Qual a finalidade do tratamento?

Verificar o consumo de álcool no sangue do motorista profissional contratado sob o regime CLT.

3. Qual a base legal aplicável?

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 celetista submeta-se ao programa de controle de uso de drogas e bebida alcoólica instituído pela empresa prestadora de serviços de transportes para a qual trabalha, desde que prévia e amplamente cientificado.

Os resultados dos exames toxicológicos e dos testes de bafômetro são considerados dados sensíveis e, por isso, devem ser tratados com fundamento nas bases legais do art. 11 da LGPD, garantindo a confidencialidade e segurança dos dados.

O tratamento de dados sensíveis, em especial os relacionados à saúde e segurança do trabalho, exige rigor e conformidade com a legislação aplicável. Dessa forma, empresas devem adotar políticas claras, garantir a segurança e a confidencialidade dos dados e ser transparentes com os titulares sobre as finalidades do tratamento e seus direitos.

Boas práticas para tratamento de dados sensíveis relativos à saúde e à segurança do trabalho

- **Confidencialidade e Uso dos Dados:** Os dados pessoais coletados pelo etilômetro, utilizados para medir a presença de álcool no sangue, não devem ser usados para finalidades diferentes da original. Não se deve tratar esses dados para o controle de pontualidade ou jornada de trabalho sem o consentimento dos motoristas, pois tal prática pode gerar impactos negativos, como procedimentos disciplinares internos e até demissão. É importante respeitar a natureza sensível dos dados, a obrigação legal do motorista de fornecê-los e o desequilíbrio de poder entre o motorista e a empresa.

- **Armazenamento Seguro:** Os resultados dos exames toxicológicos de motoristas profissionais, mesmo daqueles que não foram contratados ou já foram demitidos, devem ser armazenados separadamente de outras informações. O acesso a esses resultados deve ser restrito a pessoas expressamente autorizadas e que necessitem delas para desempenhar as suas funções.

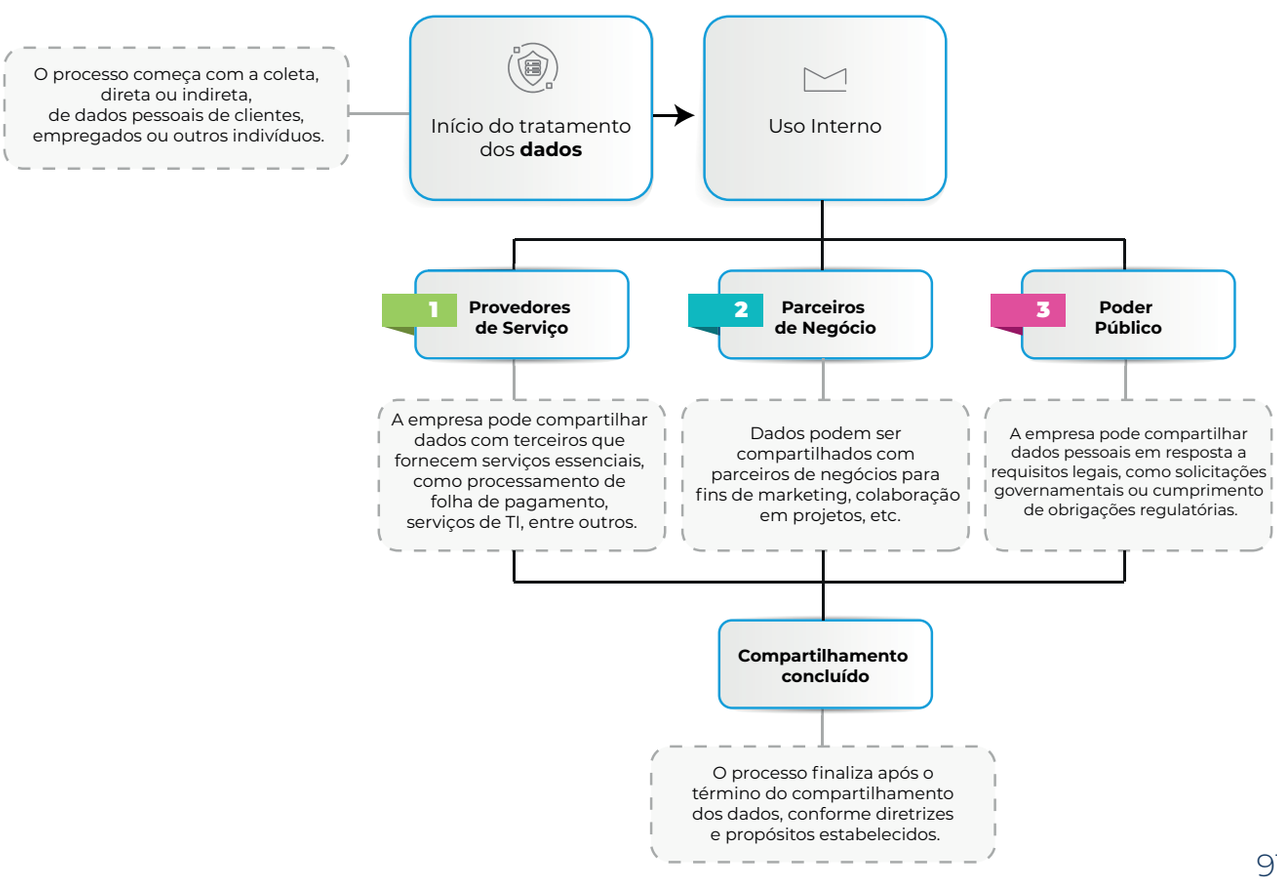
Seção 2 - LGPD aplicada ao setor de Transportes

- **Transparência e Informação:** As empresas devem documentar e divulgar amplamente entre os motoristas empregados as informações relacionadas ao tratamento de dados sensíveis resultantes do exame toxicológico e teste do bafômetro, incluindo forma de armazenamento, tempo de retenção, finalidade do tratamento e outras informações relevantes.

A proteção dos dados pessoais e sensíveis dos empregados é responsabilidade das empresas. Desde a fase pré-contratual até após a rescisão do contrato, medidas práticas e políticas rigorosas devem ser implementadas para garantir a conformidade com as normas de proteção de dados e para proteger os direitos dos empregados e atentar-se, em especial, ao trabalho remoto e à terceirização de atividades de tratamento são aspectos primordiais dessa responsabilidade.

5.3 Compartilhamento de dados com terceiros

A prestação de serviços de transporte de passageiros e de cargas frequentemente exige o compartilhamento de dados pessoais com parceiros e empresas terceirizadas, como prestadores de serviços, agências de viagens, e até empresas de assistência aos passageiros. Esse compartilhamento pode ser necessário por uma imposição legal ou regulatória, ou para cumprimento de um contrato. Em regra, ele ocorre conforme o seguinte fluxo:



Seção 2 - LGPD aplicada ao setor de Transportes

É fundamental garantir a transparência aos titulares de dados sobre essas atividades de tratamento. Além disso, os contratos celebrados com terceiros devem incluir cláusulas específicas sobre proteção de dados, assegurando o cumprimento das políticas mesmo fora do ambiente da empresa.

Os contratos que envolvem o compartilhamento de dados devem conter disposições que abordem, por exemplo, finalidades específicas do tratamento, responsabilidades das partes em responder aos questionamentos de autoridades e titulares, obrigação de reportar incidentes de segurança em tempo hábil, medidas de segurança necessárias para proteger as informações compartilhadas e outras cláusulas necessárias para preservar direitos dos titulares, por exemplo.

Cláusulas contratuais que podem ser incluídas em contatos com terceiros

- Glossário com terminologia e conceitos da LGPD.
- Duração das atividades de tratamento e deveres das partes ao término do tratamento e/ou da relação contratual.
- Realização periódica de auditorias para verificar a conformidade do terceiro.
- Indicação de todos os agentes de tratamento envolvidos.
- Finalidades específicas do tratamento de dados.
- Vedação à utilização de dados pessoais sem ciência ou autorização do controlador.
- Exigência de adequação das partes do contrato à LGPD.
- Vedação ao compartilhamento e obrigatoriedade de notificação à parte caso seja necessário.
- Obrigação de registro de informações.
- Obrigação de implementação de medidas técnicas e administrativas de segurança.
- Possibilidade de realização de auditorias.
- Dever de confidencialidade.

Seção 2 - LGPD aplicada ao setor de Transportes

Cláusulas contratuais que podem ser incluídas em contatos com terceiros

- Periodicidade de atualização de informações do contrato.
- Hipóteses de transferência e compartilhamento de dados.
- Obrigatoriedade de elaboração de plano de resposta a incidentes envolvendo dados pessoais.
- Procedimentos de destruição e devolução de dados.
- Obrigatoriedade de notificação em caso de documentos oficiais que obriguem o fornecimento de dados pessoais.
- Procedimento de resposta a incidentes de segurança envolvendo dados pessoais.
- Mecanismos de cooperação entre as partes para atender a solicitações dos titulares de dados e de requisições da ANPD.

No processo de contratação de prestadores de serviço, as empresas devem evitar a coleta excessiva de dados e garantir que os titulares sejam plenamente informados sobre a finalidade da coleta e possíveis compartilhamentos de dados devido a obrigações legais ou regulatórias. Se houver atualizações periódicas de dados dos empregados dos prestadores de serviço, o acesso a esses documentos deverá ser restrito a agentes autorizados. Abaixo, são indicados alguns casos de compartilhamento de dados realizados corriqueiramente no setor de transportes apenas a título exemplificativo.

Agências de Viagens

Quando uma empresa de transporte rodoviário possui um acordo com uma agência de viagens para venda de passagens, podem ser compartilhados dados de nome, contato e detalhes da viagem (datas, horários e destinos) para facilitar a emissão de bilhetes e a coordenação das viagens.

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Sistemas de Pagamento	Uma empresa de transporte urbano que usa cartões de transporte ou aplicativos de pagamento integrados pode compartilhar dados de pagamento, histórico de viagens e informações de uso do cartão com empresas de sistema de pagamento para processar pagamentos e gerenciar o saldo dos cartões de transporte.
Serviços de Assistência ao Passageiro	Uma empresa aérea contrata empresas de assistência para ajudar os passageiros em casos de emergências, como perda de bagagem ou cancelamento de voos. Para tais empresas poderem oferecer suporte e resolverem problemas de forma eficiente, podem ser compartilhadas informações de contato, detalhes do voo e o histórico das viagens.
Autoridades Competentes	Uma empresa de transporte rodoviário de passageiros pode vir a ser obrigada a compartilhar informações de identidade de passageiros e motorista, horários de partida e chegada e itinerários com órgãos de segurança pública, como a Polícia Rodoviária Federal para ajudar na identificação de passageiros em situações de emergência ou investigação criminal.
Gestão de Benefícios de Empregados	Uma empresa de logística que oferece planos de saúde e odontológicos aos seus empregados pode compartilhar, com o plano de saúde, dados de contato, nome, CPF e informações médicas para garantir que os empregados tenham acesso aos benefícios contratados.

Ao encerrar os contratos de prestação de serviço, as empresas devem observar os prazos legais e regulatórios para a guarda e retenção dos dados pessoais dos empregados dos prestadores de serviço. Aqueles que não forem necessários devem ser descartados de maneira consciente e cuidadosa. A gestão responsável e transparente do compartilhamento de dados é essencial para a conformidade com a LGPD e a proteção dos direitos dos titulares. As empresas devem garantir que todos os processos de compartilhamento, desde

Seção 2 - LGPD aplicada ao setor de Transportes

a celebração de contratos até o descarte final, sejam realizados conforme os princípios de proteção de dados e segurança da informação.

Outro ponto que merece atenção, especialmente em casos de compartilhamento de dados com terceiros, é a ocorrência de atividades de transferência internacional de dados (art. 33, LGPD). Transferir dados para fora do Brasil pode ser, em determinadas ocasiões, útil ou mesmo imprescindível para as atividades de transporte, sendo uma realidade inafastável em uma economia globalizada.

Parcela relevante dos instrumentos e dos critérios necessários para a definição dos parâmetros para a transferência internacional de dados ainda depende de regulamentação da ANPD. No entanto, o primeiro passo para a conformidade é a alteração contratual. Os contratos de transporte cuja execução implique em transferência internacional dos dados devem ser redigidos para deixar claros os elementos da transferência (como categorias de dados transferidos, destinatários e finalidade) e assegurar, ao titular, informação facilitada sobre a transferência e seus aspectos principais.

Para tanto, pode ser considerada a inclusão de cláusulas-padrão em contratos para garantir que o nível de proteção de dados no país de destino é equivalente ao da LGPD, bem como de especificações sobre o tratamento de dados pessoais que sejam reconhecidas por autoridades de proteção de dados de outros países, até que a ANPD elabore o próprio modelo de cláusulas-padrão contratuais. No caso de multinacionais, deve-se considerar a formulação ou adesão a cláusulas corporativas globais. Outra possibilidade é a adoção de certificações oferecidas por instituições idôneas e reconhecidas no mercado.

Sempre que uma transferência internacional for autorizada pelo consentimento do titular, este deverá ser obtido de forma específica, apartado de outras cláusulas contratuais e com destaque para a transferência, com a informação acerca do caráter internacional da operação e de outras informações que sejam relevantes no contexto da transferência.

Transferências internacionais homologadas e legitimadas perante as autoridades de proteção de dados de outros países podem ser documentadas e publicizadas como fator indicativo da proatividade na matéria até que sejam editadas regulamentações da ANPD que possibilitem a ampla utilização das hipóteses autorizativas previstas na LGPD.

Ainda, o compartilhamento de dados com terceiros pode acontecer sem que este esteja previsto em contrato, como nos casos de compartilhamento com o Poder Público. Nesses casos, autoridades públicas requerem dados pessoais para fins diversos, e cabe à empresa verificar a identidade da autoridade solicitante e a competência da autoridade.

Seção 2 - LGPD aplicada ao setor de Transportes

Atenção!

O compartilhamento de dados pessoais com instituições públicas e/ou privadas

Sempre que a organização compartilhar dados pessoais com instituições públicas ou privadas, é fundamental considerar os seguintes aspectos:

- Observar as regras previstas nos arts. 33 a 35 em caso de transferência de dados pessoais para fora do território brasileiro, isto é, em caso de transferência internacional de dados (conforme será visto a seguir);
- Certificar que o compartilhamento será realizado de forma legítima e lícita, com fundamento em uma das bases legais dispostas no arts. 7° e 11 da LGPD;
- Fornecer todas as informações e avisos necessários aos titulares a respeito das características relevantes do tratamento e do compartilhamento dos dados pessoais com tais instituições;
- Caso o compartilhamento seja necessário para cumprimento de obrigação legal/regulatória, exercício regular de direitos em processo judicial/ administrativo/arbitral ou para execução de contrato, garantir que as categorias e a quantidade de dados compartilhados sejam estritamente necessárias para cumprir com tal finalidade, abstendo-se de compartilhar dados adicionais (para os quais não haveria base/fundamento legal na LGPD); e
- Documentar todo compartilhamento realizado, para fins de auditoria (por exemplo, caso o compartilhamento ocorra para cumprir uma ordem judicial, armazenar a cópia da decisão e a comprovação do compartilhamento, seja por e-mail, pelo comprovante de protocolo ou outro documento).

Além disso, para garantir a legalidade do compartilhamento de dados pessoais com autoridades policiais, Poder Judiciário e demais autoridades competentes, as organizações devem:

- Verificar e confirmar a identidade da autoridade solicitante, para evitar o compartilhamento indevido dos dados com pessoas ou autoridades não competentes ou não autorizadas;
- Fornecer as informações solicitadas tão somente caso o requerimento seja encaminhado por autoridade competente no formato legalmente exigido, a exemplo de ordens judiciais que são necessárias para disponibilização de algumas categorias de dados;
- Encaminhar o pedido para análise do setor jurídico da empresa sempre que possível, a fim de confirmar adequadamente a legitimidade da solicitação;
- Confirmar se a solicitação possui alguma referência numérica oficial de procedimento, ofício, processo, notificação, entre outros; e
- Disponibilizar, caso seja possível, um canal de comunicação específico para recebimento das solicitações, como um e-mail corporativo, designando um responsável para o recebimento e redirecionamento dos pedidos.

Seção 2 - LGPD aplicada ao setor de Transportes

6. SEGURANÇA DA INFORMAÇÃO

A LGPD estabelece os princípios da segurança (art. 6º, VII) e da prevenção (art. 6º, VIII), determinando que os agentes de tratamento devem adotar medidas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer tratamento inadequado.

Por que é importante saber lidar com um incidente de segurança?

Uma grande empresa de transporte rodoviário que opera uma extensa rede de linhas de ônibus intermunicipais e interestaduais coleta e armazena uma grande quantidade de dados pessoais de seus passageiros, como nomes, endereços, números de telefone, CPF, informações de pagamento e dados de localização (de histórico de viagens). Além disso, a empresa trata dados sensíveis dos motoristas, incluindo as informações de saúde e dados biométricos utilizados para o controle de acesso e verificação de identidade. Num dia movimentado, os sistemas da empresa sofrem um ataque cibernético devastador. Hackers altamente sofisticados invadem os servidores da empresa, acessando e exfiltrando dados de milhões de passageiros e motoristas. Os hackers criptografam os dados, exigindo um resgate milionário em criptomoedas para devolver o acesso. Ainda, parte dos dados roubados é divulgada em fóruns da *dark web,* expondo as informações ao público e criminosos. O incidente causa pânico em passageiros e motoristas, que temem pelo uso indevido de suas informações. A mídia rapidamente divulga o caso, destacando todas as falhas de segurança e a potencial exposição de dados sensíveis. As redes sociais são então inundadas com comentários negativos e pedidos de boicote à empresa. O impacto financeiro é imediato: reservas são canceladas e a confiança do público despenca. Reguladores abrem investigações e a empresa enfrenta possíveis multas milionárias por violar as diretrizes da LGPD.

E se a empresa já estivesse adequada à LGPD e implementado robustas medidas de segurança e proteção de dados, o cenário poderia ter sido diferente? A criptografia dos dados armazenados nos servidores, por exemplo, garantiria que, mesmo em caso de acesso não autorizado, os dados fossem ilegíveis e inúteis a invasores. A utilização de método de autenticação multifator (MFA) e rigorosos controles de acesso limitaria a entrada de usuários e de administradores aos sistemas críticos, reduzindo riscos de acesso não autorizado a servidores e dados sensíveis. Além disso, a implementação de sistemas avançados de monitoramento e de detecção de ameaças identificaria e

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Por que é importante saber lidar com um incidente de segurança?

responderia rapidamente às atividades suspeitas e às tentativas de intrusão, permitindo uma resposta organizada e eficiente ao incidente. A manutenção de backups regulares e seguros dos dados críticos, armazenados em locais isolados e protegidos, possibilitaria a restauração rápida dos sistemas e dos dados sem necessidade de pagamento do resgate, garantindo a continuidade dos negócios. Ainda, programas contínuos de treinamento e conscientização sobre segurança da informação aos colaboradores reduziriam o risco de erro humano, promovendo maior vigilância contra possíveis ameaças.

Portanto, a adequação à LGPD e a implementação de medidas robustas de segurança poderiam ter prevenido ou, pelo menos, mitigado significativamente os impactos de um incidente de segurança na empresa, evitando não apenas prejuízos financeiros, como danos à reputação.

Para garantir a segurança no armazenamento e descarte de informações em papel, documentos sensíveis devem ser guardados em locais seguros, como armários trancados ou salas de arquivo com acesso restrito, garantindo que apenas o pessoal autorizado possa acessá-los. É importante também manter um registro de quem acessa esses documentos e com que finalidade. No momento do descarte, documentos em papel devem ser triturados para impossibilitar a reconstrução das informações. Ainda, deve haver uma política clara de retenção de documentos, que estabeleça por quanto tempo cada tipo de documento deve ser mantido antes de ser descartado, conforme as exigências legais e regulatórias.

As empresas devem seguir as determinações da ANPD e, quando possível, observar normas técnicas consolidadas, como aquelas da Associação Brasileira de Normas Técnicas (ABNT) e da Organização Internacional de Normalização (ISO). Os agentes de tratamento devem adotar medidas técnicas de segurança da informação em três níveis, a depender da imprescindibilidade delas para a continuidade dos negócios e confiança de parceiros.[23]

Medidas Básicas

- **Políticas e Conscientização:** Elaborar, atualizar e comunicar diretrizes baseadas em melhores práticas para assegurar a proteção dos dados, promovendo uma cultura organizacional de segurança da informação.
- **Treinamento:** Oferecer treinamentos regulares aos colaboradores sobre práticas de segurança da informação, incluindo simulações e tutoriais de como reconhecer e responder a tentativas de phishing e outras ameaças cibernéticas.

>>

23 https://static.portaldaindustria.com.br/media/filer_public/6c/a0/6ca07577-fbc6-4e9a-81cf-700e0570849b/id_1633_guia_de_boas_praticas_de_protecao_de_dados_para_a_industria_web.pdf.

Seção 2 - LGPD aplicada ao setor de Transportes

- **BYOD *(Bring Your Own Device)* e MDM *(Mobile Device Management)*:** Estabelecer políticas claras para o uso de dispositivos pessoais no trabalho, incluindo requisitos de segurança para dispositivos móveis, usando soluções de gerenciamento.

- **Controle e Gestão de Credenciais:** Garantir que o acesso aos dados seja restrito às pessoas autorizadas, removendo-os imediatamente se não forem mais necessários ou quando o colaborador sair da organização.

- **Backup e Recuperação:** Assegurar que os dados essenciais para a operação tenham cópias de segurança, armazenadas de maneira segura e protegidas contra os acessos não autorizados, permitindo sua recuperação eficiente em caso de emergências. Implementar procedimentos de troca periódica de senhas e outras credenciais de acesso aos sistemas da empresa.

- **Inventário e Segurança de Ativos:** Manter inventário atualizado dos ativos que processam dados, implementando requisitos mínimos de segurança para proteger ativos contra ameaças.

- **Segurança:** Implementar e manter atualizadas soluções de antimalware e firewalls em todos os dispositivos que manipulam dados pessoais, garantindo a proteção contínua contra ameaças.

- **Acesso Físico:** Implementar controles de acesso físico em áreas sensíveis, como data centers e salas de servidores para impedir acessos não autorizados e utilizar as câmeras de vigilância e sistemas de alarme para monitorar e proteger as instalações físicas contra invasões e roubos.

Medidas Secundárias

- **Gestão de Incidentes:** Supervisionar continuamente o comportamento de acesso e segurança dos ativos que tratam dados. Estar preparado para identificar e responder prontamente a acessos e/ou comportamentos não autorizados.

- **Fornecedores:** Verificar se os contratos com os fornecedores incluem cláusulas específicas de tratamento de dados pessoais, assegurando a conformidade com as normas aplicáveis.

- **Sistemas Críticos:** Garantir que as atividades de tratamento de dados sejam registradas, com data, horário, duração, identidade do colaborador ou responsável e ação executada.

- **Prevenção de Vazamentos:** Implementar estratégias eficazes para prevenir os vazamentos de dados pessoais em todas as etapas do ciclo de tratamento.

- **Testes de Segurança:** Executar regularmente testes de segurança nos sistemas que processam dados pessoais, com ênfase em sistemas acessíveis via internet, para mitigar vulnerabilidades.

- **Transferência dos Dados:** Assegurar que todas as transferências de dados sejam realizadas com segurança, protegendo os dados contra acessos não autorizados durante a comunicação.

Seção 2 - LGPD aplicada ao setor de Transportes

Medidas Avançadas

- **Arquitetura de Segurança:** Avaliar e melhorar continuamente a infraestrutura tecnológica, incluindo os ambientes de nuvem, para garantir uma proteção eficaz dos dados pessoais.
- **Eliminação de Dados:** Criar um mapeamento detalhado dos dados pessoais para assegurar a sua exclusão eficiente, conforme solicitações dos titulares.
- **Mascaramento:** Adotar técnicas de mascaramento de dados em cenários apropriados a fim de proteger informações sensíveis durante o processamento.
- **Pseudonimização:** Implementar a pseudonimização de dados sempre que possível, a fim de reforçar a privacidade e segurança no tratamento de informações pessoais.
- **Desenvolvimento Seguro:** Integrar requisitos de segurança no ciclo de desenvolvimento de produtos e sistemas, assegurando que a segurança seja incorporada desde a concepção.
- **Criptografia:** Aplicar criptografia para proteger dados pessoais em situações que requeiram alta confidencialidade e integridade das informações.
- ***Firewall* e IDS/IPS:** Implementar *firewalls* e sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar e proteger a rede contra acessos não autorizados.
- **VPN de Acesso Remoto:** Utilizar redes privadas virtuais (VPNs) para acesso remoto seguro, especialmente para os motoristas e demais colaboradores de campo.

A proteção de dados e a segurança da informação são pilares fundamentais para a integridade e a confiança nas operações de qualquer empresa, especialmente no setor de transporte. Nesse sentido, serão destacados 3 (três) documentos relevantes para estabelecer normas e procedimentos específicos para proteger dados, minimizar riscos de segurança e garantir a continuidade das operações da empresa.

Plano de Resposta a Incidentes de Segurança

O Plano de Resposta a Incidentes de Segurança prevê as diretrizes e procedimentos para identificar, responder e mitigar os efeitos de incidentes de segurança da informação, garantindo a continuidade dos negócios e a proteção dos dados pessoais. O objetivo é minimizar os impactos negativos, como violações de dados ou ataques cibernéticos, e assegurar uma resposta eficiente e coordenada. O documento deve ser elaborado pelo departamento de segurança da informação em colaboração com o jurídico e a alta administração. Ele deve ser revisado e atualizado periodicamente, em especial após uma ocorrência de incidentes ou mudanças significativas no ambiente de TI. O plano inclui a definição de incidentes, a composição da equipe de resposta, procedimentos de notificação interna e externa, avaliação do impacto, mitigação, recuperação e documentação, e diretrizes para a comunicação com partes interessadas e revisão pós-incidente.

Seção 2 - LGPD aplicada ao setor de Transportes

Política de Mesa Limpa

A Política de Mesa Limpa objetiva garantir que as áreas de trabalho dos colaboradores estejam livres de documentos sensíveis e de dispositivos não utilizados, minimizando o risco de acessos não autorizados e vazamentos de informações. A finalidade é proteger dados confidenciais e pessoais, promovendo um ambiente seguro e organizado. Este documento costuma ser elaborado pelo departamento de segurança da informação em conjunto com a área de recursos humanos. Ele é comunicado a todos os colaboradores e reforçado através de treinamentos regulares. Seus principais elementos incluem temas como a obrigação de guardar documentos sensíveis em armários trancados ao final do expediente, não deixar documentos confidenciais à vista em mesas de trabalho, bloquear computadores e dispositivos eletrônicos quando não estiverem em uso, e a realização de auditorias periódicas para garantir a conformidade.

Política de Armazenamento e Retenção de Dados (art. 15, LGPD)

A Política de Armazenamento e Retenção de Dados Pessoais busca estabelecer diretrizes para o armazenamento seguro e a retenção adequada de dados pessoais, garantindo a conformidade com a legislação vigente, especialmente a LGPD. O objetivo é assegurar que os dados sejam mantidos apenas pelo tempo necessário para cumprir as finalidades para as quais foram coletados inicialmente. Este documento normalmente é elaborado pela área de recursos humanos com a TI e o jurídico, e é revisado periodicamente para refletir mudanças legais, regulatórias e operacionais, mas também pode contemplar quaisquer áreas que realizem tratamentos de dados, a critério da organização. Ele abarca a classificação de dados conforme nível de sensibilidade, diretrizes para armazenamento seguro, incluindo a criptografia para os dados eletrônicos e o armazenamento físico seguro, e definição de períodos de retenção baseados em requisitos legais e necessidades de negócio. Há ainda o detalhamento de procedimentos seguros para o descarte de dados ao final do período de retenção, assim como as responsabilidades dos colaboradores. Auditorias regulares devem ser realizadas para garantir a conformidade à LGPD, e treinamentos devem ser oferecidos para conscientizar colaboradores sobre melhores práticas.

Apesar das rigorosas medidas de segurança implementadas para proteger os dados pessoais, incidentes de segurança podem ocorrer devido a diversos fatores, como as falhas humanas, as vulnerabilidades tecnológicas e ataques cibernéticos sofisticados. Incidentes de segurança são eventos adversos confirmados que comprometem a confidencialidade, a integridade, a disponibilidade ou a autenticidade dos dados, e podem incluir os acessos não autorizados, vazamento de dados, entre outros. Esses eventos podem ter consequências significativas aos titulares dos dados e organizações envolvidas, exigindo uma resposta rápida e eficaz para minimizar os danos e cumprir com as obrigações legais estabelecidas pela LGPD.

Seção 2 - LGPD aplicada ao setor de Transportes

Exemplo

Uma empresa de transporte rodoviário de cargas enfrentou um incidente grave de segurança envolvendo dados pessoais. A empresa usa um sistema de gerenciamento de frotas que armazena dados pessoais, incluindo a localização dos veículos, detalhes pessoais dos motoristas e informações de clientes sobre envios e entregas. O sistema é acessível apenas por colaboradores autorizados, que utilizam as credenciais de acesso individuais. O incidente começou quando o gerente de operações, enfrentando certas dificuldades técnicas, pediu ajuda a um colega. Durante o processo, ele deixou as suas credenciais de acesso visíveis no post-it ao lado do monitor. O funcionário temporário contratado para tarefas administrativas viu as credenciais durante uma pausa na sala de controle e, sem perceber a gravidade da situação, utilizou as credenciais do gerente para acessar o sistema de gerenciamento de frotas. Com isso, o funcionário começou a explorar os dados disponíveis. Achando estar reportando um bug ao suporte técnico terceirizado, enviou um e-mail com informações confidenciais de motoristas e clientes para um endereço externo, com dados sensíveis que, se expostos, poderiam causar sérios danos aos titulares, como fraude ou roubo de identidade. O erro foi detectado quando o suporte técnico notificou a empresa sobre a recepção inesperada dos dados confidenciais. A equipe de segurança da informação iniciou uma investigação interna imediata para avaliar a extensão da violação e identificar as causas. A análise revelou que o erro humano relacionado ao manuseio inadequado das credenciais de acesso foi o principal fator que permitiu o incidente. A falta de treinamento adequado sobre práticas seguras de gerenciamento de credenciais contribuiu para a ocorrência. Dada a gravidade do incidente e devido à exposição de dados sensíveis e potencialmente prejudiciais a um grande número de titulares, a empresa comunicou o incidente à ANPD e aos titulares afetados, conforme exigido na Resolução CD/ANPD nº 15/2024. O incidente destacou a importância de práticas rigorosas de segurança da informação e do treinamento contínuo dos colaboradores sobre o manuseio seguro de credenciais de acesso. A empresa reforçou suas políticas de segurança, implementou sessões de treinamento adicionais e introduziu sistema de autenticação multifator para aumentar a proteção dos dados, de forma a prevenir novos incidentes semelhantes e garantir a conformidade contínua com a LGPD.

Quando um incidente de segurança ocorre, a empresa deve identificar rapidamente o incidente e avaliar sua natureza e extensão, adotando medidas imediatas para contê-lo e impedir sua propagação, por exemplo, isolar sistemas afetados ou interromper atividades comprometidas.

Em seguida, deve-se avaliar os possíveis impactos e danos causados pelo incidente aos titulares dos dados e à própria empresa, determinando a categoria e a quantidade de dados afetados e titulares envolvidos. É essencial informar imediatamente os responsáveis pela proteção de dados dentro da empresa, registrando todas as ações e decisões tomadas durante a gestão do incidente.

Caso haja risco significativo aos direitos dos titulares, a comunicação com a ANPD e os titulares é obrigatória (art. 48, LGPD). Ela deve ocorrer em até três dias úteis após a ciência do incidente (com prazo em dobro aos agentes de pequeno porte) e fornecer informações

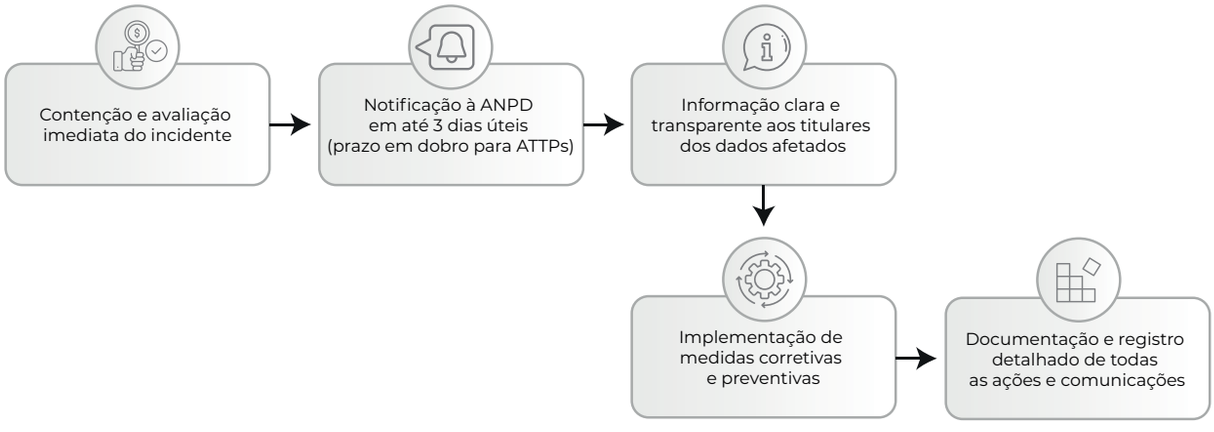
Seção 2 - LGPD aplicada ao setor de Transportes

detalhadas a respeito do incidente, incluindo a natureza dos dados pessoais afetados, informações sobre os titulares impactados, medidas técnicas e de segurança adotadas, riscos relacionados ao incidente e às medidas adotadas para mitigar esses riscos, além de provas documentais do incidente e as suas consequências (art. 6º da Resolução CD/ANPD nº 15/2024). A empresa também deve informar os titulares dos dados afetados sobre o incidente, especialmente se houver risco significativo aos seus direitos e liberdades, fornecendo informações sobre o ocorrido, as medidas adotadas e orientações sobre como os titulares podem se proteger contra possíveis consequências negativas.

É indispensável implementar ações corretivas para mitigar os danos e prevenir a recorrência de incidentes similares, além de revisar e atualizar as políticas de segurança e proteção de dados a partir das lições aprendidas durante o incidente. Por fim, é importante manter registros detalhados de todos os incidentes de segurança, incluindo ações tomadas e comunicações realizadas, e elaborar relatórios sobre os incidentes, indicando as medidas adotadas para futuras auditorias.

Ainda, quando houver compartilhamento de dados com terceiros, é recomendável desenvolver protocolos de auditoria para avaliar as práticas de segurança utilizadas pelos parceiros. Isso porque incidentes de segurança nos sistemas desses parceiros podem gerar efeitos jurídicos à empresa que compartilhou os dados. Esse mesmo cuidado deve ocorrer com a contratação de operadores e suboperadores. Estas auditorias devem ser periódicas, para garantir a conformidade contínua com os padrões estabelecidos na empresa.

A ANPD regulamentou as obrigações para comunicação de incidentes de segurança por meio da Resolução CD/ANPD nº 15/2024.



Seção 2 - LGPD aplicada ao setor de Transportes

FAQ do Regulamento de Comunicação de Incidentes de Segurança da ANPD

1) Quando um incidente deve ser comunicado e para quem? O incidente deve ser comunicado à ANPD e aos titulares afetados se puder acarretar risco ou dano relevante aos titulares (arts. 4º e 5º da Resolução CD/ANPD nº 15/2024). Isso ocorre se, cumulativamente, o incidente:

- Puder afetar significativamente interesses e direitos dos titulares, isto é, quando impedir o exercício de direitos ou utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

- Envolver dados sensíveis; de crianças, adolescentes ou idosos; financeiros; de autenticação em sistemas; protegidos por sigilo legal, judicial ou profissional; ou em larga escala (nos casos em que há número significativo de titulares, considerando ainda o volume de dados envolvidos, a duração, a frequência e a extensão geográfica de localização dos titulares).

2) Qual o prazo para comunicar a ANPD e o que deve ser comunicado? A comunicação deve ser realizada pelo controlador no prazo de três dias úteis contados do conhecimento de que o incidente afetou dados pessoais, ressalvada a existência de prazo para comunicação previsto em legislação específica, como o prazo em dobro para agentes de pequeno porte (art. 6º da Resolução CD/ANPD nº 15/2024). Ela deve ser realizada pelo formulário disponibilizado pela ANPD e conter informações sobre:

- Descrição da natureza e da categoria de dados pessoais afetados;
- Número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- Medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
- Riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- Motivos da demora, caso a comunicação não seja realizada no prazo exigido;
- Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- Data da ocorrência do incidente, se identificável, e do conhecimento pelo controlador;
- Dados do encarregado ou de quem represente o controlador;
- Identificação do controlador e, se for o caso, declaração de que se trata de um agente de pequeno porte;
- Identificação do operador, quando aplicável;
- Descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- Total de titulares cujos dados são tratados nas atividades afetadas pelo incidente.

3) É possível que a ANPD solicite outros documentos? Sim. É possível, por exemplo, que ela solicite informações adicionais sobre o incidente de segurança, como o registro das operações de

>>

Seção 2 - LGPD aplicada ao setor de Transportes

tratamento de dados afetados pelo incidente, o relatório de impacto à proteção de dados e o relatório de tratamento do incidente (art. 8º da Resolução CD/ANPD nº 15/2024).

4) Qual o prazo para comunicar os titulares e o que deve ser comunicado? A comunicação dos titulares deve ser realizada pelo controlador em até três dias úteis contados do conhecimento de que o incidente afetou dados pessoais, ressalvada a existência de prazo para comunicação previsto em legislação específica, como o prazo em dobro para agentes de pequeno porte (art. 8º da Resolução CD/ANPD nº 15/2024). Ela deve conter informações sobre:

- Descrição da natureza e da categoria de dados pessoais afetados;
- Medidas técnicas e de segurança usadas para proteção dos dados, observados os segredos comercial e industrial;
- Riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;
- Motivos da demora, caso a comunicação não seja realizada no prazo exigido;
- Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- Data do conhecimento do incidente de segurança; e
- Contato para obtenção de informações e, se aplicável, os dados de contato do encarregado.

5) De que forma a comunicação aos titulares deve ser enviada? A comunicação deve fazer uso de linguagem simples e de fácil entendimento e, se for possível identificar os titulares, ocorrer de forma direta e individualizada, isto é, realizá-la pelos meios normalmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta. Caso a comunicação direta e individualizada seja inviável ou não seja possível identificar os titulares afetados (parcial ou integralmente), o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, como o seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento, de modo que a comunicação permita o conhecimento amplo, com fácil visualização, por, no mínimo, três meses. Poderá ser considerada boa prática a inclusão de recomendações aptas a reverter ou mitigar os efeitos do incidente de segurança na comunicação aos titulares (art. 9º da Resolução CD/ANPD nº 15/2024).

6) É necessário manter um registro de todo incidente de segurança? Sim, inclusive aqueles que não foram comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção (art. 10 da Resolução CD/ANPD nº 15/2024).

7) Quais informações devem constar no registro do incidente de segurança? Ele deverá conter, no mínimo, (i) a data de conhecimento do incidente; (ii) a descrição geral das circunstâncias em que o incidente ocorreu; (iii) a natureza e a categoria de dados afetados; (iv) o número de titulares afetados; (v) a avaliação do risco e os possíveis danos aos titulares; (vi) medidas de correção e mitigação dos efeitos do incidente, quando aplicável; (vii) a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e (viii) os motivos da ausência de comunicação, se for o caso (art. 10, § 1º, da Resolução CD/ANPD nº 15/2024).

Seção 2 - LGPD aplicada ao setor de Transportes

7. USO DE NOVAS TECNOLOGIAS NO SETOR DE TRANSPORTES

A revolução tecnológica transformou profundamente diversos setores da economia e o setor de transportes não é exceção. As novas tecnologias têm o potencial de melhorar significativamente a eficiência operacional, segurança e experiência dos usuários. Porém, a adoção dessas tecnologias traz novos desafios em relação à proteção de dados.

Este capítulo aborda as principais tecnologias utilizadas no setor de transportes, os benefícios proporcionados e as preocupações com privacidade e proteção de dados, além de sugerir boas práticas e salvaguardas para mitigar os riscos associados a elas.

Inteligência Artificial (IA)

A inteligência artificial (IA) vem sendo amplamente adotada no setor de transportes para otimização de rotas (algoritmos de IA analisam dados de tráfego em tempo real para indicar rotas mais eficientes, economizando tempo e combustível), previsão de demandas (empresas de transporte público usam IA para prever os picos de demanda e assim ajustar os horários para maior fluxo de veículos) e manutenção preditiva (sensores instalados em veículos coletam dados continuamente e sistemas de IA analisam esses dados para prever falhas mecânicas antes que elas ocorram), entre outros.

As aplicações de IA, muitas vezes, envolvem a coleta e o processamento de grandes volumes de dados pessoais, incluindo dados de localização, de comportamento do usuário e de preferências no geral. Contudo, isso leva a preocupações significativas de privacidade, especialmente quando os dados são usados para criar perfis detalhados dos indivíduos. A partir disso, surgem questionamentos sobre quais boas práticas podem ser adotadas para minimizar os riscos advindos do uso de IA, que ainda não foram mapeadas por completo, até mesmo em razão dos rápidos avanços tecnológicos nessa área.

Exemplo

Os sistemas de IA vêm sendo usados em aeroportos para monitorar e otimizar o fluxo de passageiros, gerenciando os canais de atendimento e reduzindo o tempo nas filas. Por meio de câmeras inteligentes posicionadas estrategicamente nas áreas de maior circulação de passageiros, como balcões de check-in e pontos de controle de segurança, são capturadas imagens em tempo real. Essas imagens são transformadas em dados quantitativos pela IA, os quais são utilizados, por exemplo, para determinar o tempo que o passageiro leva desde a entrada na fila do check-in até a finalização do processo. A IA é capaz de identificar padrões de movimento e comportamento dos passageiros, permitindo uma análise precisa do fluxo e das possíveis causas de atrasos. Uma vez que as imagens são

Seção 2 - LGPD aplicada ao setor de Transportes

Exemplo

processadas, a IA calcula o tempo de espera e envia os dados em tempo real para companhias aéreas e autoridades aeroportuárias. Assim, é possível tomar decisões imediatas para redistribuir recursos (pessoal ou equipamentos), abrir ou fechar mais guichês de atendimento e redirecionar passageiros para áreas menos congestionadas, melhorando a eficiência operacional. Nos dias e horários de pico, as companhias aéreas podem antecipar necessidades e reforçar equipes para melhorar a eficiência e rapidez no atendimento. Como as companhias aéreas recebem somente os dados processados, sem qualquer identificação visual dos passageiros, e não acessam as imagens capturadas, que são processadas pelo software de uma empresa terceira, o tratamento de dados pelas companhias aéreas observa o princípio da minimização.

Boas práticas de proteção de dados para uso de inteligência artificial (IA)

- **Minimização:** Coletar apenas os dados estritamente necessários para a finalidade específica. Por exemplo, se o objetivo é melhorar a eficiência do combustível, coletar somente os dados relativos ao desempenho do motor e consumo de combustível. Por outro lado, se a finalidade é otimizar rotas, não é necessário coletar dados sobre as preferências pessoais dos usuários.

- **Transparência:** Informar claramente os titulares como os dados serão utilizados. As empresas devem disponibilizar políticas de privacidade acessíveis e fáceis de entender, detalhando os tipos de dados coletados para treinamento e uso de sistemas de IA e finalidades específicas.

- **Segurança:** Implementar protocolos robustos de segurança (criptografia, firewalls, sistemas de detecção de intrusões e autenticação de múltiplos fatores) para proteção das bases de dados utilizadas em sistemas de IA.

- **Análises de risco:** Elaborar relatórios de impacto à proteção de dados pessoais para avaliar e mitigar riscos associados ao uso de IA. Esses relatórios devem identificar os riscos potenciais e detalhar as medidas adotadas para mitigá-los. Por fim, devem ser revisados periodicamente para refletir novas ameaças e mudanças nas operações.

Reconhecimento Biométrico

O reconhecimento facial e outras formas de biometria são comumente usadas para controle de acesso (como verificação de identidade para acesso a áreas restritas), segurança (como monitoramento de áreas públicas para identificar indivíduos procurados e prevenir crimes) e eficiência (como facilitar processos de check-in e de embarque). Contudo, dados biométricos são considerados dados sensíveis no âmbito da LGPD, especialmente porque são únicos, não podem ser alterados e seu eventual uso inadequado tem o potencial de resultar em violações graves de privacidade e potencial discriminação.

Seção 2 - LGPD aplicada ao setor de Transportes

Exemplo

Em aeroportos, o reconhecimento facial é usado no processo de check-in automatizado e embarque. Por meio dele, é realizada uma comparação da imagem capturada com a foto do passaporte ou documento de identidade. Isso acelera o processo de embarque e aumenta a segurança, prevenindo eventuais fraudes de identidade. Há situações em que o reconhecimento facial é utilizado para monitorar áreas restritas do aeroporto, garantindo que apenas pessoas autorizadas tenham acesso a elas.

Boas práticas de proteção de dados para uso de reconhecimento biométrico

- **Teste de Balanceamento e Avaliação de Impacto:** Antes de adotar sistemas biométricos, elaborar Teste de Balanceamento e Relatório de Impacto à Proteção de Dados para identificar riscos específicos associados ao uso da tecnologia e adotar medidas para mitigá-los.
- **Consentimento:** Sempre que possível, garantir que a coleta de biometria seja voluntária, bem como fornecer informações compreensíveis sobre como os dados serão utilizados, permitindo que os indivíduos optem por alternativas, quando possível.
- **Segurança:** Adotar medidas de segurança (como criptografia) para proteger os dados.
- **Transparência:** Informar os titulares sobre como os dados serão coletados, armazenados e utilizados, disponibilizando informações detalhadas sobre a finalidade do uso de biometria e as medidas de proteção adotadas.
- **Limitação de Acesso:** Implementar políticas de controle de acesso que garantam que apenas colaboradores treinados e autorizados possam acessar os dados biométricos.

Veículos Autônomos

Veículos autônomos estão revolucionando os meios de transporte tradicionais, pois prometem maior eficiência e segurança. Eles utilizam sensores, câmeras e sistemas de IA para navegar e tomar decisões em tempo real. Para isso, coletam uma vasta quantidade de dados, incluindo imagens, vídeos, dados de localização e padrões de comportamento dos motoristas. No entanto, a potencial centralização e compartilhamento dos dados levantam questões de privacidade e proteção de dados.

Os veículos autônomos começaram a ser utilizados (i) no transporte de cargas, para aumentar a eficiência em rotas pré-definidas, (ii) no transporte de passageiros e (iii) para fins de manutenção e inspeção, por exemplo, trens autônomos que monitoram e ajustam automaticamente a velocidade e paradas, melhorando a eficiência e segurança e reduzindo erros humanos. Por exemplo, em caso de obstáculos na via, o sistema pode desacelerar ou parar o trem automaticamente para evitar acidentes.

Seção 2 - LGPD aplicada ao setor de Transportes

Boas práticas de proteção de dados para uso de carros autônomos

- **Anonimização:** Sempre que possível, implementar técnicas de anonimização para proteger a identidade dos indivíduos (passageiros e motoristas).
- **Segurança:** Assegurar que os dados coletados sejam armazenados de forma segura e fiquem acessíveis apenas para pessoas autorizadas. Recomenda-se utilizar criptografia para proteger dados em trânsito e em repouso.
- **Retenção:** Definir e seguir políticas claras sobre a retenção e descarte de dados, estabelecendo prazos para tal retenção e procedimentos para a exclusão segura de dados desnecessários.
- **Revisão:** Monitorar e revisar continuamente os sistemas para garantir a conformidade com a privacidade e segurança, implementando auditorias regulares e avaliações de segurança para identificar e corrigir vulnerabilidades.

Drones

Os drones estão sendo utilizados para diferentes funções no setor de transportes, o que inclui a entrega de pacotes (transporte rápido e eficiente de encomendas), inspeção de infraestrutura (monitoramento e inspeção de portos, ferrovias, rodovias, estações, edifícios e outras infraestruturas) e o monitoramento de tráfego (observação e gestão do tráfego em áreas urbanas e rodovias). Como eles podem capturar imagens e vídeos de áreas amplas, na maioria das vezes sem o consentimento ou o conhecimento das pessoas filmadas, a sua utilização levanta preocupações de privacidade e proteção de dados.

Exemplo

Em portos, drones costumam ser utilizados para inspecionar navios e infraestruturas, identificando rapidamente danos ou necessidade de reparos. Eles também monitoram o tráfego marítimo e auxiliam na navegação, aumentando a segurança e eficiência das operações portuárias. Por exemplo, eles podem capturar imagens aéreas detalhadas de navios para detectar corrosão ou danos estruturais.

Boas práticas de proteção de dados para uso de drones

- **Avisos:** Informar os indivíduos sobre o uso de drones e as áreas onde eles operam, utilizando sinais e comunicações públicas visíveis, afixadas nos locais de maior circulação, para garantir que todos que possam vir a ser filmados pelos drones estejam cientes da sua utilização.
- **Segurança:** Garantir que as gravações e dados coletados pelos drones sejam armazenados de forma segura, utilizando, sempre que possível, criptografia para proteger dados capturados e implementando controles de acesso rigorosos.

Seção 2 - LGPD aplicada ao setor de Transportes

- **Políticas de Uso:** Desenvolver e implementar políticas claras sobre o uso de drones e a gestão dos dados coletados, estabelecendo diretrizes sobre (i) quando e onde os drones poderão ser usados e (ii) como os dados serão tratados.

- **RIPD:** Elaborar um Relatório de Impacto à Proteção de Dados (RIPD) para avaliar eventuais riscos específicos associados ao uso dos drones e mitigar eventuais impactos negativos.

Ferramentas de Monitoramento de Frota e de Carga

Ferramentas de monitoramento de frota e de carga são comumente utilizadas para rastreamento de localização (monitoramento em tempo real da localização dos veículos e cargas), eficiência do combustível (análise do consumo de combustível para otimização do uso do veículo) e condição dos veículos (como o monitoramento contínuo do desempenho dos motores e outros componentes). O objetivo central é otimizar as operações e melhorar a segurança. No entanto, esse monitoramento constante pode ser percebido como invasivo por motoristas e outros colaboradores, além de levantar questões sobre a extensão e o uso dos dados coletados.

Exemplo

Empresas de logística utilizam sistemas de monitoramento para rastrear a localização e a condição das cargas em tempo real. Sensores nos veículos fornecem dados sobre o consumo de combustível, o desempenho do motor e o comportamento do motorista, permitindo ajustes imediatos para otimizar a operação. Por exemplo, se um sensor indicar que um caminhão está consumindo mais combustível do que o esperado, a empresa pode investigar e corrigir o problema rapidamente.

Boas práticas de proteção de dados para uso de Ferramentas de Monitoramento

- **Transparência:** Informar os motoristas e demais colaboradores impactados sobre quais dados são coletados e como eles serão usados, disponibilizando, em local de fácil acesso, políticas de privacidade internas que expliquem claramente as práticas de monitoramento.

- **Segurança:** Proteger os dados pessoais coletados contra acessos não autorizados, por meio de criptografia e outras medidas de segurança, a fim de proteger dados em trânsito e repouso.

- **Minimização:** Implementar políticas internas para garantir que apenas os dados estritamente necessários para a finalidade específica de monitoramento de frota e cargas sejam coletados.

- **RIPD:** Elaborar um Relatório de Impacto à Proteção de Dados (RIPD) para avaliar e mitigar riscos específicos associados ao uso dessa tecnologia e adotar medidas para mitigá-los.

- **Retenção:** Definir e seguir políticas claras sobre a retenção e descarte de dados, estabelecendo prazos para tal retenção e procedimentos para a exclusão segura de dados desnecessários.

Seção 2 - LGPD aplicada ao setor de Transportes

Empresa de aluguel de motos é multada pela autoridade francesa de proteção de dados por coletar dados de geolocalização excessivos [24]

A autoridade francesa de proteção de dados (CNIL) multou a empresa de aluguel de motos City Scott em 125 mil euros pela coleta excessiva de dados de geolocalização. A empresa coletava a geolocalização das motos a cada 30 segundos e guardava registros das jornadas dos clientes por diversos motivos: infrações de trânsito; reclamações de clientes; suporte ao usuário; e gestão de sinistros e roubos. A CNIL considerou que nenhuma das finalidades justifica a coleta dos dados de forma tão pormenorizada como a realizada pela empresa. A prática foi considerada intrusiva na vida privada dos titulares, na medida em que é suscetível de revelar seus movimentos, locais frequentados e paradas feitas durante uma viagem. Para a CNIL, a empresa poderia oferecer um serviço idêntico sem coletar dados de geolocalização dos clientes de forma quase permanente. A empresa não respeitou, portanto, o princípio da minimização dos dados e, por isso, foi multada.

A adoção de novas tecnologias no setor de transportes tem o potencial de trazer inúmeros benefícios, mas apresenta desafios significativos em termos de privacidade e de proteção de dados. Por isso, é fundamental que as empresas do setor implementem boas práticas e salvaguardas adequadas para mitigar os riscos associados. Assim, a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a adesão às diretrizes da LGPD são passos fundamentais para garantir a conformidade e proteger os direitos dos indivíduos.

Ao seguirem as boas práticas no uso de novas tecnologias, as empresas do setor de transportes podem não apenas melhorar suas operações e serviços, mas também fortalecer a confiança dos clientes e colaboradores na gestão de seus dados pessoais, mesmo quando relacionadas a tecnologias emergentes.

Boas práticas de proteção de dados para adoção de novas tecnologias no setor de Transportes

1. Avaliação Inicial

- **Identificação:** Descrever a nova tecnologia que será adotada e suas funcionalidades.
- **Finalidade:** Definir claramente a finalidade da implementação da tecnologia.
- **Impacto:** Avaliar como a tecnologia afetará as operações diárias e a eficiência do negócio.

2. Conformidade Legal

- **Legislação:** Verificar a conformidade com a LGPD e outras legislações aplicáveis.
- **Consultoria:** Consultar especialistas em proteção de dados para garantir a conformidade.

3. Relatório de Impacto à Proteção de Dados (RIPD)

- **RIPD:** Conduzir uma avaliação de impacto para identificar riscos e mitigar impactos.

- Para atividades que utilizem a base legal da prevenção à fraude e segurança do titular (art. 11, II, “g”), elaborar um teste de balanceamento, que pode ser concomitante com o RIPD.

24 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047346903?isSuggest=true

Seção 2 - LGPD aplicada ao setor de Transportes

Boas práticas de proteção de dados para adoção de novas tecnologias no setor de Transportes

- **Documentação:** Documentar os riscos identificados e as medidas de mitigação propostas.

4. Controle e Transparência

- **Política de Privacidade:** Criar políticas de privacidade que expliquem o tratamento de dados pessoais realizado por meio da nova tecnologia.
- **Consentimento:** Caso necessário, desenvolver mecanismos para obtenção do consentimento.
- **Comunicação:** Informar usuários e colaboradores sobre a implementação da nova tecnologia, suas finalidades e como os dados pessoais serão utilizados.

5. Segurança de Dados

- **Criptografia:** Implementar criptografia para proteger dados em trânsito e em repouso.
- **Controles de Acesso:** Estabelecer controles rigorosos para que somente pessoas autorizadas acessem os dados.
- **Auditorias:** Realizar auditorias de segurança regularmente para corrigir vulnerabilidades.

6. Minimização de Dados

- **Coleta:** Coletar apenas os dados necessários para a finalidade específica da tecnologia.
- **Retenção:** Definir políticas de retenção e descarte de dados, com prazos e procedimentos para a exclusão segura de dados desnecessários.

7. Treinamento e Sensibilização

- **Capacitação Interna:** Treinar colaboradores sobre as novas tecnologias e as melhores práticas de privacidade e proteção de dados.
- **Conscientização:** Promover a conscientização contínua sobre a importância da privacidade e segurança de dados através de workshops e campanhas internas.

8. Monitoramento e Revisão

- **Revisão:** Monitorar continuamente o uso da tecnologia e revisar as políticas de privacidade e de segurança regularmente para garantir a conformidade contínua.
- **Auditorias:** Realizar auditorias regulares para garantir que as medidas de proteção de dados estejam sendo seguidas corretamente.

9. Gestão de Incidentes

- **Plano de Resposta:** Desenvolver e implementar plano de resposta a incidentes para lidar com possíveis violações de dados pessoais.
- **Notificação:** Estabelecer procedimentos para notificar todas as partes afetadas e autoridades competentes em caso de incidentes de segurança confirmados envolvendo dados pessoais

Seção 2 - LGPD aplicada ao setor de Transportes

8. BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS

As pequenas e médias empresas (PMEs) do setor de transportes desempenham um papel crucial na economia brasileira. No entanto, sua conformidade com a LGPD pode ser um desafio devido aos recursos limitados à sua disposição. Este tópico apresenta diretrizes específicas e práticas recomendadas para as PMEs com base na regulamentação da ANPD, visando facilitar a sua conformidade com a LGPD.

Por meio da Resolução CD/ANPD nº 02/2022, a ANPD regulamentou a aplicação da LGPD para agentes de tratamento de pequeno porte (ATTPs), com várias flexibilizações e dispensas de obrigações da LGPD. Os agentes de tratamento de pequeno porte incluem as microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que tratam dados, assumindo as obrigações típicas de controlador ou operador (art. 2º, I, da Resolução CD/ANPD nº 2/2022).

Contudo, não podem se beneficiar do tratamento jurídico diferenciado previsto na Resolução CD/ANPD nº 2/2022 os ATTPs que (i) realizem tratamento de alto risco para os titulares, (ii) aufiram receita bruta superior ao limite legal para microempresas e empresas de pequeno porte na Lei Complementar nº 123/2006 ou para startups na Lei Complementar nº 182/2021, ou (iii) pertençam a grupo econômico de fato ou de direito, cuja receita global também ultrapasse estes limites (art. 3º da Resolução CD/ANPD nº 2/2022).

O que é um tratamento de alto risco? (art. 4º da Resolução CD/ANPD nº 2/2022)

O tratamento de alto risco é aquele que atende cumulativamente a pelo menos um critério geral e um critério específico abaixo.

Etapa 1 - Critérios Gerais

- Tratamento de dados em larga escala, ou seja, que abrange número significativo de titulares, considerando o volume de dados envolvidos e a duração, a frequência e extensão geográfica do tratamento realizado; ou

- Tratamento de dados que possa afetar significativamente interesses e direitos fundamentais dos titulares, isto é, quando a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

>>

Seção 2 - LGPD aplicada ao setor de Transportes

Etapa 2 - Critérios Específicos

- Uso de tecnologias emergentes ou inovadoras;
- Vigilância e/ou controle de zonas acessíveis ao público, isto é, os espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus, metrô e trem, aeroportos, portos, bibliotecas públicas, dentre outros;
- Decisões tomadas unicamente com base em tratamento automatizado de dados, inclusive as destinadas a definir o perfil pessoal, profissional, de saúde, consumo e crédito ou os aspectos da personalidade do titular; ou
- Utilização de dados sensíveis ou de dados pessoais de crianças, adolescentes e idosos.

Exemplos

Uma empresa de transporte ferroviário adotou um sistema avançado de vigilância e controle de passageiros em suas principais estações e trens. O sistema usa câmeras de alta resolução e tecnologias emergentes de reconhecimento facial para monitorar o fluxo de passageiros, detectar comportamentos suspeitos e identificar indivíduos com mandados de prisão ou outras restrições legais. As câmeras estão posicionadas em zonas acessíveis ao público, como as plataformas de embarque, salas de espera e dentro dos vagões, capturando imagens de milhares de passageiros diariamente. As informações coletadas são processadas por algoritmos de IA que tomam decisões automatizadas sobre alertas de segurança, sem intervenção humana. Além disso, o sistema coleta dados sensíveis, incluindo características biométricas, para garantir a precisão da identificação. Esta atividade de tratamento pode ser considerada de alto risco, pois envolve o tratamento em larga escala, o uso de tecnologias emergentes, vigilância de zonas públicas e decisões automatizadas, além do tratamento de dados sensíveis, que pode afetar significativamente os direitos fundamentais dos titulares.

Uma empresa de transporte rodoviário de cargas usa um sistema de monitoramento e controle em tempo real para acompanhar a localização e a condição de suas frotas e motoristas. Esse sistema envolve a instalação de sensores e de câmeras dentro dos caminhões e nos centros de distribuição, além de dispositivos GPS nos veículos. Os dados coletados incluem informações de localização, vídeos do interior da cabine, biometria dos motoristas, e dados sensíveis relacionados à saúde, como os sinais de fadiga e uso de substâncias proibidas. A empresa utiliza um sistema automatizado de análise de dados que avalia o comportamento dos motoristas, tomando decisões sobre pausas obrigatórias, alertas de segurança e desativação automática do veículo em caso de emergências. O monitoramento abrange uma vasta extensão geográfica, cobrindo várias regiões do país, e opera continuamente. Este tratamento de dados pode ser considerado de alto risco, pois envolve tratamento em larga escala, uso de tecnologias emergentes e vigilância de zonas públicas, decisões automatizadas e o uso de dados sensíveis, incluindo biometria e informações de saúde dos motoristas.

Seção 2 - LGPD aplicada ao setor de Transportes

Caso a empresa se enquadre na definição de ATTP, ela pode usufruir das dispensas e flexibilidades regulatórias concedidas pela ANPD na Resolução CD/ANPD nº 2/2022 de forma a facilitar a sua conformidade com a LGPD. A dispensa ou flexibilização das obrigações não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, incluindo bases legais, princípios e direitos do titular, bem como outras disposições legais, regulamentares e contratuais relativas à proteção de dados pessoais.

Quais são as dispensas e flexibilizações concedidas aos agentes de pequeno porte?

- **Encarregado:** É dispensada a indicação obrigatória de um encarregado de dados, mas a sua indicação será considerada política de boas práticas. Ainda assim, deve ser disponibilizado o canal de comunicação com o titular para atender as solicitações e as reclamações de titulares (art. 11, Resolução CD/ANPD nº 2/2022).
- **Comunicação de incidentes:** O prazo para comunicação de incidentes de segurança à ANPD e aos titulares será contado em dobro, totalizando 6 (seis) dias úteis contados da data em que o controlador tomou conhecimento de que o incidente afetou dados pessoais (art. 6º, § 8º e 9º, § 6º, da Resolução CD/ANPD nº 15/2024, conforme art. 10 da Resolução CD/ANPD nº 2/2022).
- **Prazos diferenciados:** Os agentes de pequeno porte podem usufruir de prazo em dobro nas seguintes circunstâncias: (i) no atendimento de solicitações dos titulares, (ii) no fornecimento de declaração clara e completa do art. 19, II, da LGPD, (iii) na comunicação de incidentes de segurança à ANPD e aos titulares, e (vi) prazos estabelecidos em normativos próprios para apresentação de informações, documentos, relatórios e registros solicitados pela ANPD (art. 14 da Resolução CD/ANPD nº 2/2022). Ainda, os agentes de pequeno porte podem fornecer a declaração simplificada do art. 19, I, da LGPD no prazo de até quinze dias contados da data do requerimento do titular (art. 15 da Resolução CD/ANPD nº 2/2022).
- **RoPA:** A elaboração e manutenção do registro de operações de tratamento de dados pode ser realizada de forma simplificada, no modelo disponibilizado pela ANPD (art. 9º da Resolução CD/ANPD nº 2/2022).[25]
- **Segurança:** Agentes de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer tipo de tratamento inadequado ou ilícito (art. 13 da Resolução CD/ANPD nº 2/2022).
- **Direitos do titular:** Os agentes de pequeno porte devem disponibilizar informações sobre o tratamento de dados e atender às requisições dos titulares em conformidade com os arts. 9º e 18 da LGPD, por meio eletrônico, impresso ou qualquer outro que assegure os direitos da LGPD e o acesso facilitado às informações pelos titulares (art. 7º da Resolução CD/ANPD nº 2/2022). Ainda, podem se organizar em entidades de representação de atividade empresarial, para negociar, mediar ou conciliar reclamações apresentadas por titulares de dados (art. 8º da Resolução CD/ANPD nº 2/2022).

25 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/modelo_de_ropa_para_atpp.pdf

Seção 2 - LGPD aplicada ao setor de Transportes

Ainda em relação ao tema de segurança e boas práticas, a ANPD publicou Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte,[26] com medidas práticas e simplificadas que podem ser adotadas para garantir a proteção de dados. Além disso, publicou também um checklist de medidas de segurança para ATTPs.

Checklist de medidas de segurança para agentes de tratamento de pequeno porte [27]

Política de Segurança da Informação

- ☐ Estabelecer uma política de segurança da informação simplificada, indicando controles relacionados ao tratamento de dados, como cópias de segurança, uso de senhas, acesso e compartilhamento, atualização de softwares, uso de correio eletrônico e uso de antivírus.
- ☐ Realizar revisões periódicas da política de segurança da informação.
- ☐ Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados.

Conscientização e Treinamento

- ☐ Realizar a conscientização dos colaboradores, com treinamentos e campanhas a respeito de obrigações e responsabilidades relacionadas ao tratamento de dados.
- ☐ Informar e sensibilizar os colaboradores da organização, em especial aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.
- ☐ Informar os colaboradores sobre como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; evitar de se tornarem vítimas de incidentes de segurança corriqueiros, como contaminação por vírus ou ataques de phishing, que podem ocorrer ao clicar em links recebidos em pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail; manter documentos físicos com dados pessoais em gavetas e não em cima das mesas; não compartilhar logins e senhas de acesso das estações de trabalho; bloquear computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros; seguir as orientações da política de segurança da informação.
- ☐ Criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto colaboradores, a informar incidentes e vulnerabilidades detectadas.

26 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf
27 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf

Seção 2 - LGPD aplicada ao setor de Transportes

Checklist de medidas de segurança para agentes de tratamento de pequeno porte[27]

Gerenciamento de contratos

- ☐ Estabelecer contratos com cláusulas de segurança da informação com o fim de assegurar a proteção de dados, com regras para fornecedores e parceiros, sobre compartilhamentos, relações entre controlador-operador, e orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com orientações do controlador.
- ☐ Assinar termos de confidencialidade (NDA) com todos os colaboradores da empresa.

Controles de acesso

- ☐ Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e acessar dados.
- ☐ Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade.
- ☐ Implementar um adequado gerenciamento de senhas, estabelecendo controles para evitar o uso de senhas padrão fornecidas por fornecedores de software ou hardware adquiridos; utilizar apenas senhas complexas para acessar sistemas; e não reutilizar senhas.
- ☐ Proibir o compartilhamento de contas ou de senhas entre colaboradores.
- ☐ Aplicar o princípio do menor privilégio (need to know). Utilizar a autenticação multi-fator para acessar sistemas ou base de dados pessoais.
- ☐ Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores).

Segurança dos dados pessoais armazenados

- ☐ Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados.
- ☐ Implementar soluções de pseudonimização, como a criptografia, para cifrar dados.
- ☐ Orientar os colaboradores a não desativarem ou ignorarem configurações de segurança nas estações de trabalho.
- ☐ Evitar a transferência de dados pessoais das estações de trabalho para os dispositivos de armazenamento externo, como pen drives e discos rígidos

Seção 2 - LGPD aplicada ao setor de Transportes

- ☐ Inventariar e cifrar dados de dispositivos externos e armazená-los em locais seguros.
- ☐ Realizar backups offline, periódicos e armazená-los de forma segura.
- ☐ Formatar e sobrescrever mídias físicas com dados pessoais antes de descartá-las. Quando não for possível a sobrescrita, destruir as mídias físicas.
- ☐ Estabelecer, no contrato de serviço, o registro da destruição/descarte (caso utilize serviços de terceiros para o descarte).

Segurança nas comunicações

- ☐ Utilizar conexões cifradas (TLS/HTTPS) ou os aplicativos com criptografia ponta-a-ponta para serviços de comunicação.
- ☐ Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF).
- ☐ Proteger e-mails adotando ferramentas anti spam, filtros de e-mail, e integrar o antivírus ao sistema de e-mail.
- ☐ Remover quaisquer dados pessoais ou sensíveis desnecessariamente disponibilizados em redes públicas.

Gerenciamento de vulnerabilidades

- ☐ Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores).
- ☐ Adotar e atualizar periodicamente softwares antivírus e antimalwares.
- ☐ Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

Dispositivos móveis

- ☐ Utilizar técnicas de autenticação multi-fator para controlar o acesso a dispositivos móveis (como smartphones e laptops).
- ☐ Separar os dispositivos móveis de uso privado daqueles de uso institucional, se possível.
- ☐ Implementar funcionalidades que permitam apagar remotamente os dados armazenados em dispositivos móveis (especialmente para casos de roubo ou furto dos dispositivos).

Serviços em nuvem

- ☐ Firmar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados.
- ☐ Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os requisitos de segurança da informação estabelecidos neste checklist.

Seção 2 - LGPD aplicada ao setor de Transportes

- ☐ Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado.
- ☐ Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relativos a dados pessoais

A conformidade com a LGPD é essencial para a proteção dos direitos dos titulares de dados e para a construção de um ambiente de negócios seguro e confiável. Pequenas e médias empresas do setor de transportes devem adotar medidas práticas e eficientes para garantir a proteção de dados, seguindo sempre as orientações da ANPD. A implementação das boas práticas contribui significativamente para a conformidade com a LGPD e para a mitigação dos riscos associados ao tratamento de dados pessoais.

Boas práticas no dia a dia das PMEs

Para manter a conformidade com a LGPD de forma contínua, pequenas empresas podem adotar as seguintes boas práticas no dia a dia.

- **Educação Contínua:** Promover treinamentos regulares sobre privacidade e proteção de dados aos colaboradores e mantê-los atualizados com base em novas ameaças e melhores práticas. Incentivar uma cultura de segurança da informação dentro da empresa.
- **Documentação e Registro:** Manter registros detalhados de todas as operações de tratamento. Documentar as medidas de segurança implementadas e incidentes de segurança ocorridos.
- **Revisão de Contratos:** Revisar regularmente os contratos com fornecedores e parceiros para garantir que existam cláusulas de proteção de dados adequadas, que abordem questões como responsabilidade pelo tratamento de dados, medidas de segurança, e a obrigação de notificar incidentes de segurança. Garantir que os fornecedores e parceiros estejam em conformidade com a LGPD.
- **Solicitações de Titulares:** Disponibilizar um canal de comunicação acessível para os titulares exercerem os seus direitos. Estabelecer procedimentos claros para responder às solicitações de titulares de forma rápida e eficiente, documentando as solicitações e respostas fornecidas.
- **Novos Projetos:** Incorporar considerações de privacidade e proteção de dados desde a etapa de desenvolvimento de novos projetos e serviços (privacy by design). Realizar avaliações de impacto à proteção de dados para novos processos que envolvam tratamento de dados pessoais e possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Documentar os resultados das avaliações e as medidas de mitigação adotadas.
- **Monitoramento e Revisão:** Monitorar continuamente as operações de tratamento de dados e revisar políticas de privacidade e de segurança da informação periodicamente, com base nas mudanças legislativas e melhores práticas, além de realizar auditorias internas regularmente, para garantir a conformidade contínua com a LGPD.

Seção 2 - LGPD aplicada ao setor de Transportes

9. ELEMENTOS DE CONFORMIDADE DE ENTIDADES REPRESENTATIVAS DO SETOR DE TRANSPORTES

As relações *business-to-business* (B2B) no setor de transporte, isto é, interações entre pessoas jurídicas, diferem-se significativamente das relações *business-to-consumer* (B2C), em que empresas do setor de transporte lidam diretamente com passageiros ou consumidores finais. Ambas possuem suas complexidades específicas, em especial quanto à finalidade de tratamento dos dados pessoais.

Entidades representativas do setor de transportes, como confederações, federações, sindicatos e associações também tratam dados pessoais para realizar as suas atividades de representação de interesses coletivos de trabalhadores ou empregadores. A nível nacional, existem confederações que abrangem diversas federações, que, por sua vez, são compostas por sindicatos locais ou regionais. Tais entidades podem tratar dados de representados, empregados, parceiros, prestadores de serviços e outros terceiros, para atender exigências contratuais e obrigações legais ou regulatórias (como previdenciárias e trabalhistas).

Exemplos de atividades de tratamento de dados por entidades representativas

Uma associação de transportadores rodoviários coleta dados pessoais dos membros para fins de registro e comunicação. Estes dados incluem nome, endereço, e-mail, número de telefone e CPF dos proprietários de empresas de transporte. Ainda, a associação realiza pesquisas de satisfação e avaliações de desempenho, coletando informações a respeito das operações das empresas e as suas necessidades. Esses dados são utilizados para enviar newsletters, informar sobre mudanças regulatórias e ainda organizar eventos e treinamentos específicos para o setor. Em alguns casos, a associação também coleta dados sensíveis, como as informações de saúde dos motoristas, para oferecer programas de bem-estar e de saúde ocupacional. O tratamento desses dados permite à associação melhorar os serviços prestados aos membros e garantir que eles estejam atualizados e bem-informados sobre as melhores práticas e novidades do setor.

Uma federação de transportadores aquaviários coleta dados pessoais e sensíveis de associados para coordenar a participação em programas de certificação e qualificação profissional. Para isso, a federação coleta dados pessoais, como nome, data de nascimento, histórico de emprego, e dados biométricos, incluindo impressões digitais e fotografias. Esses dados são necessários para garantir a autenticidade dos certificados emitidos e a segurança dos processos de qualificação. A federação também usa dados de localização dos navios e informações das cargas para monitorar as operações e fornecer relatórios de desempenho. O

Seção 2 - LGPD aplicada ao setor de Transportes

Exemplos de atividades de tratamento de dados por entidades representativas

tratamento desses dados é essencial para assegurar que transportadores aquaviários atendam aos requisitos regulatórios e de segurança, melhorando a eficiência e a confiança no setor.

Um sindicado dos trabalhadores ferroviários coleta e trata dados pessoais e sensíveis dos seus associados para defender os seus direitos trabalhistas e oferecer suporte jurídico. Entre os dados coletados estão nome, endereço, número de telefone, CPF, dados de emprego (cargo e salário), e dados de saúde, incluindo atestados médicos e informações a respeito de acidentes de trabalho. O sindicato usa esses dados para negociar acordos coletivos, acompanhar processos trabalhistas e fornecer assistência jurídica em casos de disputas com empregadores. Ainda, o sindicato coleta informações sobre a participação dos associados em greves e manifestações, garantindo que seus direitos sejam respeitados. O tratamento dos dados é essencial para a atuação eficaz do sindicato na proteção e promoção dos interesses dos trabalhadores ferroviários.

As diretrizes internas das entidades representativas devem estabelecer regras claras sobre o tratamento de dados de titulares que é responsável, priorizando a proteção desses dados em todos os processos.

Medidas de conformidade à LGPD recomendadas para entidades representativas

- **Mapeamento de Dados (art. 37, LGPD):** Realizar uma pesquisa inicial para mapear o fluxo de dados nos processos de tratamento, identificando onde os dados são armazenados, quem os acessa e com quem são compartilhados. Isso auxilia na categorização dos riscos e na definição de ações.

- **Avaliação de Riscos e Implementação:** Analisar os procedimentos necessários para adequar o tratamento de dados pessoais às diretrizes da LGPD. Revisar e atualizar cláusulas contratuais para mitigar riscos relacionados à terceirização e compartilhamento de dados.

- **Educação e Sensibilização:** Elaborar documentos orientativos sobre práticas de proteção de dados e guias específicos para diferentes funções e necessidades, incluindo procedimentos de segurança da informação.

- **Descarte de Dados (art. 15, LGPD):** Garantir que os dados sejam descartados de acordo com procedimentos internos da equipe de TI, conforme a LGPD, quando eles não forem mais necessários para o cumprimento de obrigações legais ou regulatórias.

Seção 2 - LGPD aplicada ao setor de Transportes

As entidades representativas devem implementar um comitê de crise corporativo, composto por áreas multidisciplinares, para gerenciar eventuais incidentes de segurança que possam ocorrer. É crucial monitorar acessos ao ambiente digital e físico dos bancos de dados para prevenir acessos indevidos. Sistemas de logs devem ser mantidos para garantir a rastreabilidade dos acessos. Além disso, é necessário implementar recursos técnicos de segurança da informação adequados à natureza dos dados e ao risco de incidentes.

As entidades devem ter conhecimento sobre quem controla ou tem acesso a dados pessoais, sejam colaboradores, filiados ou terceiros. Realizar testes periódicos de segurança nos bancos de dados e treinar colaboradores com acesso a informações confidenciais é uma prática recomendada.

O compartilhamento de dados, especialmente no cumprimento de obrigações legais como eSocial, DIRF, RAIS, comunicação de acidentes de trabalho e pagamentos de FGTS e benefícios, deve sempre se basear em um fundamento legal. Contratos de trabalho devem incluir cláusulas específicas sobre o dever de confidencialidade.

No caso de compartilhamento de dados biométricos para fins de registro e apuração de ponto, quando o processamento for terceirizado, é necessário especificar no contrato com a empresa terceirizada as responsabilidades de gestão e assegurar que a empresa terceirizada cumpra a LGPD.

Principais etapas para adequação de entidades representativas à LGPD

1. Mapeamento e Registro de Dados (art. 37, LGPD): O primeiro passo é realizar um mapeamento detalhado das atividades de tratamento de dados, identificando quais dados são coletados, como são armazenados, por quanto tempo são mantidos e com quem são compartilhados. Isso inclui os dados de associados, colaboradores e fornecedores. Um exemplo prático seria um sindicato de motoristas que coleta dados pessoais de seus membros para fins de filiação, benefícios e comunicação. Os dados devem ser registrados em um documento de Registro das Operações de Tratamento de Dados Pessoais (ROT ou RoPA).

2. Medidas de Segurança (arts. 46 e 49, LGPD): Adotar medidas técnicas e administrativas de segurança é essencial para proteger os dados pessoais contra acessos não autorizados, perdas ou vazamentos. Isso inclui a utilização de criptografia, controles de acesso e políticas de senha. Por exemplo, uma associação que gerencia uma base de dados de associados deve garantir que apenas pessoal autorizado tenha acesso às informações e todo compartilhamento seja criptografado.

3. Treinamento e Conscientização: Realizar treinamentos regulares sobre proteção de dados

Seção 2 - LGPD aplicada ao setor de Transportes

Principais etapas para adequação de entidades representativas à LGPD

para todos os colaboradores é crucial para garantir que eles entendam suas responsabilidades e as melhores práticas para proteger os dados pessoais. Um exemplo seria uma confederação de transportadores que organiza workshops periódicos para educar os seus colaboradores sobre a importância da LGPD e como implementar medidas de segurança no dia a dia.

4. Atendimento aos Direitos dos Titulares (art. 18, LGPD): As entidades devem estar preparadas para atender às solicitações dos titulares, como os pedidos de acesso, correção, exclusão e portabilidade de dados. Para isso, deve-se estabelecer canais de comunicação claros e eficientes. Por exemplo, um sindicato pode criar um portal online específico onde seus membros possam facilmente enviar solicitações relacionadas aos seus dados pessoais.

5. Designação de um Encarregado de Proteção de Dados (art. 41, LGPD): Nomear um encarregado de proteção de dados (DPO) é medida importante para garantir a conformidade contínua com a LGPD. O encarregado será responsável por monitorar as práticas de tratamento de dados, responder a consultas dos titulares e comunicar-se com a ANPD. Por exemplo, uma associação nacional de transportadores pode designar o encarregado para supervisionar a conformidade de todas as suas filiais regionais.

6. Auditorias e Avaliações de Risco: Realizar auditorias regulares e avaliações de risco ajuda a identificar possíveis vulnerabilidades e garantir que as medidas de proteção de dados sejam eficazes. Um exemplo seria uma federação de transportadores que contrata uma empresa de auditoria externa para revisar suas práticas de proteção de dados anualmente e recomendar possíveis melhorias.

Anexo 1 - Arcabouço Normativo

A LGPD é uma legislação geral e ampla, aplicável a todos os setores que realizam o tratamento de dados pessoais. O seu propósito não é introduzir normas granulares e específicas que endurecem minuciosamente todas as atividades de tratamento de dados do setor ou abordar todas as suas particularidades, mas sim fornecer um conjunto de diretrizes adaptáveis a diversas realidades e situações.

Reconhecendo a importância de interpretar normas gerais à luz das especificidades do setor de transporte, este Guia de Boas Práticas busca ilustrar como as regras da LGPD podem ser efetivamente aplicadas. Essa perspectiva é valiosa não apenas para as empresas de transporte, mas também órgãos reguladores e autoridades públicas, que se beneficiarão de uma visão setorial do tema.

Por isso, é essencial estar atento às normas setoriais que preveem regras específicas para o tratamento de dados pessoais no setor de transportes, para além da LGPD. Abaixo, encontram-se listadas normas e atos normativos setoriais aplicáveis ao setor de transporte, incluindo normas de agências reguladoras e órgãos públicos. Apesar de não ser exaustiva, a lista apresenta as principais normas aplicáveis ao setor no tema de proteção de dados.

Leis e Decretos Federais

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

Lei nº 3.268, de 30 de setembro de 1957, que dispõe sobre os Conselhos de Medicina, e dá outras providências.

Lei nº 5.433, de 8 de maio de 1968, que regula a microfilmagem de documentos oficiais e dá outras providências.

Lei nº 8.036, de 11 de maio de 1990, que dispõe sobre o Fundo de Garantia do Tempo de Serviço, e dá outras providências.

Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.

Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor e dá outras providências, instituindo o Código de Defesa do Consumidor.

Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

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

Social.

Lei nº. 9.503, de 23 de setembro de 1997, que institui o Código de Trânsito Brasileiro.

Lei nº 9.528, de 10 de dezembro de 1997, que altera dispositivos das Leis nºs 8.212 e 8.213, ambas de 24 de julho de 1991, e dá outras providências.

Lei nº 9.307, de 23 de setembro de 1996, que dispõe sobre a arbitragem.

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

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

Decreto nº 3.048, de 6 de maio de 1999, que aprova o Regulamento da Previdência Social, e dá outras providências.

Decreto nº 4.480, de 17 de setembro de 2003, que regulamenta a Medida Provisória no 130, de 17 de setembro de 2003, que dispõe sobre a autorização para desconto de prestações em folha de pagamento, e dá outras providências.

Lei nº 10.820, de 17 de dezembro de 2003, que dispõe sobre a autorização para desconto de prestações em folha de pagamento, e dá outras providências.

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.

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.

Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

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

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 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, instituindo o Marco Civil da Internet.

Decreto nº. 8.373, de 11 de dezembro de 2014, que institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (e-Social).

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 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

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.

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

Lei Complementar nº 182, de 1º de junho de 2021, que institui o marco legal das startups e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006.

Decreto nº 10.854, de 10 de novembro de 2021, que regulamenta disposições relativas à legislação trabalhista e institui o Programa Permanente de Consolidação, Simplificação e Desburocratização de Normas Trabalhistas Infralegais e o Prêmio Nacional Trabalhista, e altera o Decreto nº 9.580, de 22 de novembro de 2018.

Lei nº 14.553, de 20 de abril de 2023, que altera os arts. 39 e 49 da Lei nº 12.288, de 20 de julho de 2010 (Estatuto da Igualdade Racial), para determinar procedimentos e critérios de coleta de informações relativas à distribuição dos segmentos étnicos e raciais no mercado de trabalho.

Lei nº 14.611, de 3 de julho de 2023, que dispõe sobre igualdade salarial e de critérios remuneratórios entre mulheres e homens.

Decreto nº 11.795, de 23 de novembro de 2023, que regulamenta a Lei nº 14.611, de 3 de julho de 2023, que dispõe sobre igualdade salarial e de critérios remuneratórios entre mulheres e homens.

Lei nº 10.209, de 23 de março de 2001, que institui o Vale-Pedágio obrigatório sobre o transporte rodoviário de carga e dá outras providências.

Lei nº 14.599, de 19 de junho de 2023 que posterga a exigência do exame toxicológico periódico para obtenção e renovação da Carteira Nacional de Habilitação; e altera a Lei nº 9.503, de 23 de setembro de 1997 (Código de Trânsito Brasileiro), a Lei nº 11.442, de 5 de janeiro de 2007, para dispor sobre seguro de cargas, e a Lei nº 11.539, de 8 de novembro de 2007, para dispor sobre a carreira de Analista de Infraestrutura e o cargo isolado de Especialista em Infraestrutura Sênior.

Decreto nº 11.527, de 16 de maio de 2023, que altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011.

Decreto nº 68.155, de 09 de dezembro de 2023, que regulamenta a Lei federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas.

Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Resoluções e Portarias da Agência Nacional de Aviação Civil (ANAC)

Resolução nº 255, de 13 de novembro de 2012, que estabelece regras sobre a disponibilização de Informações Antecipadas sobre Passageiros (API) e do Registro de Identificação de Passageiros (PNR).

RPAC 120/ANAC - Regulamento Brasileiro da Aviação Civil - Programa de prevenção do risco associado ao uso indevido de substâncias psicoativas na aviação civil.

Resolução nº 595, de novembro de 2020, que altera a Resolução nº 255, de 13 de novembro de 2012.

Resoluções e Portarias 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. 3.106, 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 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.

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 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.

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.

Portaria nº 14.167/ASTEC, de 21 de março de 2024, que aprova Norma Complementar nº 9 que disciplina o uso compartilhado de dados pessoais entre a Agência Nacional de Aviação Civil e outros entes.

Resoluções e Portarias da Agência Nacional de Transportes Terrestres (ANTT)

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.

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. 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. 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. 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. 5.063, 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. 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.

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 5.982 de 23 de junho de 2022, que regulamenta procedimentos para inscrição e manutenção no Registro Nacional de Transportadores Rodoviários de Cargas - RNTRC, e dá outras providências.

Resoluções e Portarias da Autoridade Nacional de Proteção de Dados (ANPD)

Resolução CD/ANPD nº 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, que aprova o Regulamento de aplicação da Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

Enunciado CD/ANPD nº 1, de 22 de maio de 2023, que edita o enunciado sobre o tratamento de dados pessoais de crianças e adolescentes.

Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.

Outras Normativas

Portaria nº 3.214, de 08 de junho de 1978, que aprova as Normas Regulamentadoras - NR - do Capítulo V, Título II, da Consolidação das Leis do Trabalho, relativas à Segurança e Medicina do Trabalho.

Lei Complementar nº 709, de 14 de janeiro de 1993, do Estado de São Paulo.

Decreto nº 41.865, de 16 de junho de 1997, do Estado de São Paulo, que dispõe sobre a declaração de bens dos agentes públicos estaduais, bem como de bens e valores patrimoniais do cônjuge ou companheiro, dos filhos e de outras pessoas que vivam sob a dependência econômica do declarante, e estabelece normas relativas à declaração pública de bens das autoridades e dirigentes que especifica.

Lei nº 10.294, de 20 de abril de 1999, do Estado de São Paulo.

Resolução do Conselho Federal de Medicina 1658, de 2002, que normatiza a emissão de atestados médicos e dá outras providências.

Lei nº 13.541, de 24 de março de 2003, da cidade de São Paulo, que dispõe sobre a colocação de placa informativa sobre filmagem de ambientes, e dá outras providências.

Decreto nº 43.236, de 22 de maio de 2003, da cidade de São Paulo, que regulamenta a Lei nº 13.541, de 24 de março de 2003, que determina a colocação de placas informativas sobre filmagem de ambientes.

Ato Declaratório Executivo COANA/COTEC nº 2, de 26 de setembro de 2003, que especifica os requisitos técnicos, formais e prazos para implantação de sistema informatizado de controle aduaneiro domiciliar e de recintos alfandegados ou autorizados a operar com mercadorias sob controle aduaneiro.

Decreto nº 48.897, de 27 de agosto de 2004, do Estado de São Paulo, que dispõe sobre os Arquivos Públicos, os documentos de arquivo e sua gestão, os Planos de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo, define normas para a avaliação, guarda e eliminação de documentos de arquivo.

Decreto nº 48.898, de 27 de agosto de 2004, do Estado de São Paulo, que aprova o Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo.

Decreto nº 52.205, de 27 de setembro de 2007, do Estado de São Paulo, que institui, no âmbito da Administração Direta e Indireta do Estado de São Paulo, o Cadastro Unificado de Fornecedores do Estado de São Paulo - CAUFESP, gerido pela Secretaria da Fazenda, em conformidade com os artigos 34 a 37 da Lei federal nº 8.666, de 21 de junho de 1993, e com os artigos 31 a 34 da Lei estadual nº 6.544, de 22 de novembro de 1989, que se regerá pelo regulamento, ora aprovado, anexo a este decreto.

Decreto nº 52.624, de 15 de janeiro de 2008, do Estado de São Paulo, que dispõe sobre a criação do Banco de Informações Referentes a Pessoal, Reflexos e Encargos Sociais do Estado.

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.

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.

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. 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.

Decreto nº 58.052, de 16 de maio de 2012, do Estado de São Paulo, que regulamenta a Lei federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas

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. 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.

Decreto nº 60.812, de 30 de setembro de 2014, do Estado de São Paulo, que reorganiza a Secretaria da Fazenda e dá providências correlatas.

Instruções nº 01, de 07 de abril de 2016, do Tribunal de Contas do Estado de São Paulo, no que concerne a Repasses Públicos ao Primeiro e Terceiro Setor, revoga as Instruções Consolidadas nºs 01/2008 e 02/2008, bem como, as Instruções nº 01/2015 deste Tribunal.

Lei Estadual do Estado de São Paulo nº 16.758, de 08 de junho de 2018, que torna obrigatória a informação sobre cor ou identificação racial em todos os cadastros, bancos de dados e registros de informações assemelhados, públicos e privados, no Estado e dá providências correlatas.

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).

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.

Resolução Secretaria do Governo do Estado de São Paulo - SG-52, de 13 de setembro de 2019, que altera a Resolução SG-16, de 03 de maio de 2019, que estabelece a obrigatoriedade de parecer prévio do Comitê Gestor do Gasto Público nas contratações de serviços, ou de fornecimento de equipamentos, de tecnologia da informação.

Decreto nº 64.790, de 13 de fevereiro de 2020, do Estado de São Paulo, que institui a Central de Dados do Estado de São Paulo - CDESP, a Plataforma Única de Acesso - PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, e dá providências correlatas.

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.

Resolução SG-8, de 2 de setembro de 2020, do Estado de São Paulo, que estabelece normas complementares para aplicação do Decreto 64.790/2020.

Resolução nº 53, de 04 de setembro de 2020, da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS), que dispõe acerca da consolidação e atualização das Resoluções da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, conforme normas do Código Internacional para a Proteção de Navios e Instalações Portuárias (Código ISPS, da sigla em inglês).

Instruções nº 01, de 22 de setembro de 2020, do Tribunal de Contas do Estado de São Paulo.

Decreto nº 65.347, de 09 de dezembro de 2020, do Estado de São Paulo, que dispõe sobre a aplicação da Lei federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no âmbito do Estado de São Paulo

Portaria nº 671, de 8 de novembro de 2021, do Ministério do Trabalho e Emprego, que regulamenta disposições relativas à legislação trabalhista, à inspeção do trabalho, às políticas públicas e às relações de trabalho.

Portaria nº 672, de 8 novembro de 2021, do Ministério do Trabalho e Emprego, que disciplina os procedimentos, programas e condições de segurança e saúde no trabalho e dá outras providências.

Portaria MTE nº 612, de 25 de abril de 2024, que altera a Portaria MTP nº 672, de 8 de novembro de 2021, para regulamentar a aplicação dos exames toxicológicos por motoristas profissionais.

Resolução Contran nº 923, de 28 de março de 2022, Dispõe sobre o exame toxicológico de larga janela de detecção, em amostra queratínica, para a habilitação, renovação ou mudança para as categorias C, D e E, decorrente da Lei nº 13.103, de 02 de março de 2015.

Resolução Contran 1009, de 24 de abril de 2024, que altera as Resoluções Contran nº 789, de 18 de junho de 2020, e nº 923, de 28 de março de 2022 e nº 985, de 15 de dezembro de 2022.

Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, do Estado de São Paulo, que institui a Política de Proteção de Dados Pessoais – PPDP no âmbito da Administração Pública Estadual e dá providências correlatas.

Decreto nº 66.421, de 3 de janeiro de 2022, do Estado de São Paulo, que dispõe sobre a comprovação de vacinação contra a COVID-19 por parte dos agentes públicos que especifica e dá providências correlatas.

Portaria nº 143, de 18 de fevereiro de 2022, da Receita Federal do Brasil, que estabelece normas gerais e procedimentos para o alfandegamento de local ou recinto.

Resolução CVM nº 80, de 29 de março de 2022, que traz exigências informacionais relacionadas a riscos e oportunidades climáticas, ambientais, de diversidade e de governança que devem ser reportadas pelas Companhias Abertas no Formulário de Referência (FRE).

Portaria nº. 167, de 14 de abril de 2022, da Receita Federal do Brasil, que autoriza o Serviço Federal de Processamento de Dados a disponibilizar acesso, para terceiros, dos dados e informações que especifica.

Portaria Coana nº 72, de 12 de abril de 2022, da Receita Federal do Brasil, que especifica os requisitos técnicos, formais e de segurança para registro e armazenamento de informações em sistema informatizado de controle aduaneiro (SICA) e o envio de eventos à Application Programming Interface Recintos (API-Recintos) do Portal Único de Comércio Exterior no Sistema Integrado de Comércio Exterior (Portal Siscomex) pelos intervenientes que operam em locais ou recintos alfandegados ou autorizados a operar com mercadorias sob controle aduaneiro.

Portaria nº 1486, de 3 de junho de 2022, do Ministério do Trabalho e Emprego, que altera a Portaria nº 671, de 8 de novembro de 2021, que regulamenta disposições relativas à legislação trabalhista, à inspeção do trabalho, às políticas públicas e às relações de trabalho.

Portaria nº 3.714, de 24 de novembro de 2023, do Ministério do Trabalho e Emprego, que regulamenta o Decreto nº 11.795, de 23 de novembro de 2023, que dispõe sobre a igualdade salarial e de critérios remuneratórios entre mulheres e homens, em especial o

Relatório de Transparência Salarial e de Critérios Remuneratórios, o Plano de Ação para Mitigação da Desigualdade Salarial e Critérios Remuneratórios,protocolo de fiscalização contra a discriminação salarial e de critérios remuneratórios entre mulheres e homens e a disponibilização de canais específicos para denúncias de discriminação salarial.

Portaria 612 do Ministério do Trabalho e Emprego de 25/04/2024 que altera a Portaria MTP 672/2021 para regulamentar a aplicação dos exames Toxicológicos para os motoristas profissionais empregados do transporte rodoviário de cargas e de passageiros de que trata a Lei 13.103/15.

Resolução CONTRAN nº 923, de 28/03/2022 que dispõe sobre o exame toxicológico de larga janela de detecção, em amostra queratínica, para a habilitação, renovação ou mudança para as categorias C, D e E, decorrente da Lei nº 13.103, de 02 de março de 2015.

Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, do Estado de São Paulo, que institui a Política de Governança de Dados e Informações – PGDI, no âmbito da Administração Pública Estadual, e dá providências correlatas.

CNT / SEST SENAT / ITL
Sistema Transporte

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

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

LGPD
TRANSPARÊNCIA E SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS