



GUIA

MELHORES PRÁTICAS
PARA APLICAÇÃO DA

LEI GERAL
DE PROTEÇÃO
DE DADOS

LGPD



Prepare-se para a aplicação da Lei Geral de Proteção de Dados - LGPD

Pensando em ajudar as Associações de Marca, suas Redes de Concessionárias filiadas, assim como nossos Regionais e SINCODIV's a se preparar para a aplicação da LGPD – Lei Geral de Proteção de Dados, prevista para entrar em vigor em agosto de 2020, a FENABRAVE contratou a empresa Peck Sleiman Edu, e as dras. Patrícia Peck e Cristina Sleiman para elaborar esse Guia de Melhores Práticas para a Aplicação dessa nova legislação que, certamente, irá exigir muita adaptação e ações eficazes para evitar transtornos, seja junto aos nossos clientes como à Autoridade Nacional, que regulamentará a Lei.

Seja como Controladores ou Operadores de dados, sejam esses compartilhados ou não, consentidos ou que entrem na regra de exceção, devemos ter um Plano de Ações que vise obedecer a LGPD que tem, basicamente, três pilares fundamentais: **Transparência, Privacidade e Segurança.**

Todos deveremos começar já ou o quanto antes, a trabalhar nas adaptações necessárias, principalmente, considerando que temos, em nossos cadastros de clientes, o que este Guia chama de “legado”, que são os dados que já coletamos, de nossos clientes, fornecedores e colaboradores, mas que precisam ser atualizados, mediante consentimento de seus titulares.

Espero que esse material sirva como um verdadeiro Guia, que é o seu propósito, e que cada Associação de Marca, Concessionária, Regional FENABRAVE ou SINCODIV possam seguir, passo a passo, o que orientam as especialistas contratadas, de forma a implantar os processos necessários para o cumprimento da LGPD.

Portanto, peço que compartilhem esse material com seus associados e que informem que o Guia poderá ser impresso e reproduzido, como melhor entenderem. Para isso, o arquivo já está no formato adequado para impressão. Além disso, esse Guia também estará disponível para acesso online, no portal da FENABRAVE.

A FENABRAVE E FENACODIV lhes desejam uma ótima leitura desse Guia e sucesso na implantação da LGPD!

***Alarico Assumpção Júnior
Presidente da FENABRAVE/FENACODIV***

DISCLAIMERS: A FENABRAVE informa que esse Guia de Melhores Práticas para a Aplicação da LGPD- Lei Geral de Proteção de Dados é um trabalho contratado pela Federação e desenvolvido pela empresa Peck Sleiman Edu, e pelas dras. Patrícia Peck e Cristina Sleiman. O conteúdo deste Guia não expressa, obrigatoriamente, a opinião da FENABRAVE, ficando a critério de cada leitor considerar e utilizar as informações, nele contidas, conforme seu entendimento próprio. Desta forma, não nos responsabilizamos por quaisquer informações e dados que, porventura, possam vir a ser questionados.

Sumário

Introdução à LGPD:.....	6
1.1 Principais Conceitos.....	7
Dado Pessoal.....	7
Dado Pessoal Sensível	8
Dado Anonimizado.....	8
Titular	8
Controlador.....	9
Operador	9
Encarregado (DPO).....	10
Tratamento	10
Agentes de Tratamento	10
Anonimização	10
Relatório de Impacto à Proteção de Dados Pessoais (DPIA)	10
Exemplo:.....	11
1.2 Princípios	12
Finalidade	12
Adequação	12
Necessidade.....	12
Livre Acesso.....	13
Qualidade dos Dados	13
Transparência	13
Segurança	14
Prevenção	15
Não discriminação	15
Responsabilização e Prestação de Contas	15
2. Desafios do Comercial, Cobrança, Rh e Compras	16
3. Por onde começar - Primeiros Passos para a Conformidade.....	22
4. Primeiros passos para atender à Autoridade Nacional de Proteção de Dados Pessoais	30
5. Tempo de armazenamento	32
6. ANEXO I - Perguntas e Respostas	34
1. Quem são os titulares de dados, no universo automobilístico?.....	34
2. Quem tem acesso, aos dados pessoais, na empresa?	35
3. Qual o valor dos dados dos meus clientes? Por que preciso protegê-los?	36
4. Relação Controlador e Operador no Setor (Montadora, Distribuidor, Concessionária, Financeira, Seguradora);.....	37
5. Por que é importante saber a Finalidade da Coleta dos Dados Pessoais?	39
6. Por que é importante saber se há compartilhamento de dados pessoais com outras empresas?	44
7. Smart e IA – Dados capturados na interação dos veículos com usuários e Smart Cities – desafios para a Conformidade.....	45
8. Quais são as bases de dados que podem ser utilizadas, de forma livre, sem o pedido de Consentimento?	46
9. A quem pertencem os dados?	47
10. CRM e DMS – Como trabalhar a integração das Bases de Dados de Concessionárias e Montadoras.....	49
11. Segurança interna e câmeras de vídeo-vigilância e o Legítimo Interesse.....	51
12. Relatório de Impacto de Proteção de Dados Pessoais - RIPP.....	53
13. Quais as peculiaridades no tratamento de dados pessoais no B2B e B2C?	54
14. Como adequar a Política de Privacidade - Roteiro	55
15. Se não atender à Conformidade da Lei 13.709/18, quais as consequências?.....	56
16. Quais são os direitos dos titulares de dados e por que conhecê-los?	58
17. Quem é o Encarregado pela Proteção de Dados Pessoais - DPO?.....	59
18. O que é o dever de Report?	60
19. Como manter a Segurança da Informação na Proteção de Dados Pessoais.....	62
20. A LGPD aplica-se apenas à Coleta e Armazenamento em ambiente eletrônico?.....	63
7. ANEXO II - Fichas e Cadastros	64
8. ANEXO III – O QUE NÃO PODE FALTAR NO RELATÓRIO DE IMPACTO	67

01

INTRODUÇÃO À LGPD:

A proteção dos dados pessoais não é um tema recente. Ao contrário, é um assunto em evolução, dentro do espectro jurídico, especialmente, no rol das garantias fundamentais dos direitos humanos, devido ao aumento da importância do uso das informações dos indivíduos, no contexto da Sociedade Digital.

Na abordagem sobre a proteção dos dados pessoais, deve-se levar em consideração ao menos 3 aspectos: o da **transparência**, o da **privacidade** e o da **segurança**.

No Brasil, a privacidade já é um direito fundamental, garantido pela Constituição Federal Brasileira, de 1988, sendo tão importante que, caso haja qualquer violação, é cabível indenização, por dano material ou moral.

Além disso, no sistema legal brasileiro, há uma série de leis que, de algum modo, trazem alguns dos aspectos relacionados à proteção de dados pessoais, seja no Código de Defesa do Consumidor, no Decreto do Comércio Eletrônico ou no Marco Civil da Internet.

A necessidade de fortalecer, com regulamentações mais rigorosas, a proteção dos dados pessoais, em diversos países, veio como resultado, direto, do aumento dos incidentes de vazamento de dados, bem como, também, da discussão sobre os limites de uso das informações das pessoas e da necessidade de haver um maior empoderamento dos titulares dos dados, no processo de controle e eliminação de suas informações.



Neste contexto o Brasil, assim como outros países, seguindo a liderança da União Europeia, a fim de continuar a fomentar um ambiente de negócios saudável e seguro, com regras claras sobre tratamento de dados pessoais, implementou uma legislação específica.

Surge, então, a Lei Geral de Proteção de Dados Pessoais - Lei 13.709 de 2018, como primeiro grande marco regulatório sobre o tema no país – com previsão de entrar em vigor em agosto de 2020, caso não ocorra nenhuma prorrogação, mediante Projeto de Lei.

A LGPD aplica-se em qualquer operação, de Tratamento de Dados Pessoais, realizada por pessoa natural ou jurídica, de direito público ou privado.

Em relação à sua aplicação territorial, podemos considerar as seguintes hipóteses:

- Operação de tratamento realizada no Brasil;
- Oferta de produtos, bens ou serviços, ou o tratamento de dados pessoais, realizado no Brasil;
- Dados pessoais que tenham sido coletados no Brasil.

1.1 Principais Conceitos

Para implementação de qualquer projeto e, principalmente, para a sua aplicação, em um setor específico, como o automobilístico, é preciso conhecer os principais conceitos, trazidos pelo Art. 5 da Lei 13.709/2018, conforme veremos a seguir:



Dado Pessoal

Informação relacionada à pessoa natural, identificada ou identificável. O termo “identificável” significa que sempre que uma informação permitir identificar um titular/pessoa, ainda que seja agregada a outra informação, essa informação será considerada um **Dado Pessoal**.

Exemplo: Nome, RG, CPF, E-mail, Telefone, Endereço, Placa de Veículo, Número de Matrícula, Número de O.S e Número do Cliente, quando forem relativos à pessoa física, chassis. Até mesmo o Número de uma Proposta, quando tornar o cliente identificável, será considerado **Dado Pessoal**.

Dado Pessoal Sensível

O **Dado Pessoal Sensível** é o Dado Pessoal relacionado à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização, de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Exemplo: Ficha de Saúde, Atestado Médico, Declaração de Tipo Sangüíneo, Declaração de Religião, Formulário de Cotas (Estudantil), Ficha para Seleção de Funcionário (Cota Especial).

Atenção aos Cadastros, nos quais são solicitadas informações como: Sexo, Origem Racial, Afiliação a Congregações Religiosas ou, mesmo, Dados Relacionados à Saúde.

Dado Anonimizado

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Exemplo: Dados estatísticos, apenas inseridos em Relatório de Vendas, referentes aos dias ou períodos, sem identificação de clientes, ou mesmo do vendedor, como movimentação do showroom, por calor, onde se identifica o fluxo da loja, mas não identifica, individualmente, as pessoas.

Um outro exemplo de **Dado Anonimizado** é a identificação, por relatório, sobre o setor de vendas mais visitado, quando coletado de forma sem identificar o titular, como por sensores de movimento ou de calor.

Titular

Pessoa natural/Física a quem se referem os dados pessoais, que são objeto de tratamento. Todos nós somos titulares de dados.

Exemplo: Cliente, Visitante, Candidato à Vaga, Funcionário, Terceirizado (Pessoa Física que Trabalha no Prestador/ Pessoa Jurídica), Acionista (que Consta de Contrato Social).

Controlador

Pessoa natural/física ou jurídica, de direito público ou privado, a quem competem as decisões, referentes ao tratamento, dos dados pessoais.

Exemplo: Empresa Empregadora, que Captura Dados do Cliente, ou ainda, de Seleção de Pessoal, que captura dados de candidato.

A Concessionária, ao coletar dados de funcionários e clientes; Montadoras ao coletar, em relação direta, dados de funcionários, terceirizados ou clientes; ou mesmo a Financeira e a Seguradora, uma vez que o tratamento de dados não é feito em nome da Concessionária.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais, em nome do controlador. É o caso das empresas dentro do próprio ecossistema, que, por força da relação jurídica, promove o tratamento de dados em nome de quem a contratou.

Exemplo: Empresa prestadora de serviços terceirizados, que executa tratamento mediante ordens (limitado), como é o caso de uma empresa de courier, de serviços de TI, agências de mídias digitais, de marketing, despachantes, entre outras.

Para melhor exemplificar a **diferença** entre **Controlador** e **Operador**, do ponto de vista do ecossistema automobilístico, utilizaremos a **Financeira** e a **Seguradora**, que são ambas **Controladoras**, uma vez que atuam mediante contrato direto com o titular/cliente, ainda que seja por intermédio de uma concessionária.

Já o **Despachante** é um **Operador**, pois o titular/cliente não o contrata separadamente. Normalmente, as concessionárias embutem este serviço na venda.

Observamos que o Artigo 41 cita, apenas, o **Controlador**, por tratar do dever de deixar o contato do **DPO** (encarregado pela proteção de dados pessoais) divulgado no site. Isso se deve ao fato de que cabe ao **Controlador** o dever de reportar, à autoridade, e receber requisições de titulares/clients sobre o tratamento de seus dados. Lembre-se de que mesmo um **Operador** acaba sendo **Controlador** de dados, quando se refere a seus próprios funcionários e acionistas, ou a seus fornecedores.

Em resumo, no geral, em algum momento, a instituição acaba tendo posição de um **Controlador**.

Encarregado (DPO)

Pessoa indicada, pelo **Controlador e Operador** (art. 50, VIII), para atuar, como canal de comunicação, entre o Controlador, os titulares dos dados/pessoas e a Autoridade Nacional de Proteção de Dados (**ANPD**).

Exemplo: Pode ser pessoa, interna ou externa, física ou jurídica, ou mesmo um comitê, responsável por executar várias funções para atender aos titulares dos dados, à autoridade, responder por incidentes de vazamentos de dados, implementar o programa de proteção de dados pessoais e cumprir com o dever de reportá-los.

Tratamento

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração dos dados.

Exemplo: O mero armazenamento de dados pessoais é um tipo de tratamento, por isso, alcança o legado (arquivo).

Agentes de Tratamento

São considerados Agentes de Tratamento o **Controlador e o Operador**.

Anonimização

Utilização de meios técnicos razoáveis e disponíveis, no momento do tratamento de dados, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Exemplo: Em uma Base de Dados, onde conste apenas o resultado final das vendas, sem identificação do comprador, como nos tipos de Relatórios de Veículos Vendidos, mas que não identificam a placa desses veículos, nem o nome ou CPF dos compradores.

Relatório de Impacto à Proteção de Dados Pessoais (DPIA)

Documentação do Controlador, que contém a descrição dos

processos de tratamento de dados pessoais, que podem gerar riscos às liberdades civis e aos direitos fundamentais do cidadão/titular, bem como medidas, salvaguardas e mecanismos de mitigação de risco.



Exemplo:

Toda vez que houver Tratamento de Dados Pessoais Sensíveis, ou a base legal que justifique o tratamento de dados pessoais for o legítimo interesse, poderá ser exigida, pela ANPD, a apresentação do Relatório de Impacto.

Isso ocorre, por exemplo, no uso de tecnologias disruptivas, onde possa ser questionado o risco à privacidade, como ocorre em algumas soluções, que utilizam reconhecimento facial, uso de Score, algoritmos de inteligência artificial, entre outros.

Ao elaborar um **DPIA (Relatório de Impacto à Proteção de Dados Pessoais)** devemos garantir que, no mínimo, estejam presentes:

- A natureza, escopo, contexto e finalidade do tratamento;
- Avaliação da necessidade, proporcionalidade e Medidas de Compliance;
- Identificação e Assessment dos Riscos aos titulares de dados;
- Identificação das medidas para mitigar esses riscos.

1.2 Princípios

Conhecer os princípios da LGPD é um requisito para que o Tratamento de Dados Pessoais seja considerado de boa-fé, segundo o caput do artigo 6º. da Lei, que prevê o seguinte:



Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular/pessoa, sem possibilidade de tratamento posterior, de forma incompatível com essas finalidades. **Isso quer dizer que é fundamental deixar claro para quais finalidades serão tratados os dados.** Essas finalidades devem ser informadas ao titular dos dados, de forma específica e explícita. Ou seja, **pela Lei da LGPD, um dos princípios mais importantes é o da transparência.** Por isso, só podem ser tratados dados para finalidades que foram informadas, previamente, de forma explícita (não implícita) ao titular dos dados, e que seja evitado o tratamento para finalidades ocultas, que gerem surpresa ou sejam novidade para o titular.

Pode até haver uma mudança de finalidade futura, mas ela deverá ser, igualmente, informada para toda a base de titulares de dados, sem esquecer da solicitação de consentimento, quando necessário.

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Assim, deve haver consistência entre o que foi informado ao titular e o real uso que se faz do dado pessoal, atendendo a uma proporcionalidade.

Necessidade

Limitação do tratamento do dado, ao mínimo necessário, para a realização das finalidades legítimas, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Não se pode, por exemplo, exigir a coleta e uso de dados de religião para a compra de um veículo, pois a coleta desse dado foge ao objetivo principal do negócio e não é necessário.

Livre Acesso

Garantia, aos titulares dos dados, à consulta facilitada e gratuita sobre a forma e duração do tratamento de seus dados, bem como sobre a integralidade dos mesmos. No entanto, a exemplo da liberdade de expressão, com base no Art. 19, pode-se constatar que este não é um princípio absoluto, ou seja, pode haver limitações ao seu cumprimento.

Por exemplo, quando o tratamento tiver origem no consentimento do titular ou estiver em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial dos agentes de tratamento, nos termos de regulamentação específica da Autoridade Nacional.

O direito ao exercício do livre acesso, e confirmação de existência, de tratamento deverá ser atendido pelo agente de tratamento, no prazo máximo de 15 dias, contados a partir da data do requerimento do titular. No entanto, a Autoridade Nacional poderá dispor de prazo diferenciado, para setores específicos.

É muito importante se esforçar para demonstrar o empenho do **Controlador**, na tentativa de comprovar a real identidade do solicitante, atentando-se para eventuais fraudes.

Qualidade dos Dados

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Portanto, facilitar o acesso, forma de correção e atualização dos dados, ao titular, será imprescindível. Este princípio permite, às instituições, manter as bases de dados pessoais atualizadas e, inclusive, promover o enriquecimento da informação, com a justificativa de não gerar uma situação de tratamento equivocado (como enviar uma mensagem para um contato ou endereço desatualizado).

Transparência

A transparência é a garantia, dada aos titulares, em fornecer informações claras, precisas, e, facilmente, acessíveis sobre a realização do tratamento de seus dados, e os respectivos agentes deste tratamento, neste caso, também observados os segredos comercial e industrial.

A regulação ou orientação específica, da autoridade regulatória, sobre qual será o nível de transparência exigido e/ou como ele pode ser atingido, de forma satisfatória, depende da criação da ANPD.

O princípio da transparência poderá ser exercido por meio de uma Política de Privacidade e Proteção de Dados Pessoais, por disclaimers (notificações), contratos e por outras formas de comunicação com o titular dos dados.

Pelo princípio da transparência, ainda que certos dados sejam coletados com base em exigência legal, ou qualquer hipótese que dispense o consentimento, será necessário informar, ao seu titular, as informações detalhadas sobre o tratamento pretendido para seus dados.

É importante destacar que a comunicação com o titular deverá ser, sempre, pautada na clareza e objetividade, sendo de responsabilidade do **Controlador** a demonstração de que disponibilizou, ao titular, todas as informações, antes da coleta de qualquer dado pessoal.

Segurança

O princípio da Segurança pressupõe a utilização de medidas técnicas e administrativas, aptas a proteger os dados pessoais, de acessos não autorizados e de situações accidentais ou ilícitas, de destruição, perda, alteração, comunicação ou difusão. Portanto, está, diretamente, ligado ao tema **Segurança da Informação (SI)**.

Ocorre que a Lei não especifica os requisitos de Segurança e, tendo em vista que a ANPD ainda está em processo de formação, não há direcionamento, até o presente momento. No entanto, a ANPD poderá, no futuro, dirimir as dúvidas ou regulamentar questões específicas de Segurança.

O dever de segurança foi instituído nos Art. 46 e 47, sendo obrigação do **Controlador, Operador** e, também, de qualquer pessoa que tenha contato com dados pessoais. Por isso, a capacitação das equipes pode ser um verdadeiro diferencial.

Justamente, por não terem sido disponibilizados requisitos específicos, é de suma importância seguir padrões mundiais de Segurança da Informação, conforme ISO/IEC 27001 e 27002, bem como a ISO 27701:2019.

Prevenção

Adoção de medidas para prevenir a ocorrência de danos, em virtude do tratamento de dados pessoais. Este princípio está relacionado à capacidade de identificar potenciais riscos e aplicação de medidas para prevenir que tais riscos possam se materializar.

Na ocorrência de qualquer incidente, será muito importante que o agente comprove os meios aplicados para prevenção e que não tem, apenas, uma política voltada à reação, a fim de evitar potenciais danos aos titulares de dados pessoais. Além disso, é uma forma de demonstrar sua boa-fé.

Não discriminação

A LGPD é clara quanto à impossibilidade de realização do tratamento de dados para fins discriminatórios, ilícitos ou abusivos. Portanto, não poderá promover o tratamento sempre que este puder causar dano ao titular, por discriminação.

Deve-se ter muito cuidado com a aplicação deste princípio, visto que, até mesmo em uma situação onde há uma definição de locais de entrega de mercadoria, por seleção de CEP ou Bairro, isso pode levar a uma interpretação de uso de dados pessoais com característica discriminatória. Por isso, é importante a instituição estar respaldada, com justificativas que esclareçam que o tratamento de dados pessoais não possui características que gerem este tipo de desvio. Isso toma maior importância nas soluções que envolvem algum tipo de algoritmo de Score, situação em que podem ser solicitados os atributos ou fatores combinatórios, até o limite em que isso não exponha segredo de negócios.

Responsabilização e Prestação de Contas

Em termos práticos, trata-se da demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

02

DESAFIOS DO COMERCIAL, COBRANÇA, RH E COMPRAS



Por certo que a LGPD é, e será, um grande desafio de implementação e, também, de continuidade da conformidade, tendo em vista que as ações protetivas e preventivas deverão ser, permanentemente, atualizadas.

No setor automobilístico, especialmente, nas concessionárias de veículos, é importante destacar quatro áreas relevantes, as quais tratam um volume expressivo de dados pessoais: **Comercial, Cobrança, Recursos Humanos e Compras.**

Para a **Área Comercial**, destaca-se, principalmente, o atendimento na ponta, ou seja, a venda direta para o consumidor. Nesse caso, recomenda-se cuidado com detalhes que, às vezes, podem passar despercebidos como, por exemplo, a coleta de informações e documentos do comprador (pessoa física), com os quais o vendedor tem acesso e contato, e que podem envolver Imposto de Renda, CPF, RG, Comprovante de Endereço, Número de Celular, WhatsApp, entre outras informações exigidas.

Vale lembrar que **a placa do veículo também é um dado pessoal**. É comum que vendedores recebam cartões dos clientes, onde constam nome, sobrenome e número de telefone pessoal, assim como fiquem de posse dos dados constantes na ficha cadastral. Logo, essa é uma fonte de entrada de dados pessoais que precisa ser muito bem tratada, para estar em conformidade com a nova legislação, tanto no sentido de atender aos princípios apontados, quanto, principalmente, para prevenir e evitar

vazamentos de informações que são o tipo de incidente cujo impacto, da violação, é o que gera as multas maiores pelas Autoridades. Logo no primeiro contato com o cliente, que é o titular dos dados pessoais, esse deverá ser informado sobre todas as finalidades, para as quais seus dados pessoais serão tratados. Se possível, já coletar o consentimento no padrão novo da LGPD, na primeira ficha, que é preenchida e assinada (seja ela física, em papel, ou digital, em um aplicativo).

O comercial também lida com bases de dados pessoais, oriundas de outras fontes, para geração de leads, sejam de parceiros ou mesmo de fontes públicas, como a Internet. É importante dizer que a Lei permite o uso dessas informações, mas é preciso que sejam de fontes legítimas, e para as quais o titular tenha consentido o compartilhamento dos seus dados pessoais, com terceiros, em alguma política de privacidade.

Um bom exemplo é se o titular dos dados tiver participado de um evento, como um Feirão de Automóveis, e visitado um estande, para o qual forneceu seus dados. Se tiver preenchido alguma ficha, que já o avisava e coletava seu consentimento para compartilhamento de seus dados, vinculados às finalidades informadas, então, não haverá problema.

É preciso ficar atento a situações semelhantes, pois, nem toda base disponível ou acessível é legítima, ou seja, pode ter sido coletada em desacordo com a legislação em vigor. E, às vezes, pode ter sido coletada de forma lícita, mas, não significa que esteja disponível para tratamento por terceiros. É importante buscar, sempre, por fontes confiáveis, pois não compensa arriscar utilizar dados, sem saber sua precedência, tendo em vista as sanções previstas na Lei.

Para a **Área de Cobrança**, destaca-se que, além de **Dados Pessoais**, por vezes, utilizam-se **Dados Pessoais Sensíveis** (como ocorre com a autenticação, e verificação biométrica, ou a análise de reconhecimento facial) e, muito embora possam ser tratados como exceção de consentimento, conforme as bases legais, previstas na LGPD, com a finalidade de proteção do crédito de prevenção à fraude, será necessário atender ao princípio da transparência, ou seja, informar, ao titular, para que os dados, que estão sendo coletados, serão usados. Esses avisos legais, prévios, são conhecidos

pelo termo, em inglês, “privacy notice”, e são muito importantes para a blindagem da operação e para evitar riscos de CONFORMIDADE com a nova legislação.

Além disso, saber abordar o consumidor/titular pode fazer muita diferença. Atenção! Dados bancários, que permitem identificar, direta ou indiretamente, o titular/ pessoa natural/pessoa física, também são considerados **dados pessoais**. No entanto, se forem dados de uma conta de Pessoa Jurídica/Empresa, não serão considerados dados pessoais, exceto se a documentação tiver alguma informação sobre a pessoa responsável pela empresa (que a identifique).

Um ponto importante é o cuidado com a qualidade de dados, pois, durante a cobrança, pode acontecer de se entrar em contato com a pessoa por canais que podem não estar atualizados, e a LGPD traz esta exigência.

Já houve aplicação de multa, na Europa, devido ao envio de mensagem para o celular da pessoa errada, fazendo cobrança, por informação desatualizada.

Desse modo, é possível realizar o enriquecimento da base de dados para atualizar as informações, para fins de cobrança, inclusive, a partir de dados de origem pública, justamente, para atender ao princípio da qualidade e evitar este risco.

Por fim, também alertamos sobre o **Compartilhamento de Dados**, pois, **na terceirização**, será, extremamente, necessário estabelecer regras e responsabilidades, tendo em vista que o **contratado**, neste caso, será considerado, sempre que promover o tratamento de dados, em nome do **Controlador**, o que é comum nos contratos com agências de mídias digitais, marketing, despachantes, entre outros.

A área de **Recursos Humanos** merece atenção especial, pois, apesar de não lidar com dados de clientes, promove o tratamento de dados pessoais dos colaboradores. Existem vários desafios para o RH, a começar pelo processo seletivo, tendo em vista que se trata de uma relação onde ainda não há vínculo empregatício e nem, sequer, um contrato.

Portanto, recomenda-se estabelecer regras específicas, controles e formas de informar, ao titular/candidato, antes da coleta dos dados pessoais, a política do processo seletivo, e que diga, ao menos, quais dados pessoais são necessários, para quais finalidades, por quanto tempo esses dados serão tratados e se haverá compartilhamento com terceiros.

Ou seja, para adequar a base do “Trabalhe Conosco” à LGPD é importante que o candidato seja informado, e aceite, as condições, previamente, estabelecidas, em algum momento, no fluxo de cadastro. Isso porque o recebimento de currículum pode ocorrer por várias formas, mas, deve haver um momento em que haja a centralização e o controle.

Deve-se, também, lembrar que, pela nova Lei, onde houver uma base de dados pessoais, deve ser aplicado o descarte seguro. Logo, se for impresso, depois do seu uso, para realizar alguma entrevista ou dinâmica, é recomendável que seja feita sua eliminação, picotando os papeis. O que percebemos é que será necessária uma mudança de procedimentos, e de cultura, no ambiente de trabalho.

DICA

Quando o titular/cliente usa a mídia social, como meio de autenticação para serviços (para não preencher cadastro), o primeiro contato da empresa pode ser feito, também, pela rede social. Vale ressaltar que o cliente terá que ser informado sobre as finalidades futuras, inclusive, para novos contatos do mesmo **Controlador**.

Para outras finalidades, será preciso analisar se essas estão descritas na própria mídia social e acompanhar o que está ali contido. Portanto, os dados não poderão ser utilizados para qualquer finalidade que não a expressa quando o dado se tornou público, pela mídia social.

Nos termos do art. 8º, parágrafo 6º em caso de nova finalidade o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Existem outros **desafios** como, por exemplo, o tratamento de dados como os **antecedentes criminais, exames médicos, declaração de Imposto de Renda** e seu compartilhamento com entidades competentes.

Pode ocorrer, ainda, o compartilhamento de dados dos colaboradores para concessão de benefícios, como saúde, alimentação, transporte, previdência, entre outros, incluindo informações do cônjuge e dependentes. Vale ressaltar que, quando isso ocorrer por exigência legal, para cumprimento do contrato de trabalho ou legítimo interesse, não haverá necessidade de consentimento.

São muitos os cuidados do RH, até mesmo com o uso das fotos e imagens dos colaboradores. O ideal é atualizar o **Código de Conduta** e o contrato de trabalho, bem como a Política de Benefícios, para que fiquem claros quais dados são coletados, se há compartilhamento, com quem, se há internacionalização dos dados, e que haverá tratamento, também, para registro de acervo histórico e memória da empresa, com guarda permanente. Este último item é, extremamente, relevante, pois haverá dados pessoais, como registros de imagens, vídeos, fotos, e mesmo documentos que ficarão guardados, no legado, e não poderão ser apagados.

Em relação à área de **Compras**, talvez esta seja a que lide com dados pessoais em menor quantidade e finalidade. O principal ponto de atenção é para dados relacionados aos parceiros e fornecedores, pessoa física envolvida nas transações contratadas, como funcionários dos contratados ou responsáveis ou representantes dos prestadores de serviços, que constam dos contratos.

Mas, podem ocorrer situações que envolvam compartilhamento de dados pessoais com esses terceirizados, em função da atividade contratada como, por exemplo, contratação de serviços de armazenamento ou análise de dados (como serviço de “cloud”). Portanto, na contratação de operadores, os contratos deverão ser atualizados, com cláusulas específicas, considerando atribuição de responsabilidades e obrigações relacionadas à proteção de dados pessoais.

Recomenda-se que a área de **Compras** passe a ter um questionário para identificar se, naquela contratação, haverá compartilhamento de dados pessoais e, nesse caso, aplique um anexo ao contrato.

Além disso, também deve ser atualizado o **Termo de Confidencialidade**, conhecido por **NDA**, para que tenha uma cláusula sobre proteção de dados pessoais, que será aplicada, previamente, em todas as reuniões em que forem trocadas informações, que contenham dados pessoais. Isso deve ocorrer antes de uma contratação, seja numa relação de pessoas jurídicas ou com pessoas físicas, e deve fazer parte da rotina da empresa.

Em todos os casos, a criação de políticas e procedimentos, agregados aos treinamentos, deve ser percebida como uma forma de mitigar riscos e capacitar os funcionários sobre como devem proceder, em todos os estágios da coleta das informações.

03

POR ONDE COMEÇAR PRIMEIROS PASSOS PARA A CONFORMIDADE.

Todo projeto de implementação deve considerar um fluxo mínimo para levantamento de informações e, consequentemente, identificação de seu cenário interno. Desta forma, poderá traçar um plano de ação para implementação e verificar sua eficiência e possibilidade de atender a um cronograma, dentro do prazo de adequação da Lei.



Como passo inicial, a empresa deve:

1. Nomear o “Encarregado (DPO)”, função exigida pela LGPD e que pode ser exercida por profissional interno da empresa, por um comitê nomeado, um líder, ou mesmo um terceirizado.

Não há uma exigência legal sobre os pré-requisitos para assumir a função do DPO, no entanto, recomenda-se conhecimento de leis, tecnologia e segurança da informação. A estrutura de sua equipe e sua posição no organograma da empresa dependerá de cada perfil e cultura da própria empresa. Recomenda-se autonomia ao DPO e que ele se reporte, diretamente, à alta gestão.

Todos os processos e projetos, que envolvam Dados Pessoais, deverão passar pela análise de sua equipe;

2. Promover um workshop inicial, a fim de engajar todos os profissionais, na fase de análise e implementação da LGPD, dentro da empresa;

- 3. Formar o Comitê de Proteção de Dados Pessoais,** que pode aproveitar um Comitê já existente como, por exemplo, o Comitê de Riscos, de Segurança ou de Qualidade, e adicionar a nova pauta, caso ainda não o tenha criado;
- 4. Levantar o Mapa de Dados e Processos de Tratamento de Dados Pessoais;**
- 5. Analisar as finalidades e tratamentos.** aplicados aos dados pessoais;
- 6. Elaborar um Plano de Ação** para adequação à LGPD, com base nos dados e na análise realizada;
- 7. Implementar o Plano de Ação,** incluindo adequação dos processos, criação de regras e atualização de documentos jurídicos;
- 8. Implementar Campanha de Sensibilização e Capacitação das Equipes Programa de Privacidade e Proteção de Dados Pessoais** (que pode ser adicionado à Campanha de Segurança da Informação). As ações de sensibilização podem ser um fator crucial para o sucesso da implementação de um projeto de LGPD, tendo em vista que o fator humano é uma das maiores vulnerabilidades para vazamento de dados;
- 9. Realizar o monitoramento, acompanhar a evolução legislativa e da Autoridade (ANPD);**
- 10. Realizar as reuniões periódicas do Comitê;**
- 11. Aplicar lições aprendidas e atualizações futuras.**

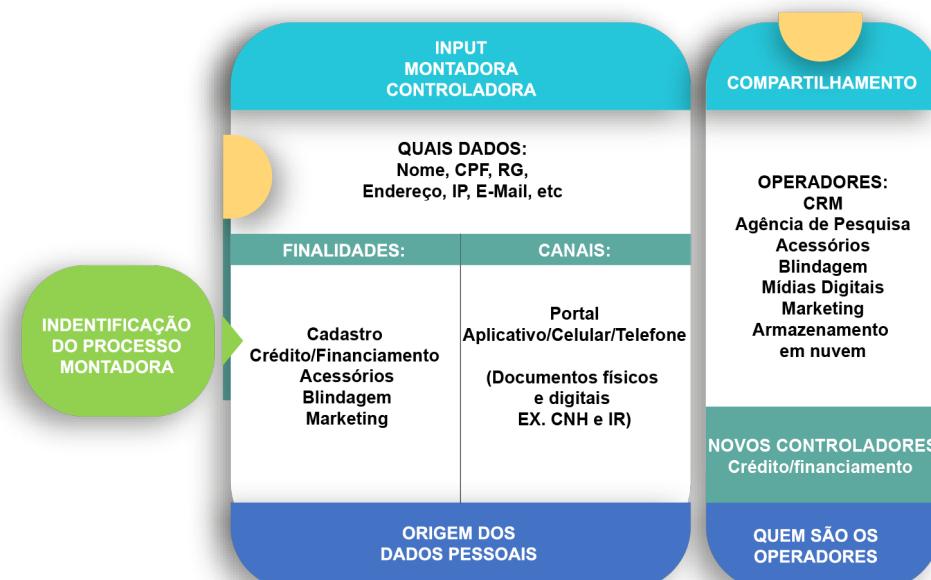
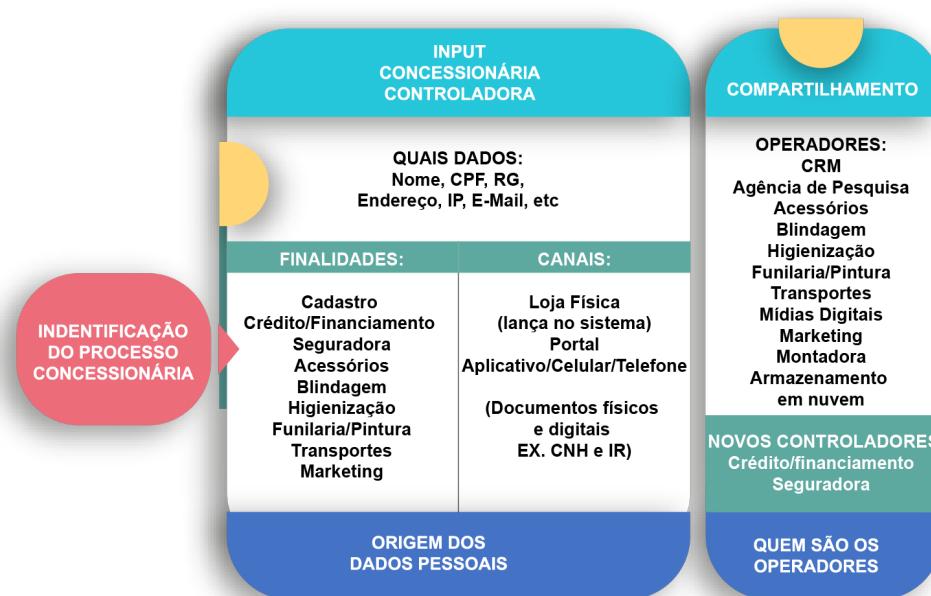
Para análise de cenário e diagnóstico, sugerimos a seguinte trilha:



Dependendo do porte da empresa, será possível e necessário buscar um nível de maturidade mais seguro, além de outras informações:



A seguir exemplo de levantamento de dados:



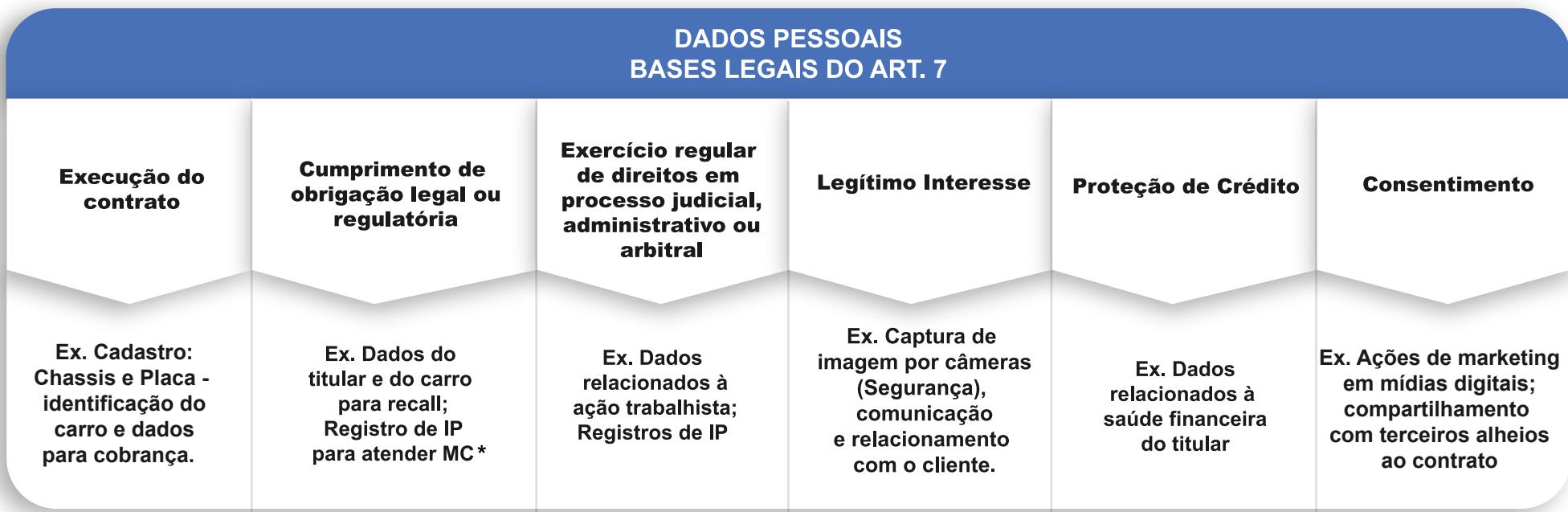
Exemplo de dados conforme a categoria do titular:

CATEGORIA DO TITULAR	PESSOAIS	SENSÍVEIS
EXEMPLOS DE DADOS PESSOAIS TRATADOS	Nome CPF RG Endereço E-Mail Telefone Passaporte Imposto de Renda Placa do Carro Chassis N. da Proposta N.O.S, n. Cliente (pessoa física)	Informações de Saúde Exames Atestados Médicos Gênero Religião

O que preciso saber sobre armazenamento:

	SERVIDORES PRÓPRIOS	SERVIDORES TERCEIRIZADOS
TRANSFERÊNCIA	NÃO	SIM
TRANSFERÊNCIA INTERNACIONAL	Possível se o servidor estiver em outro país	Possível se o servidor estiver em outro país

Exemplo de Enquadramento da Finalidade de base legal:



*Marco Civil da Internet

04

PRIMEIROS PASSOS PARA ATENDER À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS



Conforme preceitua a Lei, o **Encarregado (DPO)** será o responsável pela interlocução entre **Controlador e ANPD - Autoridade Nacional de Proteção de Dados Pessoais**, mas não quer dizer que ele seja o único responsável pela elaboração dos documentos necessários.

Ter uma equipe preparada será o diferencial, pois, mesmo o **Encarregado** precisará de apoio e auxílio das demais áreas.

Atender à ANPD é mais um dos muitos desafios da LGPD, tendo em vista que a própria Autoridade ainda regulamentará muitas questões e deverá dirimir dúvidas latentes, atualmente.

Dois pontos serão obrigatórios, e o **Controlador** já pode, e deve, estar preparado para: atender ao dever de **Report** e saber elaborar o **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**.

O primeiro, previsto no Art. 48, estabelece que, na ocorrência de um incidente de segurança, que possa acarretar risco ou dano relevante aos titulares dos dados, esse incidente deverá ser reportado à ANPD e aos titulares envolvidos.

Neste caso, a LGPD fala em prazo razoável, que deverá ser definido pela ANPD, enquanto a legislação europeia determina, expressamente, 72 horas.

Como já mencionado, em outros trechos dessa Cartilha, a LGPD apresenta os principais tópicos (informações) que devem constar do Relatório.

Além disso, a ANPD poderá verificar a gravidade do incidente, caso necessário, para a salvaguarda dos direitos dos titulares, e determinar, ao **Controlador**, a adoção de providências, tais como: ampla divulgação do fato, em meios de Comunicação, e medidas para reverter ou mitigar os efeitos do incidente.

O **Report**, para a ANPD, relacionado a um determinado incidente, pode ser bem semelhante ao Relatório de Impacto, desde que atenda às exigências do Artigo 48, da LGPD.

Por outro lado, independente da ocorrência de um incidente de segurança, a ANPD poderá solicitar, ao **Controlador**, um **Relatório de Impacto à Proteção de Dados Pessoais**, que deverá ser elaborado com base nas exigências do parágrafo único do Art. 38, da LGPD, e deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e garantia da segurança das informações e a análise do **Controlador**, com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

05

TEMPO DE ARMAZENAMENTO

Atrelado ao princípio da necessidade, surge a limitação de tempo no armazenamento dos dados pessoais. Neste sentido, os dados pessoais somente poderão ser armazenados enquanto forem necessários para a execução do contrato, cumprimento de obrigação legal, regulatória ou para uso exclusivo do **Controlador**, vedado seu acesso por terceiro, e desde que anonimizados.

A seguir, apresentamos uma sugestão de guarda, por prazo mínimo. No entanto, **cada empresa deve estabelecer e detalhar sua própria tabela de temporalidade**, da qual deve constar o tipo de dado coletado, finalidade, tempo de guarda e embasamento legal.

Alertamos, ainda, que os dados podem ser tratados por áreas distintas e finalidades diversas. Para uma área pode haver justificativa, como exigência legal e, para outra, pode ocorrer a necessidade de coletar o consentimento, ou ambas as hipóteses poderiam ocorrer, com base legal.

De qualquer forma, é preciso distingui-las (áreas e finalidades), informar ao titular e proteger os dados devidamente. Por exemplo, tomemos como base os dados de biometria, que são coletados com a finalidade de identificação do proprietário e funcionamento de veículo, ou a coleta dos mesmos dados para a identificação do cliente ao entrar na concessionária (como ocorre em portarias).



Dados pessoais	Tempo de Armazenamento
Histórico Empresarial de Carteira de Clientes (Fundo de Comércio) ativo empresarial	Prazo permanente
Relação de consumo	5 anos após encerramento da relação
Ex. de Relações trabalhistas	Aviso de Férias 5 anos
	Cópia da Caderneta de vacinação dos filhos 10 anos após desligamento do colaborador
Ex. Dados Fiscais	Livros Fiscais – Registro de Apuração do ICMS 10 anos
	Registro de Entrada de Mercadorias 10 anos
Processos indenizatórios Reparação cível	Dependendo do caso pode ser de 3 a 10 anos

(*) Três anos para casos que versem sobre responsabilidade civil extracontratual. A Corte entende pelo prazo de 10 anos para ações de reparação de danos provenientes de relação contratual com base no art. 205 do Código Civil: “A prescrição ocorre em dez anos, quando a lei não lhe haja fixado prazo menor”.

06

ANEXO I PERGUNTAS E RESPOSTAS

Apresentamos as principais perguntas e respostas para os pontos mais importantes da LGPD, conforme a seguir:

1. Quem são os TITULARES DE DADOS, no universo automobilístico?



Os clientes, vendedores, funcionários internos, funcionários de terceirizadas, entre outros, que tenham vínculo direto ou indireto.

A Lei não se aplica aos dados de pessoa jurídica, no entanto, no contexto da relação jurídica entre as empresas, caso envolva dados pessoais ou sensíveis, sejam de funcionários ou terceiros, esses estarão sob a proteção da LGPD.

2. Quem tem acesso, aos DADOS PESSOAIS, na empresa?

É importante saber quem tem ou pode tratar dados pessoais como, por exemplo, o vendedor nas concessionárias, que tem acesso aos módulos de CRM, vinculados ao DMS, e aos controles e monitoramento de qualidade de atendimento da montadora.

No universo automobilístico será necessário considerar toda a cadeia interativa, como as concessionárias, montadoras, fornecedores, prestadores de serviços (despachantes, seguradoras, financeiras, agências de mídias digitais, centrais de controles de leads) e, ainda, colaboradores relacionados ao processo de monitoramento da qualidade e atendimento ao cliente. Neste último caso, podemos considerer as áreas de vendas e pós-vendas, além do marketing e desenvolvimento de rede.



Sabemos que o universo automotivo não se limita aos exemplos utilizados acima e cada empresa deve fazer o seu próprio organograma, que possibilitará identificar qual o fluxo da informação e quem tem acesso a ela.

Além dos exemplos citados, não podemos esquecer que a LGPD também abrange **DADOS PESSOAIS** e **DADOS PESSOAIS SENSÍVEIS** de funcionários e terceirizados, e não apenas dos clientes.

3. Qual o valor dos dados dos meus clientes? Por que preciso protegê-los?

Na Sociedade do conhecimento, **dados têm valor econômico**, pois, de alguma forma, **podem gerar lucro** e, nesse ponto, passam a ser **chamados de informação**. Imagine o seu banco de dados, de clientes, nas “mãos” do seu concorrente?

E quais os dados agregam valor para as concessionárias, montadoras e seguradoras? Quanto valem esses dados? Informações de tendências e gostos, vinculados ao perfil de um cliente, com certeza, valem muito.

Portanto, os dados fazem parte de todo negócio, sendo, nesse contexto, um valioso ativo empresarial e, portanto, se faz necessária a sua proteção.

Os Artigos 46 e 47, da LGPD, são claros ao instituir o **dever de proteção dos dados pessoais**, incluindo a necessidade de proteção técnica e comportamental.

Além disso, pensar na **Proteção de Dados**, desde o nascimento de um projeto, a fim de atender ao Art. 46 § 2º (Privacy by Design) e, acima de tudo, prevenir que, realmente, ocorra algum incidente.

Portanto, essa preocupação faz parte de uma blindagem de Segurança da Informação e Proteção de Dados Pessoais, incluindo segurança jurídica, implementação de recursos técnicos, adequação dos documentos e sensibilização de todas as áreas, que devem contar com a capacitação de seus profissionais.

4. Relação Controlador e Operador no Setor (Montadora, Distribuidor, Concessionária, Financeira, Seguradora);

A LGPD define que os **Agentes de Proteção de Dados Pessoais** são o **Controlador** e o **Operador**. Neste sentido, quais seriam os agentes de proteção de dados pessoais no segmento automobilístico?

O **Controlador** é aquele que toma a decisão, ou seja, define quais dados serão coletados, o que deverá ser feito com eles e, portanto, qual tratamento será aplicado. Neste caso, ocorre o **princípio da responsabilidade**, que demanda, do **Controlador**, o Registro de sua Conformidade Legal, para comprovação em eventual fiscalização, por órgãos públicos (no Brasil, atualmente, as fiscalizações são feitas pelo Ministério Público do Distrito Federal e Territórios, e pelos PROCONs dos Estados).

A empresa, que promove o tratamento de dados, sob a instrução do **Controlador**, é a **Operadora**. Vale ressaltar que **uma empresa pode ser, ao mesmo tempo, Controladora e Operadora**. Exemplo: uma empresa de Mídias Digitais é **Controladora**, do ponto de vista de dados de seus funcionários, e **Operadora**, em relação às concessionárias e/ou montadoras que a contratam.

A concessionária é Controladora, à medida em que **define quais Dados Pessoais e/ou Sensíveis** devem ser coletados e para qual finalidade. Já os terceiros/empresas contratados para fazer a coleta, armazenamento e análise dos dados são **Operadores**.

É o caso das empresas, dentro do próprio ecossistema que, por força da relação jurídica, promovem o tratamento de dados, em nome de quem as contratou.

Para melhor exemplificar a **diferença entre Controlador e Operador**, no ecossistema automobilístico, utilizaremos a **financeira e a seguradora**, que são ambas **Controladoras**, uma vez que se trata de contrato direto com o titular dos dados/cliente, ainda que seja por intermédio de uma concessionária. Já a empresa, que faz análise de comportamento, dos clientes da concessionária, é **Operadora**.

Também pode haver concurso de controladores, onde mais de uma empresa é controladora de bases de dados pessoais, que ficam reproduzidas em todas (Ex.: quando é cliente tanto da concessionária, como da financeira e da seguradora).

Mas, lembre-se: Toda empresa, seja a concessionária, montadora ou fornecedor, são **Controladores**. Isso porque ainda que não coletem ou recebam, de terceiros, dados pessoais de consumidores, por certo, têm controle sobre os dados pessoais de seus funcionários.

Outro exemplo prático: **Uma agência de marketing, contratada pela concessionária, para trabalhar o banco de dados pessoais dos clientes**, que já tenham comprado veículos e/ou serviços na concessionária, no passado. Nesse caso, enquanto a **concessionária é a Controladora**, a **agência de marketing é a Operadora**.

Apenas será considerado **Operador** aquele que recebe os dados ou que promove seu tratamento, incluindo a coleta, em nome de terceiros. A financeira, distribuidora, seguradora não são operadores, tendo em vista que não promovem o tratamento, uma em nome das outras, mas são negócios autônomos e ligados entre si, de forma que, na prática, pode ocorrer o compartilhamento e não uma subordinação, onde há o **Controlador** e o **Operador**.

Em resumo...



CONTROLADOR

Toma as decisões relativas ao tratamento de dados pessoais

OPERADOR

Realiza o tratamento de dados pessoais em nome do controlador

5. Por que é importante saber a Finalidade da Coleta dos Dados Pessoais?

Um dos fatores mais importantes da LGPD é estabelecer a **Finalidade da Coleta de Dados Pessoais**, ou seja, para que será usado o dado pessoal coletado, uma vez que **esse uso será determinante para identificar a justificativa de tratamento**, qual base legal irá permitir o seu uso, de forma a **definir se haverá necessidade, ou não, da Coleta do Consentimento, ou se aquele uso pode ser feito com base em uma Exceção de Consentimento**, trazida pela própria Lei.

As hipóteses, que justificam o **Tratamento de Dados Pessoais**, são:
Consentimento: ter permissão específica para aquela finalidade
O Art. 5, inc. XII, define o **Consentimento** como a livre manifestação, informada e inequívoca pela qual o titular concorda com o tratamento de seus **Dados Pessoais** para uma finalidade determinada.

Isto quer dizer que o **Consentimento** tem que demonstrar, e refletir, fielmente, a vontade do titular. Portanto, deve ser uma ação positiva e

não impositiva, de forma que as “famosas” caixas de aceite, previamente, preenchidas, serão consideradas nulas.

- **Livre:** O Consentimento não pode ser concedido mediante coação ou imposição do controlador.

- **Informado:** Agregado ao princípio da transparência, trata-se da necessidade de **informar, ao titular, previamente, sobre o tratamento a ser aplicado ao seu dado**, bem como as consequências do seu aceite, ou não.

- **Inequívoco:** Trata-se da comprovação da vontade do titular. Detalhe muito importante é que deverá ser informado **como o titular poderá exercer seu direito de revogar o consentimento**.

O caso pode estar, também, dentro das hipóteses de **Exceção de Consentimento**, quais sejam:

• **Cumprimento de obrigação legal ou regulatória pelo Controlador:** Trata-se da coleta do dado, por uma exigência legal, ou seja, exigida por determinada Lei, Decreto, Medida Provisória, Resolução, etc. Podemos utilizar, como exemplo, aplicável a todas as empresas, o **Marco Civil da Internet**, que **exige o armazenamento de dados pessoais, que identifiquem o titular/ usuário, pelo prazo de seis meses, para provedores de aplicativos, e de um ano, para provedores de conexão**.

As empresas do ramo automobilístico deverão verificar a quais leis estão sujeitas e promover uma análise com base em todos os dados coletados.

• **Pela administração pública, para o Tratamento e uso compartilhado de dados, necessários à execução de políticas públicas, previstas em Leis e Regulamentos ou respaldadas em Contratos, Convênios ou Instrumentos Congêneres:**

Somente a **administração pública**, de forma direta e atuando como **Controladora**, pode realizar **Tratamentos de Dados Pessoais sob essa base legal**. Ainda que atuando na execução de políticas públicas,

as organizações privadas não poderiam utilizar essa base legal como justificativa para o Tratamento de Dados Pessoais.

• **Execução de Contrato ou de procedimentos preliminares relacionados a Contrato, do qual seja parte o titular e a pedido do titular dos dados:**

Refere-se ao Tratamento de Dados Pessoais, com base nas informações necessárias para executar o serviço contratado. Por exemplo: Ao adquirir um plano de consórcio, para aquisição de um automóvel novo, a fim de participar dos sorteios mensais, será necessária a identificação do consorciado, assim como o contato com ele, para informá-lo sobre sua contemplação.

• **Exercício regular de direitos em processo judicial, administrativo ou arbitral:**

Toda relação está sujeita a desentendimentos ou ocorrências que levem as partes a juízo, ou seja, à busca de solução pelo judiciário. Neste contexto, os dados podem ser armazenados sem o consentimento do titular, para a finalidade de utilização em processos judiciais, ou, por exemplo, em um processo administrativo, proveniente de órgãos públicos ou para a solução de conflitos, por arbitragem.

• **Realização de estudos por órgãos de pesquisa:**

Embora o próprio título já seja autodescritivo, ressaltamos que, segundo a LGPD, entende-se como **Órgão de Pesquisa** entidade da administração pública, direta ou indireta, ou pessoa jurídica, de direito privado, sem fins lucrativos, legalmente constituída, sob as leis brasileiras, com sede e foro no País, que inclua, em sua missão institucional, ou em seu objetivo social ou estatutário, a pesquisa básica ou aplicada, de caráter histórico, científico, tecnológico ou estatístico.

• **Proteção à vida ou da incolumidade física do titular ou do terceiro:**

Ligado, diretamente, com a proteção do interesse essencial à vida, de qualquer pessoa natural/física.

• **Tutela da saúde:**

Autoexplicativo, quando se fala em tutelar a saúde, mas esta justificativa aplica-se, especificamente, pela utilização de profissionais da área da saúde.

• **Interesse legítimo do Controlador ou do terceiro:**

O legítimo interesse pode ser do Controlador, dos titulares ou de uma coletividade, como a própria sociedade. Tem sido muito utilizado para hipótese de bases legadas, em que há uma anterioridade na relação e uma justificativa plausível, mas seu uso não pode ser indiscriminado. Por isso, pressupõe a possibilidade de ser exigido **Relatório de Impacto** pela ANPD. Destaca-se que **o legítimo interesse não se aplica ao Tratamento de Dados Sensíveis**, mas tão somente aos **Dados Pessoais**, e o **Controlador** deve adotar medidas para garantir transparência, no tratamento dos dados pessoais.

• **Proteção do crédito:**

O Tratamento de Dados Pessoais para Proteção do Crédito é uma exceção, considerando a ótica de proteção do próprio ofertante, onde são necessárias informações para identificação e análise de perfil, além de haver uma proteção coletiva do crédito, devido à gestão de risco e do custo desse crédito.

• **Garantia de Prevenção à fraude e à segurança do titular:**

Justifica-se o **Tratamento de Dados Pessoais Sensíveis** para prevenção à fraude, nos processos de identificação e autenticação de cadastro, em sistemas eletrônicos (o que inclui biometria, reconhecimento facial, outros), visando a proteção do próprio titular e de sua segurança, visto que há necessidade da sua identificação, ou mesmo da sua proteção, caso a pessoa identificada não seja o titular).

Ao levantar a finalidade da coleta, será possível identificar as **justificativas legais**, que permitem o **Tratamento de Dados Pessoais**. Caso a justificativa não se enquadre em uma das hipóteses, previstas nos Artigos 7 e 11, a partir do inciso II, ou, ainda, do Art. 14, **quando se tratar da coleta de dados de crianças ou adolescentes, será necessária a Coleta do Consentimento**.

A principal, e mais segura, justificativa, no âmbito privado, refere-se à **Finalidade de Execução do Contrato**, pois, ainda que exista embasamento no legítimo interesse, esse, além de ser uma lacuna, para discussões sobre o que, realmente, seria o legítimo interesse, permite que a Autoridade Nacional requeira um **Relatório de Impacto** pelo **Controlador**.

Um ponto, já mencionado anteriormente, aborda o fato de que, **ainda que exista uma justificativa**, nas hipóteses anteriores, de forma **que justifique a coleta de dados sem o Consentimento** do titular, **será necessário atender ao princípio da Transparéncia**, previsto no Art. 6, e deve-se, portanto, apresentar informações, claras e exatas, aos titulares dos dados, antes da coleta.

Assim, recomendamos que a **Finalidade de Uso dos Dados** seja **apresentada** sempre, de modo evidenciado, **para que não restem dúvidas** perante às autoridades, ao mercado e ao próprio titular dos dados pessoais, quanto à transparéncia na relação entre o responsável pelo tratamento e o titular dos dados pessoais.

Alertamos, também, para a **necessidade de minimização e proporcionalidade** no **Tratamento de Dados Pessoais**. Lembramos que o tratamento de dados engloba todos os tipos de usos e destinações aos dados pessoais, desde a coleta, armazenamento, uso, compartilhamento até o descarte/eliminação. Aqui nos deparamos com o **Princípio da Necessidade**, no qual somente os dados pessoais, estritamente, necessários para o cumprimento das finalidades legitimadas, junto ao titular, é que poderão, de fato, ser tratados de modo legítimo.

Não se pode, por exemplo, exigir a coleta e uso de dados de religião para a compra de um veículo na concessionária, pois a coleta desse dado foge ao objetivo principal do negócio.

6. Por que é importante saber se há compartilhamento de dados pessoais com outras empresas?

O **Compartilhamento de Dados** pressupõe alguns cuidados, principalmente, na contratação, pois saber quem será contratado e o nível de segurança oferecido é essencial. Em caso de incidente, por vazamento de dados, existe o risco de causar danos aos titulares e, também, de afetar, diretamente, a reputação do **Controlador**, além de lhe causar perdas financeiras.

Além disso, a LGPD prevê algumas regras, entre elas, **o dever de informar**, ao titular dos dados, que será feito o **Compartilhamento** de seus dados com terceiros, bem como para qual finalidade se destina. Dependendo do caso, pode ser necessário o **Consentimento** do titular.

Veja o que diz o art. 7, § 5º

O controlador, que obteve o consentimento, referido no inciso I do caput deste artigo, que necessitar comunicar ou compartilhar dados pessoais, com outros controladores, deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento, previstas nesta Lei.

No caso de **Dados Sensíveis**, se o Compartilhamento tiver, por objetivo, vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da Autoridade Nacional.

É preciso, também, muita atenção, pois caso o titular **revogue o Consentimento dado anteriormente**, o **Controlador** deverá comunicar os agentes com os quais tenha compartilhado os dados:

Art. 18 - § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação

seja, comprovadamente, impossível ou implique esforço desproporcional.

Além dos cuidados em relação às informações prestadas ao titular ou à coleta do **Consentimento**, quando necessário, será preciso atentar-se à necessidade de ajustes e adequações dos contratos, onde o serviço envolver o **Compartilhamento de Dados Pessoais**.

7. Smart e IA – Dados capturados na interação dos veículos com usuários e Smart Cities – desafios para a Conformidade;

Com o rápido avanço das tecnologias, muitos sistemas já promovem a coleta de dados, de forma inteligente, inclusive, com a utilização de soluções de Inteligência Artificial, com algoritmos para levantar muito mais informações sobre os titulares e usuários dos veículos.

Além disso, com o uso de dispositivos com IoT (internet das coisas), em um contexto de Cidades Inteligentes (Smart Cities), será possível ter muito mais dados para o setor Automobilístico, de mobilidade urbana, de varejo, de seguros, financeira, entre outros. Neste contexto, é importante que as políticas de privacidade sejam bem definidas e que o contrato de venda tenha previsão expressa em referência ao tratamento de tais dados, incluindo coletas futuras, desde que seja possível prever as finalidades.

Além disso, temos destacado que a **organização das bases de dados deve ser feita já diferenciando a base primária da base secundária**, e já criando uma camada de proteção, relacionada ao segredo de negócios.

8. Quais são as bases de dados que podem ser utilizadas, de forma livre, sem o pedido de Consentimento?

Por certo que vários dados pessoais são de uso comum, em diversas empresas e áreas internas, mas podem, obviamente, ter finalidades distintas. Como mencionado anteriormente, **nem sempre será preciso coletar o Consentimento, embora permaneça o dever de atender ao princípio da Transparência.**

As hipóteses de uso sem a necessidade de **Consentimento** estão elencadas no próprio Art. 7º, incisos II a X, e no artigo 11, também incisos II a X; todas já mencionadas no item 5.

Destaca-se, portanto, que todas as hipóteses dependem da finalidade de uso. Por outro lado, existem dados que são de livre acesso, ou seja, que podem ser utilizados independente de se enquadrar em uma das hipóteses do Art. 7º. Trata-se dos **Dados Anonimizados**, aqueles que não podem ser mais revertidos e não permitem a identificação de qualquer titular. O processo de anonimização não pode ser passivo de reversão, portanto, dados estatísticos, métricas, entre outros, podem ser utilizados, livremente, inclusive compartilhados.

Atenção para dados coletados em mídias sociais, pois estes nem sempre são livres, para qualquer tipo de utilização.

Não é porque os dados estão disponíveis que poderão ser utilizados por terceiros, assim como a foto, que possui, além da proteção constitucional, o caráter de dado pessoal. Telefones e e-mails, por exemplo, mencionados em posts de conversas entre amigos, não estão autorizados para varredura e tratamento por terceiros, a não ser que sejam disponibilizados para esta finalidade ou que, apesar de finalidade diversa, tenham sido autorizados para esse fim.

A Lei prevê a possibilidade de uso de dados pessoais a partir de fontes públicas, mas desde que o tratamento seja com finalidade compatível.

Essa situação é diferente de uma informação de telefone e e-mail de uma plataforma, onde o titular autorizou deixar a informação aberta, pois quer receber contatos de pessoas, especialmente, para manter relações profissionais o que permite abordagens para propostas de trabalho, por exemplo.

É importante distinguir fontes públicas, de informação pública. A LGPD não faz menção expressa a fontes públicas, mas, tão somente a informações tornadas públicas, manifestamente, pelo titular. Portanto, exige uma ação proativa do titular e deve estar disponível por sua própria vontade.

*O Art. 7, § 4º dispõe: É dispensada a exigência do **Consentimento**, previsto no caput deste artigo para os dados tornados públicos, manifestamente, pelo titular dos dados, resguardados seus direitos e os princípios previstos nesta Lei.*

Além disso, a Lei resguarda os direitos dos titulares, bem como os princípios do Art. 6º. Em outras palavras, a base de uso está na finalidade, e deve atender ao princípio da **Transparência**, minimização, entre outros.

Vamos utilizar um exemplo prático: para qual finalidade uma pessoa cria perfil em uma rede social de relacionamento? Certamente, não é para receber oferta de veículos, mas, sim, para encontrar novos amigos. Neste caso, dados como **nome, foto e contato** podem estar disponíveis para outros membros. Para que um vendedor utilize esses dados, para fins comerciais, será preciso o **Consentimento** do titular.

9. A quem pertencem os dados?

Uma dúvida muito comum, para empresas de qualquer segmento, é sobre a propriedade dos dados. A princípio, o dado pertence ao seu titular, portanto, não pertence à concessionária, à montadora ou à financeira, etc.

O Controlador pode ser o proprietário da base de dados, considerando o valor da informação ali contida, **mas não de cada dado por si**, tendo em vista que o próprio titular tem a gerência de

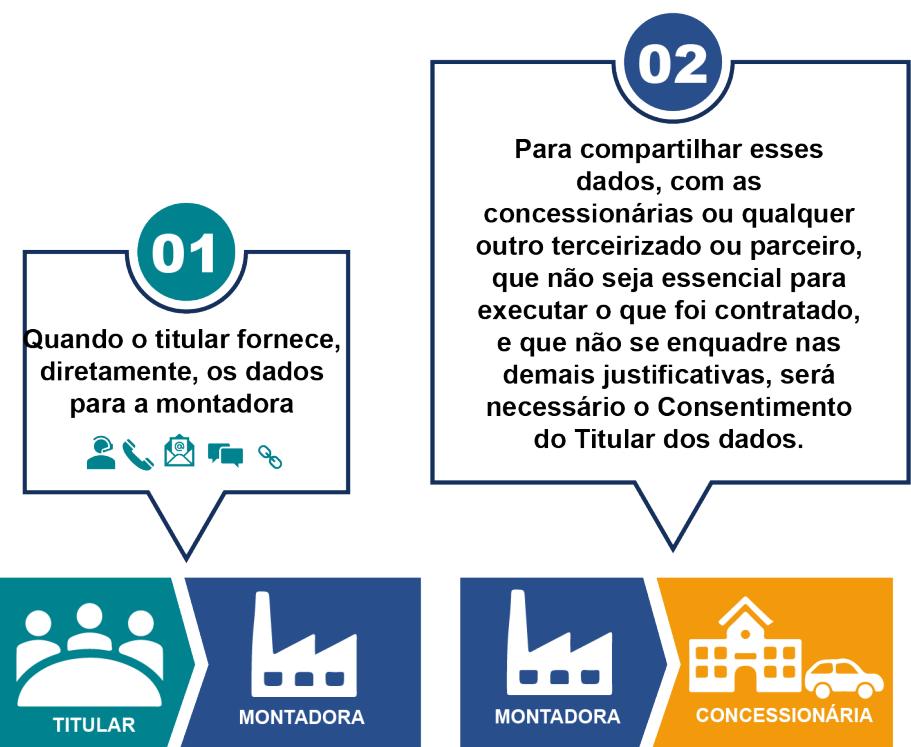
seus dados, quando não forem armazenados pelas hipóteses excluientes de consentimento.

Lembre-se de que o titular tem o direito de revogar o Consentimento e, também, de pedir a eliminação dos seus dados, com base no Art. 18 da LGPD.

No entanto, o **Controlador** deve atentar-se às exceções do art. 16, que prevê a manutenção dos dados, mesmo após término da finalidade inicial ou pedido de apagamento, conforme descrito a seguir:

- I - cumprimento de obrigação legal ou regulatória pelo Controlador;
- II - estudo por órgão de pesquisa, garantida, sempre que possível, a Anonimização dos dados pessoais;
- III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados, dispostos nesta Lei; ou
- IV - uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que Anonimizados os dados.

10. CRM e DMS – Como trabalhar a integração das Bases de Dados de Concessionárias e Montadoras

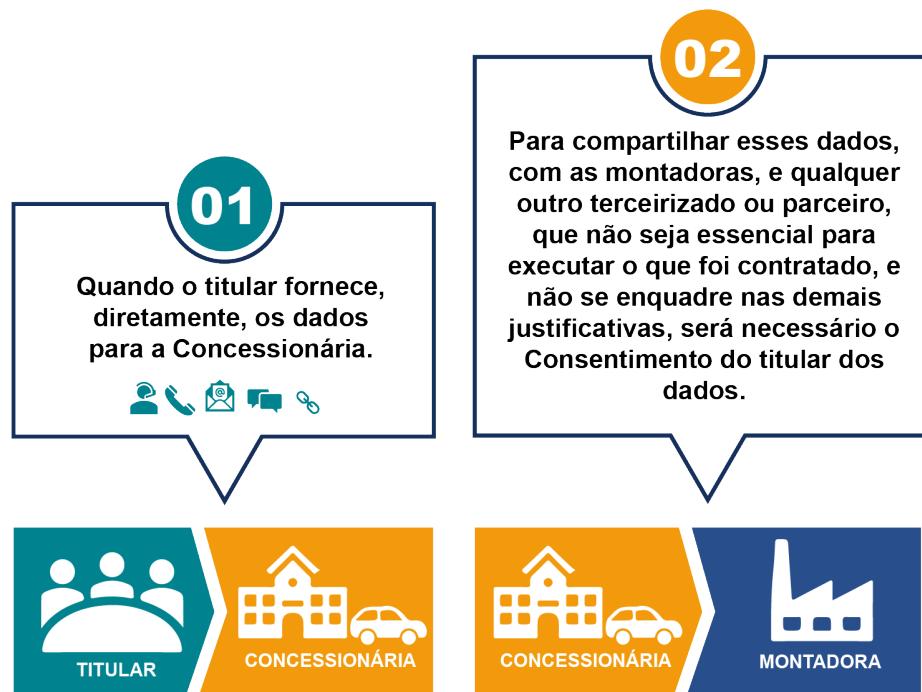


A integração da base de dados, entre empresas distintas, pressupõe levantamento das finalidades. Neste caso, será necessário verificar se as empresas compartilham dados, enquanto **Controlador** e **Operador**, ou apenas pela execução de contratos distintos, **onde ambos são Controladores**, embora seja referente a uma mesma venda. Esse é o caso do financiamento, onde o titular firma contrato com a concessionária e com a instituição financeira.

No entanto, quando o titular firma contrato com a concessionária, ao fazer a compra de um veículo, e a concessionária compartilha os dados desse titular com a montadora, essa assume o papel de Operador, se o tratamento for feito em nome da concessionária.

Para que a montadora possa fazer o tratamento dos dados, coletados pela concessionária, essa deverá informar o **Compartilhamento** dos dados ao titular, com detalhe das finalidades e, consequentemente, será necessária a análise, para verificar os casos em que será necessário o pedido de Consentimento. Neste caso, do dado compartilhado pela concessionária com a montadora, essa última estará fazendo o tratamento do referido dado, para dar andamento ao contrato celebrado com a concessionária.

Para tanto, será preciso o alinhamento estratégico entre Associação de Marca e Montadora.



O passo a passo, sugerido anteriormente, deverá apontar este **Compartilhamento, sua Finalidade, Forma de Coleta** e qualquer outro tratamento. **Quando se tratar de execução de contrato**, ou seja, essencial para prestar o serviço contratado, previsto no documento de contratação, **bastará o esclarecimento comprovado**, ou seja, a informação ao titular, caso contrário, para outras finalidades, sem embasamento legal, será necessário o **Consentimento**.

11. Segurança interna e câmeras de vídeo-vigilância e o Legítimo Interesse

O uso de câmeras de vídeo vigilância é muito comum, considerando a necessidade de identificação de pessoas para acesso a ambientes internos de empresas e prédios e, também, no próprio conceito e aplicação de cidades inteligentes.

A identificação de qualquer pessoa, ainda que feita por imagens, pressupõe autorização prévia, no entanto, sem adentrar na questão de Políticas Públicas e de Segurança Nacional, para a realidade das concessionárias e montadoras, bem como qualquer empresa no âmbito privado, a vídeo-vigilância pode ter um caráter de **Legítimo Interesse**, tanto do Controlador, como do próprio titular do dado pessoal.

A premissa é poder monitorar o ambiente, mas, como já ocorria anteriormente, considerando a proteção constitucional, se faz necessário o aviso prévio de ambiente monitorado (de que está capturando imagem, áudio), mesmo que seja por placas ou banners, como ocorre com a famosa frase “**sorria, você está sendo filmado**”, acrescentando, abaixo, a sua finalidade “**para questões de segurança**”.

Mas, a base da finalidade é a essência, para uso lícito de tais gravações, pois este dado poderá ser utilizado, apenas, para a finalidade informada, ou seja, para segurança. Para qualquer outra finalidade, deverão ser avaliadas as hipóteses legais ou será necessária a coleta do **Consentimento do titular do dado** que, vale lembrar, poderá ser revogado a qualquer momento.

A coleta de biometria facial, por se tratar de dado pessoal sensível, encontra amparo no Art. 11, g, que permite a coleta para a finalidade de prevenção à fraude e para a segurança do titular, nos processos de identificação e autenticação. Portanto, a biometria facial segue a mesma premissa, ao utilizar os dados para outra finalidade que não seja segurança como, por exemplo, para a análise de humor, será necessário o consentimento do titular.

Por outro lado, **para os dados Anonimizados** ou coletados de forma anônima **não há incidência da mesma proteção**, podendo ser utilizados livremente, como na análise de interesse, em produtos, dentro de uma feira, ou

showroom, baseado em agrupamento / intensidade de calor nas proximidades de determinado veículo.

É importante que as operações de tratamento de dados pessoais, que se utilizam do Legítimo Interesse, estejam, devidamente, registradas, ou seja, formalizadas, bem como tenham sido determinadas com base em análise sólida e fria sobre riscos inerentes a esta posição, tendo em vista que o Legítimo Interesse, apesar de previsto na LGPD, deixa lacunas sobre sua abrangência.

É muito provável que a **ANPD - Autoridade Nacional de Proteção de Dados Pessoais** regulamente, com mais detalhes, no futuro, sobre sua aplicação, pois, podem ocorrer controvérsias, de acordo com interesses.

Fato importante é que o tratamento, com base no Legítimo Interesse, é suscetível de questionamento, pela ANPD, uma vez que esta pode solicitar um Relatório de Impacto, conforme previsto no Art. 10, § 3º.

O Legítimo Interesse deve ficar como última hipótese de finalidade, ou seja, quando o tratamento dos dados não se enquadra em outra hipótese, de base legal de exceção de consentimento e, normalmente, **quando não há como obter o Consentimento** do titular, previamente, ao tratamento.

Entendemos que um exemplo prático é o contato com um titular, cujos dados pessoais estão em uma base legada (antiga) e a instituição quer reativar a Comunicação, com envio de uma mala direta. A justificativa, ainda que não exista mais contrato/obrigação legal (trata-se de uma base legada antiga), existe uma relação pretérita entre as partes que justifica um novo contato, no futuro.

Não há formato padrão para embasamento e análise do Legítimo Interesse mas, a exemplo do que faz a União Europeia, recomendamos o Teste de Finalidade, em três etapas:

Teste em 3 etapas	
Teste de finalidade	Existe Interesse Legítimo para o tratamento dos dados?
Teste de necessidade	O tratamento dos dados é necessário para essa finalidade?
Teste de balanceamento	Avaliar o Interesse Legítimo, frente aos direitos e liberdades fundamentais ao titular dos dados.

12. Relatório de Impacto de Proteção de Dados Pessoais - RIPD

Quando um tipo de tratamento de dados utilizar novas tecnologias, levando em conta a sua natureza, âmbito, contexto e finalidades, caso possa implicar num elevado risco para os direitos e liberdades das pessoas físicas, o Controlador, antes de iniciar o tratamento, deve realizar uma Avaliação de Impacto das Operações de Tratamento, para garantir a Proteção de Dados Pessoais. Portanto, seu maior objetivo é identificar e mitigar os riscos inerentes ao seu tratamento.

Além disso, como mencionado anteriormente, **sempre que o tratamento de dados pessoais for baseado no Legítimo Interesse** (Art. 10. Inciso 3º), a ANPD poderá solicitar um Relatório de Impacto.

O DPIA – Data Protection Impact Assessment, assim chamado pela GDPR (legislação da União Europeia) encontra amparo no ordenamento jurídico nacional, nos Arts. 5, 10 e 38º da LGPD. Enquanto o Art. 5º mostra o conceito do termo, o Art. 10º apresenta a hipótese de solicitação do DPIA, nos casos de Legítimo Interesse, e o Art. 38º preceitua que a ANPD poderá determinar a elaboração do DPIA, inclusive de **Dados Sensíveis**, nos termos do regulamento. Portanto, ainda caberá, à ANPD, manifestar-se neste sentido.

O Art. 38º apresenta, também, as informações mínimas, que devem estar previstas no documento, sendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada, para a coleta e para a garantia da segurança das informações, e a análise do Controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A responsabilidade de apresentar o DPIA é do Controlador, portanto, este deve antever situações, que possam gerar a solicitação, por parte da ANPD. Além disso, independente da requisição da ANPD, o Assessment necessário, para a elaboração do Relatório, é de extrema importância para qualquer organização, uma vez que permite a análise efetiva, para gestão de risco, e consolida o embasamento para decisões estratégicas, sendo fator importante na comprovação da boa fé e cultura de prevenção, como essência da empresa.

Apresentamos, no anexo III, uma sugestão para o Relatório de Impacto.

13. Quais as peculiaridades no tratamento de dados pessoais no B2B e B2C?

As relações *Business to Business* (*empresa para empresa*) e *Business to Costumer* (*empresa para consumidor*) se diferem pela finalidade de coleta, mas não pela complexibilidade, tendo em vista que ambos devem atender às necessidades da LGPD. É muito comum que as preocupações recaiam sobre a relação B2C mas, muito embora a Lei não se aplique aos dados de pessoa jurídica, normalmente, a relação entre empresas (B2B) envolve dados pessoais dos funcionários, alocados ou responsáveis pela prestação/ entrega do serviço, sejam Dados Cadastrais como CPF e RG ou Dados Sensíveis, como biometria,

entre outros exemplos. Neste caso, é preciso que os contratos tenham previsão de cláusula específica para garantir que cada parte assuma a responsabilidade que lhe cabe, no dever de Transparência, Proteção e Coleta do Consentimento, quando necessário.

Nas relações B2C, cujo foco recai na preocupação da maioria, acontece o mesmo, sendo necessário, para ambos os casos, a identificação, que deve ocorrer logo no início, por meio do Mapa de Dados e posterior Análise de Finalidade e enquadramento nas hipóteses do art. 7º.

Para os dois casos citados, **recomendamos a criação de uma Política de Gestão de Proteção de Dados Pessoais e Adequação/Criação da Política de Privacidade** que passa a ser, também, de **Proteção de Dados Pessoais**. Na Política de Gestão serão criadas as regras para tratamento de dados pessoais e, na Política de Privacidade, são definidas as regras e informações a serem disponibilizadas aos titulares.

14. Como adequar a Política de Privacidade - Roteiro

Adequar a Política de Privacidade, a princípio, pode parecer fácil, mas, na prática, é bem complexo, pois, para eficiência de qualquer documento é necessário passar pela primeira fase, que é o diagnóstico, que tem, como premissa, **Identificar os Dados que são Coletados, a Finalidade da Coleta, a Proteção Aplicada, entre outras questões**, demonstradas no diagrama, apresentado no início deste Guia.

É possível fazer um *checklist* com as principais informações, que devem constar na **Política de Privacidade**, como, por exemplo (mas não se limitando a elas):

1. Indicação do DPO – Data Protection Officer;
2. Possibilidade de confirmação e limitação/oposição ao tratamento, acesso, alteração ou exclusão do Dado Pessoal;
3. Limitação do uso do Dado Pessoal, conforme finalidade;

4. Possibilidade de retirada do Consentimento, pelo Titular do Dado Pessoal, em qualquer momento, sem comprometer a lícitude do tratamento efetuado, previamente, com base no Consentimento anteriormente dado;

5. Pseudonimização/anonimização;

6. Informação de quais Dados Pessoais são coletados;

7. Informação sobre para quem os Dados Pessoais serão divulgados/revelados;

8. Finalidade específica e explícita de Tratamento do Dado Pessoal e o fundamento jurídico;

9. Existência de Coleta de Dados Pessoais Sensíveis (Em destaque);

10. Informações de identidade e contato do Controlador disponíveis e, se aplicável, do seu representante;

11. Possibilidade de o titular dos dados não fornecer Consentimento e as consequências dessa negativa;

12. Responsabilidades do Controlador;

13. Informações sobre o Uso Compartilhado de Dados pelo Controlador e sua Finalidade.

15. Se não atender à Conformidade da Lei 13.709/18, quais as consequências?

O Art. 52, da LGPD, preceitua as consequências da **Não Conformidade**, ou seja, as penalidades que poderão ser aplicadas, a princípio, por infração:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas, às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas, aplicáveis pela Autoridade Nacional:

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

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica, de direito privado, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração, após devidamente apurada, e confirmada, a sua ocorrência;

V - bloqueio dos dados pessoais, a que se refere a infração, até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO);

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração, pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019);

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração, pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

É importante esclarecer que a atuação da ANPD se trata de processo administrativo, que independe de eventual processo civil, criminal e denúncias em órgãos como o Procon.

Além disso, tanto o **Controlador como o Operador podem responder por incidentes, quando:**

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde, solidariamente, pelos danos causados pelo tratamento, quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no Art. 43 desta Lei;

II - os controladores que estiverem, diretamente, envolvidos no tratamento, do qual decorreram danos ao titular dos dados, respondem, solidariamente, salvo nos casos de exclusão previstos no Art. 43 desta Lei.

16. Quais são os direitos dos titulares de dados e por que conhecê-los?

O Art. 18 elenca os direitos dos titulares, sendo de extrema importância que as empresas se preparem, e disponibilizem, os meios que permitam, ao titular, exercer seus direitos:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer Consentimento e sobre as consequências da negativa;

IX - revogação do Consentimento, nos termos do § 5º do Art. 8º desta Lei.

Além disso o Controlador deve considerar o **Art. 9º**, em atendimento ao **princípio do Livre Acesso**, o que versa sobre o direito de **acesso facilitado** às informações sobre o tratamento de seus dados. Estes deverão ser disponibilizadas, de **forma clara, adequada e ostensiva**:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no Art. 18.

17. Quem é o Encarregado pela Proteção de Dados Pessoais - DPO?

O **Encarregado** pela Proteção de Dados Pessoais é a função instituída, pela própria Lei, que, a princípio, deveria ser exercida, apenas, por uma pessoa natural/física, mas que mudou, devido à Medida Provisória e atual Lei 13.853/19, possibilitando que seja um serviço terceirizado.

Uma das funções principais do encarregado é ser o canal de comunicação entre o Controlador, os Titulares de Dados e a Autoridade Nacional (art. 5º, VIII).

As atividades do Encarregado envolvem:

- I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações da autoridade nacional e adotar providências;
- III - orientar os funcionários e os contratados da entidade, a respeito das práticas a serem tomadas em relação à **Proteção de Dados Pessoais**;
- IV – executar as demais atribuições, determinadas pelo Controlador ou estabelecidas em normas complementares (Art. 41, §2º).

Importante ressaltar que a identidade e as informações de contato do Encarregado deverão ser divulgadas, publicamente, de forma clara e objetiva, preferencialmente, no site do Controlador (Art. 41, § 1º).

18. O que é o dever de Report?

O dever de *Report* é a obrigação trazida pelo Art. 48 da LGPD, que preceitua que todo incidente, que possa acarretar risco ou dano relevante ao titular, deverá ser informado à ANPD e aos titulares dos dados.

Uma observação importante é que o **Operador sempre deverá notificar o Controlador, sem demora, após tomar conhecimento de uma violação de dados pessoais.**

A LGPD fala em prazo razoável e não determina, em dias, até quando deverá ser feita a Comunicação ao Controlador e Titular. No entanto, é bem provável que a própria ANPD estipule o prazo a ser atendido. Enquanto isso não acontece, sugerimos que a comunicação seja feita, imediatamente, após tomar ciência e apuração real dos fatos.

Os tipos de violações de dados pessoais, que geram elevado risco para os titulares, seriam:

- a) exposição (que é, praticamente, o vazamento);

- b) perda (que é quando os dados pessoais são eliminados, seja por apagamento, indisponibilidade (como é o caso de ficar criptografado) ou perda do dispositivo em que estavam armazenados e não se tem o backup);
- c) uso indevido e/ou ilícito (que pode ocorrer porque foi usado para uma finalidade não informada, sem transparência, ou, então, foi usado por um terceiro não autorizado, ficou da posse de um hacker e/ou foram roubados).

Portanto, um exemplo de fácil entendimento seria o sequestro de dados, assim como ocorreu com algumas empresas com o *Ransomware WannaCry* que, após criptografar o banco de dados, de diversas empresas, os criminosos pediam por resgate em *bitcoins*.

No report, a informação encaminhada deverá ocorrer por um Relatório de Impacto, onde deverá constar:

- I - a descrição da natureza dos dados pessoais afetados;
 - II - as informações sobre os titulares envolvidos;
 - III - a indicação das medidas técnicas e de segurança, utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
 - IV - os riscos relacionados ao incidente;
 - V - os motivos da demora, no caso de a comunicação não ter sido imediata;
 - VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- § 2º A Autoridade Nacional verificará a gravidade do incidente e poderá, caso necessário, para a salvaguarda dos direitos dos titulares, determinar, ao Controlador, a adoção de providências, tais como:
- I - ampla divulgação do fato, em meios de comunicação;
 - II - medidas para reverter ou mitigar os efeitos do incidente.

19. Como manter a Segurança da Informação na Proteção de Dados Pessoais

Assim como mencionado nos princípios trazidos pela LGPD, a Segurança dos dados pessoais, que significa Segurança da Informação (SI) é um requisito que não pode ser negligenciado. Tem, como base, três pilares: **Integridade, Confidencialidade e Disponibilidade.**

Com o decorrer do tempo, espera-se que a ANPD delibere sobre os requisitos de SI, mas, enquanto isso não acontece, tomam-se, por base, as boas práticas mundiais sob o alicerce da Norma ABNT ISO 27001 e 27002 e a nova Norma ISO IEC 27701:2019 atualizada para Proteção de Dados Pessoais.

Para contribuir com a blindagem da Segurança da Informação, no quesito Privacidade e Dados Pessoais, apresentamos uma sugestão de checklist:

- A Empresa considera todas as questões da legislação (Consentimento, Transferência, Tratamentos, Retenção, etc.) em suas trilhas de auditoria?
- A Empresa mantém registro de todas as atividades de Tratamento de Dados Pessoais?
- A Empresa monitora os ambientes físicos, lógicos e virtuais onde os Dados Pessoais estão disponíveis?
- A Empresa confirma, em dupla verificação, se os Dados Pessoais armazenados, em um recurso tecnológico, foram eliminados, de forma definitiva, antes do descarte ou reutilização do recurso?
- A Empresa realiza a gestão do ciclo de vida dos Dados Pessoais, incluindo a criação, duplicação, transmissão e descarte ao término da finalidade?
- Todos os sistemas da Empresa refletem as políticas e procedimentos de legitimação de processamento dos Dados Pessoais?
- A Empresa utiliza técnicas de Pseudonimização ou Anonimização de Dados Pessoais, sempre que necessário?

- Os Dados Pessoais existentes, de forma repetitiva, em diversos sistemas, possuem algum processo de consolidação eletrônica e com qualidade assegurada?
- A Empresa realiza a Avaliação ou Relatório de Impacto sobre a Proteção de Dados, nos casos previstos na legislação ou definidos pela Autoridade Nacional, antes de iniciar o tratamento?
- A Empresa reporta o resultado das Avaliações de Impacto sobre a Proteção de Dados ao Encarregado?
- A Empresa mantém o Plano de Resposta a violações de Dados Pessoais, formalizado e divulgado aos colaboradores?
- A Empresa garante que o Plano de Resposta, a violações de Dados Pessoais, contém a forma de notificação, às autoridades competentes e aos Titulares de Dados?
- A Empresa mantém uma equipe treinada para responder os incidentes relacionados a violações de Dados Pessoais?
- A Empresa mantém o controle da rastreabilidade dos incidentes relacionados aos Dados Pessoais?

20. A LGPD aplica-se apenas à Coleta e Armazenamento em ambiente eletrônico?

A LGPD se aplica a todos os Dados Pessoais e Sensíveis, independente do meio de Coleta ou Armazenamento e, tampouco, das ferramentas utilizadas, para qualquer outro tipo de Tratamento. Além disso, aplica-se, também, ao legado que, por sua vez, terá que ser legitimado. Isso quer dizer que dados coletados, anteriormente à vigência da Lei, também precisarão ser analisados, e legitimados, no sentido de identificar as hipóteses legais ou necessidade de obtenção do Consentimento do titular.

07

ANEXO II FICHAS E CADASTROS

Apresentamos, a seguir, alguns exemplos na Identificação de Categoria de Dados:

1. Ficha Cadastral

Dados Pessoais

Detalhes do Cliente			
Cliente	Dado Pessoal	Nome:	Data de nascimento
CEP		Endereço:	Dado Pessoal
Bairro	UF:	No.	Compl.
Fone1 Tipo	Dado Pessoal	()	
Fone2 Tipo		()	
Fone3 Tipo		()	
Email		SCORE	SMD

Endereço e complemento, que possibilitam identificar o proprietário do imóvel.

Em um banco de dados, com outra informação, poderá ser considerado Dado Pessoal.

Dados Pessoais

Física/Jurídica	Nacionalidade *	Dado Sensível
Profissão	Time Futebol	
Escolaridade	Sexo *	Dado Sensível
RG / INSC.	No. Pessoas Fam.	
Org. Exp.	Estado Civil *	Dado Sensível
CPF/CNPJ	Não permitir contato por	<input type="checkbox"/> Telefone <input type="checkbox"/> Corresp. <input type="checkbox"/> Email
Insc. Municipal	Contato	Dado Sensível
	Situação	<input type="checkbox"/> Inativo
	Renda Mensal	
	Atividade	
	Área Geográfica	

Alguns dados podem ser considerados dados pessoais no contexto de um grupo, caso ele possa identificar um titular ou ainda que de forma indireta seja identificador quando, agregado a outra informação.

Atenção, pois ainda que seja uma ficha de pessoa jurídica, pode conter dados pessoais de sócios, diretores ou qualquer outro representante.

Área Geográfica: Fax: Nr. Pessoas/Família:

Diretor: Dado Pessoal **Contato:** Dado Pessoal **Nome Fantasia:**

Cliente do Grupo: **Sócio/Procurador:** Dado Pessoal

Habilitação: Dado Pessoal **Categoria:** **Renda Mensal:** ,,00

Programa de Pontos
Nº Cartão: Dado Pessoal **Pt. Acumulados:** ,,,00 **Resgate (R\$):** ,,,00

Plus
Adic. Pts.: ,,,00 **Motivo:**

Endereço de Cobrança
Endereço: Dado Pessoal **+ Adicion.**
Nr: **Complem.:** **UF:** **- Classif.**
Cidade: **Bairro:** **CEP:** - - **Situação**
Telefones: Dado Pessoal **Cadastro**
Tipo Tel. : <NENHUM> **<NENHUM>** **<NENHUM>**

Informações Bancárias
Banco: **Agência:** **Conta:** **Default Identificador:**
+ Adicion. **Serviço**
Excluir **Peças**

Cliente : **CPF/CGC:** Dado Pessoal **+ Adicion.**

Tipo
 Física Jurídica Departamento Seguradora Montadora Concessionária Governo

Cod. Conces. Montad.: **Cod. Fábrica:** **Fabricante:**

Nacion.: * **RG/Passaporte:** Dado Pessoal **Órgão Exp.:**
Insc. Mun.: **IE Prod Rural:** **Dt Nasc.:** Dado Pessoal
Insc. Ant.:

CEP: * **UF:** **Cidade.:** *
Endereço: * **Dados Pessoais** **Nr.:**
Bairro: * **Comp.:** **Permitir divulgação de E-Mail**
E-Mail: *

Tel.(DDD): Dado Pessoal **Tipo Tel.:** <NENHUM>

Sexo: * Dado Sensível **Estado Civil:** *
Escolaridade: * **Profissão:** *
Faixa de Renda: * **Atividade:** *

2. Proposta de Compra de Veículos

Página:	1				
Emissão:					
FONE: CNPJ: INSC.ESTADUAL:					
PROPOSTA DE COMPRA DE VEÍCULO - NR. 00					
Vendedor: Dado Pessoal	Emissão da Proposta: Prev. Entrega Veic.:				
IDENTIFICAÇÃO DO PROPONENTE					
Cliente: Dados Pessoais	CNPJ/CPF: Dado Pessoal	Ident./Inscrição: Dado Pessoal			
Endereço:	Cidade:	Estado:			
Bairro:	CEP:	Telefone: Dados Pessoais			
Código:	Data Nasc.: Dados Pessoais	Fax: Dado Pessoal			
Celular:	Cônjugue: Dados Pessoais	Data Nasc.: Dado Pessoal			
Email Casa:	Email Trab:				
IDENTIFICAÇÃO DO VEÍCULO					
Veículo:	Modelo:	Cor:			
Ano Fab/Mod:	Chassi: Dado Pessoal	Combustível:			
Cod. Modelo:	Marca:	Nota Entrada:			
Pacote/Catálogo:	Placa: Dado Pessoal				
Situação:	Opcionais do Veículo				
Código	Descrição	Valor	Código	Descrição	Valor
DESCRÍÇÃO DO(S) VEÍCULO(S) USADO(S) (PARA TROCA)					
Placa	Modelo	Cor	Valor	Fab/Mod	Chassi
VALORES / CONDIÇÕES DE PAGAMENTO					
Valores de Venda			Financiamento		

08

ANEXO III – O QUE NÃO PODE FALTAR NO RELATÓRIO DE IMPACTO

Por certo que, na prática, o **Relatório de Impacto** pode ser bem mais complexo do que os dados a seguir apresentados, pois trata-se de uma sugestão inicial, de forma que cada empresa deverá criar o seu próprio **DPIA**, sem esquecer dos pontos básicos.

ROTEIRO DE REFERÊNCIA PARA O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - DPPIA

Identificação do Controlador	
Nome do Encarregado de Dados (DPO)	
Contato do encarregado	

DESCRIÇÃO DO PROJETO

IDENTIFICAÇÃO E JUSTIFICATIVA PARA O DPPIA

NATUREZA E ESCOPO DO TRATAMENTO	
Quais Dados Pessoais são coletados?	
Quais Dados Sensíveis são coletados?	
Envolve Dados Pessoais/Sensíveis de Vulneráveis ou menores de 18 anos?	
Envolve Dados Pessoais de terceiros?	
Qual a natureza do relacionamento entre Controlador e Titular?	
Quais os meios de coleta?	
Quais sistemas são utilizados para o tratamento dos dados?	
Qual a finalidade da coleta? (mentornar se há outra maneira de alcançar o resultado)	
Qual a base jurídica da coleta?	
Há benefícios para Controlador ou terceiros?	
Qual o volume de dados?	
Qual o prazo de tratamento?	
Há compartilhamento?	
Há Transferência internacional?	
Área geográfica a ser prevista/atingida:	
Há monitoramento de dados pessoais/sensíveis?	
Há decisões automatizadas?	
Há informações de <i>score</i> ?	
Envolve contato futuro?	
Envolve tratamento de dados financeiros?	
Envolve migração de sistema?	
Há conhecimento de incidentes anteriores, com o mesmo tipo de tratamento?	

AÇÕES PARA CONFORMIDADE E MITIGAÇÃO DE RISCO	
Riscos identificados para cada tratamento (mentornar nível de criticidade e probabilidade):	
Medidas de salvaguarda e impacto:	
Sistemas de Segurança:	
Ações de Sensibilização:	
Ações de Capacitação:	
Plano de Ação:	
Ações para atender aos princípios do Art. 8º. :	
Há hipótese de tratamento com base no Consentimento? Como será esta coleta?	
Recomendações para os Titulares:	
OPERADORES	
Haverá tratamento de dados por Operadores?	
Descrever tratamento:	
Identificar Operadores:	
Descrever responsabilidades:	
É empresa nacional ou internacional?	
Tem escritório no Brasil?	
Quais medidas serão tomadas para garantir que os Operadores estão em conformidade com a LGPD?	
Descrever se operadores já estiveram envolvidos em incidentes de vazamento de Dados Pessoais:	
EQUIPE DE PROTEÇÃO DE DADOS PESSOAIS	
Quantas pessoas existem na equipe de Proteção de Dados Pessoais?	
Quais são as áreas envolvidas?	
Há contratação de terceiros para apoio à equipe (identificar)?	
DADOS DE APROVAÇÃO/RECUSA INTERNA	
Quem apresentou o projeto:	
Parecer do DPO:	
Aprovado pelo comitê (integrantes):	
Data de Aprovação:	

ANOTAÇÕES



Este Guia de melhores práticas para aplicação da Lei Geral de Proteção de Dados – LGPD é uma publicação da FENABRAVE – Federação Nacional da Distribuição de Veículos Automotores elaborada em março de 2020.