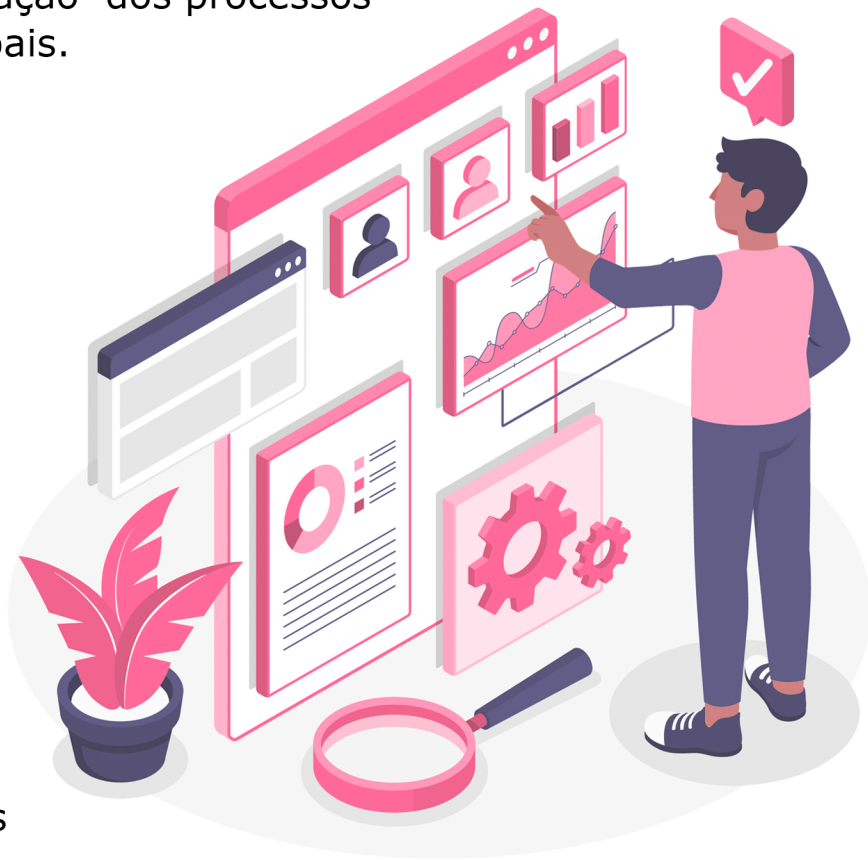
eBook
LGPD
Princípios básicos

CONTACT PRO

Olá, cliente Contact PRÓ. Tudo bem?

Elaboramos esse eBook para compartilhar com você como desenvolvemos o nosso Programa de Governança em Privacidade e realizamos a adequação dos processos da Contact PRÓ à LGPD – Lei Geral de Proteção de Dados Pessoais.



A Contact PRÓ é uma empresa familiar, que atua no mercado brasileiro oferecendo soluções de Marketing, Vendas, Cobrança e Pesquisa por meio da prestação de serviços personalizados para a necessidade de cada cliente, pelo uso de tecnologias de softwares modernas, rápidas e com excelentes níveis de assertividade.

Nosso objetivo é aproximar nossos clientes de outras pessoas, sejam elas naturais ou jurídicas, permitindo a criação de laços e interações que ampliem as comunicações e gerem oportunidades.

Para a prestação dos nossos serviços a matéria prima são os dados, sejam eles pessoais ou não. Os dados são tratados pela Contact PRÓ para que possam gerar informações preciosas para nossos clientes, que transformam estas informações em conhecimento e em negócios.

De onde são os dados tratados pela Contact PRÓ?

Os dados tratados nos serviços realizados pela Contact PRÓ são provenientes de três fontes:

1. Dados levantados pela Contact PRÓ para atendimento das necessidades de clientes:

Quando nosso cliente contrata os serviços de mailing, que consiste na pesquisa e extração pela Contact PRÓ de dados de fontes públicas ou dados tornados manifestamente públicos pelo titular e na organização destes dados em tabelas operacionalizáveis (formato Excel), entregamos, em poucos dias, o resultado do levantamento realizado para que o cliente possa realizar suas operações com o público-alvo identificado no mailing. Esses serviços ajudam nossos clientes a formarem o banco de dados próprio.

Dica: *Esse banco de dados deve ser segmentado em grupos distintos: "leads" (termo para possíveis ou futuros clientes), "clientes ativos" e "clientes inativos", assim pode ser bem direcionado para cada tipo de comunicação.*

2. Dados fornecidos pelo próprio cliente:

A partir de bancos de dados que o cliente fornece, realizamos os serviços de **Higienização dos Dados** (atualizando ou enriquecendo o banco de dados com novas informações), **Disparo de Ligações Telefônicas**, **Disparo de Mensagens de WhatsApp** e **Disparo de Ligações por WhatsApp**.

Nestas ferramentas de contato, os dados do público-alvo indicado pelo cliente são inseridos nos softwares de comunicação e é realizada a operação durante o período contratado pelo cliente, sendo emitidos relatórios de desempenho, que possibilitam acompanhar a performance da ferramenta utilizada e do impacto de comunicação com o público.

Dica: *A mensagem disparada é produzida pelo cliente, então vale a pena preparar uma mensagem bem direcionada àquilo que se quer comunicar, com linguagem clara, direta e curta.*

3. Dados públicos, disponíveis em processos judiciais

São os dados que estão nos sistemas do Judiciário brasileiro, disponíveis para consulta pública e que podem ser acessados com o uso da ferramenta **Rastreador de Processos**, mediante a definição de perfil por tipo de processo, tipo de tribunal, região do país etc.

Dica: *Quanto mais definido o perfil de pesquisa na ferramenta, melhor o resultado do relatório.*

Quais tipos de dados são utilizados nos serviços da Contact PRÓ?

Os dados pessoais utilizados na realização dos serviços são aqueles classificados como dados comuns, não sendo utilizados dados sensíveis e nem dados de crianças e adolescentes.
É considerado dado pessoal qualquer informação relacionada à pessoa natural, que a torne identificada ou identificável.

Por exemplo, um banco de dados de cliente pessoa física está recheado de dados pessoais, enquanto um banco de dados de cliente pessoa jurídica pode ou não conter dados pessoais (nome e CPF do representante legal, nome e telefone da pessoa de contato na organização, são exemplos de dados pessoais que podem estar nesse banco de dados).

Os dados pessoais sensíveis são aqueles definidos pela LGPD (Lei nº 13.709/2018) como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Os dados de criança e adolescente são aqueles relacionados às pessoas com idade inferior aos 18 anos.

Dica: *Identifique aí na empresa quais são os tipos de dados pessoais utilizados nas operações e atividades. Essa informação é fundamental para atender à LGPD.*

Por que foi necessário fazer a adequação à LGPD?

A Contact PRÓ foi fundada em maio de 2020. Nasceu de operações realizadas desde 2015 por outras pessoas jurídicas já extintas, pertencentes aos sócios e que ofereciam soluções para a área de telecomunicações. Com o sucesso das atividades empresariais anteriores, os empreendedores promoveram uma reformulação empresarial, criando a Zappo Tecnologia da Informação e Publicidade Ltda, que adotou o nome fantasia de Contact PRÓ.

Esse nome inclusive veio do principal serviço prestado pelas empresas antecessoras. A LGPD é uma lei de agosto de 2018, mas que passou a vigorar no Brasil em setembro de 2020, trazendo um conjunto de normas para o tratamento de dados pessoais. A Contact PRÓ trata dados em geral, entre eles os dados pessoais. E por tratar dados pessoais, todas as atividades e operações da empresa passaram por uma avaliação de conformidade à LGPD.

Essa avaliação de conformidade foi feita pela realização de um mapeamento de processos e de dados utilizados nos processos (chamamos aqui esta etapa de **Data Mapping**), o que permitiu a realizaçãoda identificação de pontos de conformidade e pontos de não conformidade às regras trazidas pela Lei (essa fase foi chamada de **Gap Analysis**). Após esse diagnóstico inicial, realizamos o **Planejamento de Ações** para implantação das correções dos pontos com não conformidade e para melhorias naquilo que estava em conformidade, mas que poderia evoluir. Com esse processo, iniciamos o primeiro Ciclo PDCA do nosso **Programa de Governança em Privacidade.**

Imediatamente, os pontos de não conformidade passaram por uma correção e nos pontos de conformidade estamos implantando melhorias, para cumprir da melhor forma possível os preceitos que a LGPD traz e oferecer um ambiente de segurança da informação para os agentes internos e para nossos clientes.

Não pense que a Contact PRÓ parou por aí... O processo de conformidade à LGPD é permanente e contínuo. Estamos sempre nos perguntando como podemos fazer melhor para atender aos padrões trazidos pela LGPD e às regulamentações a essa legislação que estão sendo emitidas pela ANPD – Autoridade Nacional de Proteção de Dados Pessoais.

A ANPD é a autarquia de caráter especial, criada na LGPD, componente do Poder Executivo Federal, que tem a função, entre outras, de regulamentar a proteção dos dados pessoais. Acompanhamos a evolução da regulamentação da LGPD e desde a sua criação estamos utilizando suas Resoluções, Enunciados, Notas Técnicas, Guias Orientativos, Relatórios e Estudos Técnicos para aprimorar nossas atividades, adequando sistematicamente nossos processos internos e externos.

Dica: *A implantação da LGPD requer conhecimento específico e aprofundado. Se não contar com profissionais capacitados para a implantação do Programa, é interessante a contratação de consultoria externa, a realização de cursos de capacitação ou a seleção desse profissional para sua organização.*

Esse Programa é exclusivo para a Contact PRÓ?

Mesmo sendo personalizado e direcionado às atividades da Contact PRÓ e aos agentes internos da empresa, que são treinados para conhecer a LGPD e seus padrões, e para utilizar as medidas de segurança e de privacidade da informação para proteger os dados, a boa prática indica que a empresa deve se preocupar também com o alcance da aplicação do programa nas suas relações externas.

Por isso, uma das medidas utilizadas na Contact PRÓ é a disseminação de conhecimentos para seus clientes e fornecedores, motivo de criação deste material informativo e de publicações em nossas redes sociais, com temas específicos de LGPD que volta e meia produzimos e compartilhamos.

O que vamos compartilhar nas próximas páginas?

Informações importantes sobre a LGPD
e dicas práticas para a sua implantação.

Caro cliente, agradecemos a leitura deste material informativo e nos colocamos à disposição para esclarecimentos, compartilhar conhecimentos, receber suas contribuições e experiências.

Saudações!

Contact PRÓ

LGPD – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E BOAS PRÁTICAS

Onde encontro o texto da LGPD?

É importante que você conheça a LGPD em fonte oficial,
por isso indicamos o site do Planalto:
www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Lá você encontra a LGPD, que é a Lei 13.709, de 14 de agosto de 2018, em duas versões: a completa, com a indicação de todas as modificações que a Lei sofreu desde 2018 (essas modificações aparecem nos textos tachados) e a compilada, com o texto limpo, sem a indicação das modificações. Ambas as versões estão atualizadas e essa é a importância de utilizar essa fonte oficial e atualizada, afinal não devemos estudar a LGPD por meio de um texto defasado.

Dica: *Uma boa prática a ser implantada na organização é que sempre seja utilizada a versão mais recente de documentos internos e demais normativas, evitando-se a aplicação de práticas já defasadas.*

Como devemos tratar os dados pessoais para atender o que está contido na LGPD?

Se a gente pudesse responder isso de forma simples (o que não é possível), escolheríamos o artigo 6º da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios". Aprendemos, na implantação do Programa de Governança em Privacidade da Contact PRÓ, que se a gente mantiver os princípios da LGPD na nossa mente, nos preocupando se as nossas operações atendem a todos eles, já estaremos com grande parte da tarefa de proteção dos dados pessoais bem feita.

O princípio trazido no início do artigo 6º é super importante: a boa-fé. Entendemos que esse princípio indica que devemos considerar os nossos interesses e os interesses dos titulares de dados pessoais (as pessoas naturais às quais os dados estão conectados e que são os proprietários destes dados), de forma que não tenhamos danos, não sejam infringidos direitos e que o uso dos dados traga benefícios às partes envolvidas no processo.

A boa-fé também é aplicada na relação com os nossos clientes, que são os controladores do uso dos dados pessoais que estamos tratando. Entendemos que nossos clientes utilizarão os dados pessoais encontrados nos relatórios de mailings para formar o banco de dados de suas organizações e que estes dados serão utilizados para fins lícitos, legítimos, legais. Por isso, sempre que um cliente orça um serviço com a Contact PRÓ solicitamos que seja indicada a finalidade de uso dos dados pessoais. Se percebemos que a finalidade é incompatível com a boa-fé e legalidade, preferimos não realizar o serviço.

Gostamos de aplicar os demais princípios em grupos, que apelidamos assim:

1. O grupo de princípios de coleta e tratamento de dados pessoais:

FINALIDADE:

É necessário um motivo real e lícito para coletar e utilizar dados pessoais, o que a LGPD chama de "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

São exemplos coletar e utilizar dados pessoais com a finalidade de celebrar um contrato com o titular; coletar e utilizar dados pessoais para realizar uma campanha de marketing dos produtos da empresa; coletar e utilizar dados pessoais para encaminhar a contratação de um funcionário.

ADEQUAÇÃO:

Refere-se à quando e como devo coletar/usar os dados (momento certo e meio correto), e se há compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Devo coletar a foto do colaborador no momento do processo seletivo ou somente quando da contratação? Quais dados são adequados para a campanha de marketing? Preciso da data de nascimento quando da celebração do contrato com o titular? Sim, pois ele pode ser uma criança ou adolescente, o que impede a contratação direta com essa pessoa.

NECESSIDADE:

Só devem ser coletados/utilizados os dados realmente necessários para atingir a finalidade definida. A LGPD indica a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Por exemplo, para a definição de perfil de clientes a serem atingidos na campanha de marketing, definimos os dados "nome, sexo, idade, telefone, e-mail e cidade", para que possamos atingir, na campanha a ser remetida por ligação de telefone e disparo de e-mail, o público masculino, de 20 a 40 anos, que reside no mesmo munícipio da sede da nossa nova loja de artigos masculinos esportivos.

2. O grupo de princípios da relação com o titular:

LIVRE ACESSO:

Ao titular deve ser garantido o acesso simples e gratuito aos seus dados pessoais, bem como ter informação sobre a forma e a duração do tratamento realizado. Afinal, se o titular é o "dono" dos dados pessoais, deve poder acessá-los e ter conhecimento do uso que é feito com a sua "propriedade".

TRANSPARÊNCIA:

Significa mostrar para o titular porque os dados pessoais são coletados e utilizados pelos agentes de tratamento, por meio de informações claras, precisas e facilmente acessíveis. Aqui vale a honestidade com o titular.

Dica: *Sabe aquela pergunta "de onde vocês conseguiram o meu contato"? Essa resposta deve ser o mais sincera possível: conseguimos seu contato no nosso cadastro de clientes... conseguimos seu contato por meio de levantamento em dados públicos e dados tornados públicos pelo titular... realizamos uma pesquisa de perfil na internet e identificamos você e os seus dados de contato... outro cliente nosso, o José, indicou você como possível interessado no nosso serviço... seus dados foram disponibilizados por nosso parceiro comercial, a empresa XXX.*

QUALIDADE DOS DADOS:

Trata-se de que os dados pessoais devem ser mantidos atualizados e fidedignos, livres de incorreções e incongruências. A LGPD traz como a garantia para o titular ter os seus dados tratados com exatidão, clareza, relevância e atualização, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

O serviço que a Contact PRÓ realiza de higienização do banco de dados é bem importante para cumprir esse princípio. Quando do atendimento dos clientes, é sempre interessante confirmar os dados de cadastro, mantendo-os atualizados e corretos.

Dica: *Cuidado com as incorreções na digitação de informações, afinal, para os sistemas informatizados Souza e Sousa são dois cadastros distintos, portanto é imprescindível que os nomes e demais dados sejam registrados corretamente.*

NÃO DISCRIMINAÇÃO:

Impedir que os dados sejam utilizados para finalidades discriminatórias ilícitas ou abusivas. Vamos combinar: discriminação não cabe em nenhuma operação de uma organização, seja ela por preconceito de raça, credo, sexo ou qualquer outro quesito.

Dica: *Não discriminação não quer dizer que não seja possível o perfilamento de público: aqueles que possuem ou não determinada renda; aqueles que possuem ou não determinada formação escolar; aqueles que possuem ou não habilitação técnica para o desempenho da atividade. Cuidado com os dados sensíveis, pois eles podem ser facilmente fontes de discriminação.*

3. O grupo de princípios do controle e proteção dos dados:

SEGURANÇA:

Refere-se a utilizar os meios mais seguros possíveis para coletar/tratar dados, evitando ao máximo os riscos de incidentes de segurança (internos ou externos). Afinal, se vamos tratar os dados que pertencem aos titulares, temos que utilizar medidas se segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Dica: *Estabelecer um processo de gerenciamento dos riscos de segurança da informação na empresa é fundamental para cumprir com esse princípio.*

PREVENÇÃO:

Significa buscar permanentemente medidas para evitar ocorrência de danos aos titulares dos dados pessoais. Convém lembrar que esses danos podem acontecer em razão de falhas nos sistemas informatizados, mas também em razão de ameaças humanas, intencionais ou não.

Dica: *Não se esqueça de treinar as pessoas da organização para a cultura da proteção dos dados, pois a maior causa de incidentes de segurança da informação são as ações humanas.*

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:

Os agentes de tratamento de dados pessoais são responsáveis pelo tratamento que realizam, devendo responder perante o titular e perante as autoridades sobre a regularidade do tratamento, a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia das medidas de segurança que emprega no tratamento dos dados.

Para que seja possível prestar contas é necessário ter as informações sobre a segurança da informação de maneira organizada e documentada na empresa.

Dica: *A implantação de um SGSI – Sistema de Gestão de Segurança da Informação, combinado com um SGPI – Sistema de Gestão de Privacidade da Informação ajuda muito na organização e prestação de contas aos agentes internos e a terceiros.*

Muitas outras ações devem ser adotadas numa organização para atingir, no máximo possível, a proteção dos dados pessoais, mas isso depende da estrutura, escala e volume de suas operações, bem como da sensibilidade dos dados tratados.

Um estabelecimento de saúde (muitos dados sensíveis) é muito diferente de uma escola (muitos dados de crianças e adolescentes) e muito diferente de uma loja de material elétrico (muitos dados comuns), sendo que em cada uma destas organizações há a necessidade de medidas personalizadas para a realização dos processos com dados pessoais em cumprimento da LGPD.

O que devemos observar para avaliar a conformidade das operações à LGPD?

No processo que fizemos da Contact PRÓ levamos em consideração os seguintes requisitos:

a. Aplicabilidade da LGPD ao processo mapeado: nisso os artigos 3º e 4º da LGPD são os nossos guias.

b. Atendimento aos princípios da proteção de dados pessoais: com base no artigo 6º da LGPD, avaliamos se todos os nossos processos atendiam aos princípios.

c. Classificação dos dados pessoais e identificação das hipóteses de tratamento conforme os artigos 7º, 11 e 14 da LGPD: em cada processo identificado, mapeamos os dados pessoais utilizados e realizamos a classificação. No nosso caso, encontramos somente dados comuns. E nesses dados, identificamos qual era a hipótese de tratamento que fundamentava a operação com os dados pessoais (aquelas do artigo 7º).

d. Gestão do consentimento: identificamos nas operações cuja hipótese de tratamento seja o consentimento, se havia a gestão desse consentimento nos moldes dos artigos 7º, 8º, 9º, 15 e 19 da LGPD. E, quando não estava bem feita a gestão do consentimento, elaboramos termos de consentimento mais bem redigidos para a utilização na empresa e processos internos para gerenciar essas autorizações.

e. Aplicação do legítimo interesse do controlador ou de terceiro nas operações da empresa: verificamos em quais das operações da Contact PRÓ estava sendo aplicada a hipótese de tratamento prevista no artigo 7º, IX, da LGPD, e nessas operações aplicamos um Teste de Legítimo Interesse, bem como realizamos o Relatório de Impacto à Proteção de Dados Pessoais (o RIPD), atendendo ao artigo 10 da LGPD.

f. Ciclo de vida do tratamento dos dados pessoais e do seu armazenamento: para essas avaliações os artigos 15 e 16 da LGPD são os fundamentos. Descobrimos a importância da gestão documental na empresa, que deve levar em consideração a classificação da informação quanto ao seu valor ou importância (primário ou secundário), a temporalidade (de uso corrente, guarda intermediária, descartável ou permanente), o tipo de documento (impresso, digital e finalidade do documento), o nível de confidencialidade (sigiloso, privativo/confidencial ou público) e a natureza do assunto (ostensiva ou sigilosa).

g. Exercício de direitos pelo titular de dados pessoais: avaliamos quais os direitos do titular, previstos nos artigos 9º e 18 a 22, são possíveis de serem exercidos nos processos da empresa (sim, em decorrência da hipótese de tratamento dos dados pessoais em cada processo alguns direitos podem ou não ser configurados para o titular) e por quais meios eles podem ser exercidos. Implantamos na Contact PRÓ o canal de comunicação direta do titular com o Encarregado de Proteção de Dados Pessoais (lgpd@contactpro.com.br) e um processo interno de atendimento do titular, que o auxilie no exercício de seus direitos e, ao mesmo tempo, formalize o atendimento na Contact PRÓ e evite incidentes de segurança na realização desse processo (como a possibilidade de fraude na identificação do titular, por outra pessoa que não o verdadeiro titular, quando for solicitado o direito de confirmação, acesso e retificação de dados).

h. Transferência internacional de dados pessoais: identificamos nos processos da Contact PRÓ se existe a transferência internacional de dados pessoais e se ela atende aos requisitos do artigo 33 da LGPD.

i. Nomeação de Encarregado de Proteção de Dados Pessoais e suas competências: em atendimento ao artigo 41 da LGPD, verificamos a importância da nomeação do Encarregado de Proteção de Dados Pessoais e do papel de atuação na empresa. Já em setembro de 2020 nomeamos o nosso Encarregado, como está divulgado no site da empresa.

j. Segurança e boas práticas para a proteção de dados pessoais: em atendimento aos preceitos do artigo 46 a 50 da LGPD, foi possível identificar as condições de segurança da informação e de segurança da privacidade na empresa, e avaliar os riscos para a proteção das informações em geral e dos dados pessoais com relação a acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A implantação do SGSI-SGPI tem ajudado muito no cumprimento desta obrigação.

A Contact PRÓ não trata dados sensíveis, mas caso seja a realidade da sua organização, indicamos que faça a avaliação do tratamento de dados sensíveis nas operações da empresa, utilizando o enquadramento nas hipóteses de tratamento trazidas no artigo 11 da LGPD, bem como seja cumprido o artigo 38, que estabelece a necessidade de avaliação do tratamento dos dados sensíveis por meio do RIPD – Relatório de Impacto à Proteção dos Dados.

Se houver o tratamento de dados de crianças e adolescentes, que seja avaliado o atendimento ao artigo 14 da LGPD.

E se ocorrer compartilhamento de dados pelos órgãos públicos, que sejam observados os artigos 23 a 32 da LGPD.

O que são estas hipóteses de tratamento de dados pessoais?

São possibilidades de tratamento regular de dados pessoais que a própria LGPD traz para serem aplicados pelos Controladores e Operadores. Assim, o agente de tratamento fica "autorizado" a tratar os dados mediante o correto enquadramento da operação de tratamento na hipótese trazida na LGPD.

Basicamente, temos dois tipos de situações: aquelas em que se obtém o consentimento do titular do dado pessoal para realizar o tratamento do dado e aquelas em que esse consentimento não é necessário. Não se pode confundir a dispensa do consentimento para tratar o dado pessoal com a falta de transparência perante o titular, está bem?

Mesmo que não seja utilizado o consentimento, o titular tem o direito e o agente de tratamento tem o dever de informar o titular sobre os usos dos dados pessoais nas operações da empresa. Por isso que esses usos devem ser divulgados a público na Política de Privacidade da empresa.

Dica: *Não confunda Política de Privacidade (que é mais abrangente e engloba todas as operações da empresa com dados pessoais) com a Política ou Termos de Uso do site, que explicam somente o que é tratado no site.*

Bom, você já entendeu que obter o consentimento do titular é uma hipótese de tratamento de dados pessoais, que cabe tanto para dados comuns (art. 7º, I) quanto para dados sensíveis (art. 11, I) e dados de crianças e adolescente. Mas nem sempre é necessário, conveniente ou possível obter esse consentimento.

Por exemplo, quando tratar o dado for uma obrigação legal da empresa (por exemplo, para registrar a CTPS do empregado) não será necessário obter o consentimento.

Quando não for conveniente obter o consentimento para tratar o dado: o problema está em que o consentimento pode ser revogado a qualquer momento, e em determinadas situações, como o armazenamento dos registros de saúde em prontuários, não é possível parar de tratar o dado pessoal, não sendo conveniente o uso do consentimento.

E há situações em que não é possível obter o consentimento antes de realizar a operação, como é o caso do uso de dados de leads para a realização de campanhas de marketing, pois nem sempre o dado é obtido diretamente com o titular e, portanto, antes mesmo de impactá-lo com o primeiro contato, o dado pessoal já está sendo tratado pelo agente de tratamento.

Dica: *Quando a hipótese de consentimento for a escolhida para a realização da operação, é dever do agente de tratamento de dados manter o registro do consentimento, seja esse registro impresso ou digital. Isso é super importante, pois o consentimento pode ser revogado e por isso a revogação deve estar "colada" ao registro de autorização.*

Não sendo utilizado o consentimento, os dados pessoais classificados como comuns podem ser tratados utilizando-se as demais hipóteses de tratamento do artigo 7º da LGPD, que são as seguintes:

II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III. 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, observadas as disposições do Capítulo IV desta Lei;

IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.”

São hipóteses bastante comuns nas empresas privadas,
o uso de dados pessoais para o cumprimento de obrigações legais ou regulatórias (art. 7º, II), para a realização de etapas preliminares, celebração e execução de contratos tendo o titular como parte, seja ele como pessoa física ou como representante legal de pessoa jurídica (art. 7º, V), para o exercício de direitos via processo judicial, administrativo ou arbitral (art. 7º, VI), para o atendimento dos legítimos interesses da empresa (art. 7º, IX), para consulta aos órgãos de proteção de crédito, como o SERASA (art. 7º, X).

Se a empresa for da área da saúde, provavelmente utilizará a hipótese da tutela da saúde (art. 7, VII). E, em situações extraordinárias, as empresas utilizarão a hipótese do art. VII para situações de proteção à vida ou à incolumidade física do titular (imagine aqui a ocorrência de um acidente na empresa, seja com o funcionário, um cliente ou um fornecedor).

Se for o caso de sua empresa, tratar dados sensíveis, não sendo obtido o consentimento, é possível usar os dados nas seguintes hipóteses do artigo 11 da LGPD:

II. Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a. Cumprimento de obrigação legal ou regulatória pelo controlador;

b. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c. Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d. Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e. Proteção da vida ou da incolumidade física do titular ou de terceiro;

f. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.”

Podemos perceber que a LGPD traz várias possibilidades de utilização de dados pessoais sem a necessidade de consentimento prévio do titular.

Vamos a um exemplo:

Uso de câmeras de segurança no estabelecimento da empresa. As câmeras de segurança captam dados pessoais (imagens) considerados como dados biométricos e, portanto, dados sensíveis. Geralmente esses dados são gravados em equipamentos de segurança para que seja possível assistir as imagens de forma assíncrona.

Podem permanecer armazenados pela empresa por um tempo, desde que aplicadas as medidas de segurança contra acessos indevidos, e desde que o uso dos dados (das imagens) seja somente para a finalidade de segurança.

Seria muito difícil obter o consentimento de cada pessoa que transita nas dependências da empresa, principalmente se houver setor de atendimento ao público, portanto o art. 11, I (consentimento), não é indicado para a situação, e sim o art. 11, II, g.

Como você lê no artigo 11, II, g, a finalidade de uso deve ser compatível com a hipótese de prevenção à fraude e à segurança do titular, prevalecendo, no entanto, os direitos e liberdades individuais. Dessa forma, em setores onde cabe a intimidade do indivíduo, como os banheiros, vestiários, quartos, não devem ser instaladas câmeras, preservando-se esse direito fundamental.

Falando em direitos, quais são os direitos do titular de dados?

Podemos agrupar os direitos dos titulares em duas classificações: os direitos em geral e os direitos atrelados ao consentimento.

Nos direitos em geral, encontramos o direito à titularidade, isto é, à propriedade sobre os seus dados pessoais, e os direitos fundamentais de liberdade, de intimidade e de privacidade (esses direitos já estavam previstos na Constituição Federal).

Também são direitos em geral:

a. O direito à confirmação da existência de tratamento do dado pessoal pelo Controlador;

b. O direito de acesso do titular aos seus dados pessoais;

c. O direito de correção de dados incompletos, inexatos ou desatualizados;

d. O direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (você também pode chamar isso de direito ao esquecimento);

e. O direito à portabilidade dos dados a outro fornecedor de serviço ou produto (você já deve ter visto isso quando há a troca de operadora de celular, de plano de saúde, de seguro de vida etc.);

f. O direito à informação sobre o uso compartilhado dos dados pessoais;

g. O direito de oposição sobre o uso de dados pessoais pelo Controlador quando não for utilizada a hipótese de consentimento;

h. O direito à revisão de decisões em processos automatizados/robotizados (como é a aprovação de cadastro num aplicativo operado por inteligência artificial);

i. Direito de defender-se perante órgãos administrativos ou judiciais, de maneira individual ou coletiva.

Quanto aos direitos atrelados ao consentimento, temos os seguintes:

a. O direito à revogação do consentimento já manifestado;

b. O direito de receber informações claras e precisas sobre a finalidade do consentimento, sendo este nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca;

c. O direito de receber informações sobre a necessidade de manifestar o consentimento para o fornecimento de produto ou serviço e sobre as consequências da negativa do consentimento;

d. O direito de eliminação dos dados pessoais tratados exclusivamente com o consentimento do titular e desde que o Controlador não tenha a obrigação legal de guarda dos dados.

Para exercer seus direitos o titular deve comunicar-se perante o Controlador dos dados pessoais em primeira mão. Na Contact PRÓ esta comunicação deve ser feita para o Encarregado de Proteção de Dados Pessoais pelo e-mail: lgpd@contactpro.com.br.

Dica: Se o Controlador não atender ao titular, respondendo aos seus requerimentos, o titular poderá buscar a ANPD. Na ausência do Controlador, o titular poderá realizar seus requerimentos, subsidiariamente, perante o Operador dos dados pessoais.

Podem explicar melhor o que é Controlador e Operador de dados pessoais?

Sim, apesar de pertencerem aos titulares, os dados pessoais podem ser utilizados em diversas operações, pelas mais diferentes instituições ou profissionais, mas sempre atendendo os parâmetros da LGPD. Se contrariar a LGPD, a instituição cometerá um ilícito.

O nome que a LGPD deu para quem trata dados pessoais foi o termo "agente de tratamento" e refere-se a dois tipos: o Controlador de dados pessoais e o Operador de dados pessoais.

O Controlador de dados pessoais pode ser uma pessoa natural que trata os dados pessoais com finalidade econômica (ex.: profissionais liberais, autônomos, informais) ou uma pessoa jurídica, de qualquer natureza ou porte, e que utiliza os dados pessoais nas suas operações. Pode-se dizer que todo CNPJ corresponde a um Controlador de dados pessoais.

Assim, a Contact PRÓ ocupa a posição de Controladora de Dados Pessoais nas situações em que realiza operações em seu próprio benefício, por exemplo, quando realiza uma campanha de marketing para vender os serviços da Contact PRÓ.

É chamada de "Controladora de Dados Pessoais" porque coleta e utiliza dados pessoais que pertencem a um titular para a realização de operações que lhe beneficiam ou interessam. E esse tratamento dos dados é uma decisão deste agente, devendo controlar o uso dos dados dentro de suas atividades.

Por exemplo, quando a Contact PRÓ coleta dados pessoais porque necessita deles para a abertura de cadastro de cliente, fechamento do contrato de prestação de serviços e execução deste contrato.

Dica: *Para saber se a sua empresa é uma Controladora de dados pessoais responda a pergunta: a atividade a ser realizada com o dado pessoal será em proveito ou benefício da empresa ou será para o benefício de outra organização?*

Um Operador de dados pessoais é um terceiro contratado pelo Controlador de dados pessoais para a realização de atividades de tratamento com dados pessoais em seu benefício ou interesse, e sempre de acordo com as instruções dadas pelo Controlador.

Um exemplo, é quando uma empresa (Controladora de dados pessoais) contrata uma empresa de recrutamento e seleção de RH (Operadora de dados pessoais) para buscar novos empregados para as suas atividades.

Os candidatos às vagas são os Titulares de dados, a empresa de recrutamento e seleção é a Operadora dos dados dos candidatos, e a empresa contratante é a Controladora dos dados dos candidatos.

Trazendo para a relação com os clientes, quando a Contact Pró é contratada para a realização de um serviço em prol do cliente, essa prestação de serviços é uma terceirização, sendo que o Controlador dos dados é o nosso cliente, a Contact PRÓ é sua Operadora e o Titular é a pessoa impactada pelo serviço.

Assim, a extração de um dado pessoal apresentado em um mailing poderia ser feita pelo nosso cliente, mediante pesquisa na mesma fonte pública que nós utilizamos. Só que vale muito a pena para nossos clientes contratarem a terceirização desse serviço com a Contact PRÓ.

O que o cliente levaria meses para realizar, a Contact PRÓ, com a tecnologia que possui, leva poucos dias, e ainda apresenta o relatório do levantamento (da extração) organizado em planilha interoperável, com os dados solicitados pelo cliente, prontinha para uso nos sistemas e operações que beneficiem o cliente.

Quando o cliente contrata a ferramenta de disparo de ligações por WhatsApp ou por telefone, a mensagem que chega ao destinatário (ao titular) é a mensagem do nosso cliente, disparada para o banco de dados de nosso cliente, com impacto nas atividades do cliente. Nosso papel é fornecer o serviço do software de comunicação, ou seja, ser um Operador do nosso cliente, que é o Controlador do processo.

Como vimos, tanto o Controlador quanto o Operador de dados pessoais precisa estar e atuar em conformidade à LGPD, além de oferecer medidas de segurança para proteger os dados e as informações que foram tratados. Por isso, nossos esforços em oferecer aos clientes um ambiente de segurança, proteção dos dados pessoais e conformidade à LGPD, para que, na posição de Operador, possamos trazer tranquilidade e garantias para os Controladores.

Somos solidariamente responsáveis por proteger os dados pessoais dos titulares.
E a gente leva isso muito a sério!

Quais são as boas práticas de segurança da informação que devem ser utilizadas pelos agentes de tratamento de dados pessoais?

Cada organização deve ter a sua estrutura de segurança da informação considerando os recursos que estejam disponíveis, o tipo de atuação no mercado, os dados (tipo e volume) que são tratados na empresa.

A ANPD apresentou um documento que traz orientações para os agentes de tratamento de dados de pequeno porte (como as microempresas), para que possam estruturar a segurança da informação atendendo as melhores práticas internacionais de proteção para os dados pessoais e para toda a informação tratada na organização.

Dica: *Para acessar o documento completo visite:* ***https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf.***

São medidas de segurança, em resumo:

- A existência de Políticas de Segurança da Informação;
- A realização de ações de conscientização e treinamento;
- O gerenciamento dos contratos (incluindo nestas cláusulas de segurança da informação e de confidencialidade);
- O controle de acesso às informações e sistemas a partir do perfilcolaborador/agente;
- Regras de uso de criptografia, antivírus, backup;
- Existência de equipamentos de proteção como firewalls e filtros de aplicação;
- Registro de eventos e gerenciamento de vulnerabilidades;
- Regras para uso de dispositivos móveis e serviços em nuvem.

O uso das medidas ajuda a organização a diminuir os riscos quanto à segurança da informação e a proteger os dados pessoais contra eventos indesejados e incidentes.

Dica: *As medidas de segurança devem estar registradas em documentos da empresa, em manuais, em código de conduta ou regulamentos. E o treinamento da equipe interna deve ser realizado para que usem corretamente essas medidas.*

Mas mesmo com a aplicação de medidas de segurança, podem ocorrer incidentes envolvendo dados pessoais. Isso pode acontecer em qualquer empresa, pois, por mais que se previna e evite a ocorrência de eventos indesejados, eles acontecerão. Costumamos dizer que não existe o risco zero. Sempre haverá algum tipo e nível de risco quando lidamos com dados pessoais e informações.

E para enfrentar estas situações, é necessário que a empresa possua um Plano de Contingência, com medidas de resposta aos incidentes (o artigo 50, I, g, da LGPD traz esse requisito). Um plano de contingência é um planejamento de medidas a serem adotadas para ajudar a controlar uma situação de emergência.

Assim é possível minimizar os prejuízos e consequências negativas. Ele também é conhecido como plano de continuidade ou plano de recuperação. É uma importante ferramenta para minimizar o risco de inoperância de componentes essenciais de uma operação.

Trata-se de um documento composto por uma sequência de procedimentos necessários para fazer com que processos afetados por um evento negativo voltem a funcionar. Possibilita minimizar perdas, ajudando a restabelecer a normalidade, podendo ser a diferença entre sucumbir ou sobreviver a um desastre. Além disso, o Plano de Contingência orienta o comportamento da equipe interna em situações atípicas e traz visibilidade para os riscos corporativos. Treinar a equipe para essas situações é fundamental.

Estas situações atípicas podem ser do tipo que envolve os dados diretamente, como o impedimento de acesso aos ativos de informação da empresa nos equipamentos e sistemas de informação e comunicação, a perda de backup das informações, a perda, roubo ou extravio de equipamentos de TIC, o vazamento de dados pessoais tratados pela empresa.

Ou podem ser situações que envolvam a estrutura física da empresa e indiretamente comprometam os dados e informações, como incêndio na sede da empresa, vendavais, enchentes, inundações, vazamentos de água que impeçam o acesso ao ambiente físico da empresa, falta de energia elétrica, interrupção dos serviços de lógica (telefonia e internet).

Esperamos que nunca aconteça nenhuma dessas situações na sua organização, mas não custa estar prevenido!

Chamamos a atenção para os incidentes que envolvem dados pessoais.
Se houver qualquer possibilidade de dano ao titular de dados pessoais, o Controlador deverá comunicar o titular do dado sobre a situação, cumprindo o artigo 48 da LGPD.

Além do titular, a ANPD também deverá ser informada, mediante procedimento próprio chamado CIS – Comunicação de Incidente de Segurança, que você pode encontrar no site da Autoridade:
https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.

Se o incidente ocorrer ou for percebido pelo Operador dos Dados Pessoais, este deve comunicar imediatamente o Controlador dos Dados Pessoais para que sejam tomadas as medidas de contingência em conjunto.

Dica: *Prevenir é melhor que remediar, como diz o ditado... Mas quando a prevenção falhar, estar preparado para a remediação do incidente é uma exigência da própria LGPD.*

Concluindo...

Parece tanto coisa a ser feita, não é mesmo? Mas nós já passamos por esse processo e descobrimos que muito do que é necessário para cumprir a LGPD já vinha sendo feito na empresa.

O que a gente fez foi reconhecer isso, documentar, melhorar, ajustar algumas coisas (sim, a gente teve que fazer ajustes e continuamos fazendo sempre que a gente acha que pode fazer melhor).

Olhando para trás podemos dizer que evoluímos em termos de maturidade para tratar os dados pessoais, gerenciar os riscos, tomar decisões nos processos internos e externos. Estamos mais seguros e confiantes nas operações que realizamos como Controladora de Dados Pessoais e também como Operadora de Dados Pessoais. Sabemos quando desempenhamos um papel e outro nas atividades da empresa.

Apesar de mais tranquilos, estamos sempre alertas, realizando os ciclos de avaliação, identificando melhorias e treinando nossos agentes internos. A LGPD está presente no nosso dia a dia e nos ajuda a ser quem somos.

CONTACT PRÓ

Telefone: **(48) 3036-2530**

E-mail: **atendimento@contactpro.com.br**

Site: **www.contactpro.com.br**

@contactpro.business

/contactpro.bi

/contactpro-bi