Cartilha sobre a Lei Geral de Proteção de Dados para Associados ABF

ABF ASSOCIAÇÃO BRASILEIRA DE FRANCHISING

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações, sob o conhecimento de que qualquer disseminação, distribuição ou cópia deste conteúdo é proibida.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

SUMÁRIO

1. INTRODUÇÃO: O VALOR DOS DADOS PESSOAIS

Com o avanço da tecnologia e a sua presença cada vez mais marcante em nossas vidas, o fluxo de dados circulantes pelas redes vem tomando grandes proporções.

Não à toa, Clive Humby, um cientista de dados inglês, afirmou: "*data is the new oil*" (dados são o novo petróleo) – e anos depois, já em 2019, Ajay Bang, então CEO de uma grande companhia, complementou com maestria o discurso afirmando que "A diferença é que o petróleo um dia vai acabar".

As afirmações não poderiam ser mais acertadas: dados impulsionam, cada vez mais, os negócios, desde dos gigantes da indústria até dos pequenos do varejo, atingindo, inevitavelmente, o setor de franquias.

Tais dados (que podem incluir dados pessoais) são utilizados para conhecer melhor os clientes de um determinado estabelecimento, analisando seus hábitos de compra e direcionando produtos que podem ser de seu interesse; são utilizados também para compreender melhor o "gosto geral", analisando a performance de consumo de cada produto; e, também, para compreensão da percepção de uma marca por seu público, influenciando assim no lançamento de novos produtos, substituição de outros, e até a disposição de uma vitrine. São infindáveis as possibilidades.

Especificamente no setor de franquias, há grande interesse (pelo franqueador) em tais dados, que geram uma ampla inteligência de mercado – afinal, a franquia se estabelece na marca, em sua exposição e força.

Como comentamos, no meio de todos esses dados, existem dados pessoais: nome, documento de identidade (RG, CPF, *social security number*, número do bilhete de identidade, etc.), endereço de e-mail, telefone... são dados que são fornecidos, ora em um cadastro em um site, ora em um *e-commerce*, e muitas vezes em um cadastro efetuado quando do atendimento em uma loja – mas que nem sempre são utilizados para os fins que deveriam.

Por tantas vezes, *hackers* se apropriam, também, de tais dados, e passam a comercializá-los – afinal, são listas e mais listas de potenciais clientes a serem abordados.

E foi, com base nesse cenário, que pouco a pouco o uso que se dá a tais dados pessoais foi chamando cada vez mais a atenção, tendo os dados a sua importância ressaltada – concluindo-se serem uma extensão dos direitos mais básicos da personalidade humana.

Aos poucos, diversos países ao redor do globo editaram normas para regular o correto uso – e por conseguinte outorgar proteção – a tais dados pessoais. E no Brasil não foi diferente: aos 14 de agosto de 2018, foi promulgada a Lei Federal nº 13.709, também conhecida como "Lei Geral de Proteção de Dados" ou, por sua sigla, "LGPD".

E é, com base nesse cenário – e concomitantemente à entrada em vigor da LGPD – que nasce o Manual de Boas Práticas em Proteção de Dados da ABF, desenvolvido em parceria com o PG Advogados, cujo objetivo é apresentar, de forma concisa, as principais diretrizes da Lei, bem como as melhores práticas sobre proteção de dados pessoais, com base no conteúdo produzido pela *Global Privacy Assembly* (GPA) e pelo *European Data Protection Board* (EDPB), além das recomendações de segurança presentes nas ISOs 27001 e 27701.

2. MAS AFINAL, O QUE É A LGPD?

Conforme seu artigo 1º, a LGPD "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Daí se nota a importância recentemente atribuída pelo direito brasileiro aos dados pessoais: um *status* equiparado ao de direito fundamental.

Como o próprio dispositivo legal indica, o objetivo da Lei é regulamentar a forma com que dados pessoais são operacionalizados (o que a lei chama de "tratados") para assegurar que os donos de tais dados (a quem a lei chama de "titulares") tenham sua privacidade respeitada.

Com o advento da Lei, o Brasil entra no rol dos pouco mais de 100 países que buscam garantir aos dados pessoais algum nível de proteção, refletindo as tendências globais.

3. PRINCÍPIOS NORTEADORES

Como forma de garantir os direitos dos titulares de dados pessoais, a LGPD se baseia em alguns princípios norteadores, previstos em seu art. 6º e os quais, bem compreendidos, podem auxiliar na compreensão das diretrizes da Lei e, em especial, dos deveres e responsabilidades perante o titular e a própria ANPD. São eles:

I - finalidade: determina que o tratamento apenas será considerado regular se baseado em um propósito legítimo e específico, informado ao titular;

II - adequação: prevê que apenas podem ser tratados dados pessoais compatíveis com a finalidade informada ao titular;

III - necessidade: determina que sejam tratados apenas os dados pessoais pertinentes à finalidade informada ao titular;

IV - livre acesso: garante que os titulares possam consultar quais dados pessoais seus estão sob guarda do Controlador, bem como que sejam informados sobre a forma e duração do tratamento;

V - qualidade dos dados: garante aos titulares que seus dados serão mantidos corretos, devendo ser atualizados se corretos ou atualizados se não estiverem;

Você sabe o que é "tratar" dados pessoais?

A LGPD define o tratamento de dados pessoais como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" – ou, de forma mais simples e objetiva, tudo que se faz com algum dado pessoal (art. 5º, X).

VI - transparência: garante aos titulares que recebam, por meios mais fáceis, informações claras, precisas e acessíveis sobre a realização do tratamento e os agentes envolvidos;

VII - segurança: determina que os agentes de tratamento façam uso de medidas técnicas e administrativas para proteger os dados pessoais de qualquer incidente;

VIII - prevenção: impõe aos agentes de tratamento o dever de adotarem medidas para prever danos decorrentes do tratamento de dados pessoais;

IX - não discriminação: veda o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: determina aos agentes de tratamento que mantenham registro do cumprimento das normas de proteção de dados pessoais.

4. TODO DADO É UM DADO PESSOAL?

A LGPD define como dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável", ou seja, sempre que a informação que se tem permitir identificar uma pessoa (e é importante lembrar que estamos falando de pessoa natural, ou seja, pessoa física), essa informação é um dado pessoal.

Alguns dados pessoais são bem obviamente identificados, como o nome, o RG ou o CPF; outros são assim classificados em decorrência de sua relação direta com o titular, como o endereço, o e-mail ou o número de telefone.

Não existe um rol específico e objetivo; na prática, todo dado que, isoladamente ou em conjunto com outras informações, for apto a identificar alguém, direta ou indiretamente, será considerado um dado pessoal. Assim, podem também ser considerados dados pessoais uma foto ou vídeo, a placa de um veículo, um número de matrícula, ou até mesmo dados bancários.

A maioria desses dados é amplamente coletada em cadastros de clientes, formulários de contato, para a emissão de Notas Fiscais ou de *gift cards* e até mesmo em programas de fidelização do cliente e similares – e não há problema algum nisso. Mas é importante ter em mente que o tratamento de tais dados observe sempre a finalidade informada a seu titular e se dê de acordo com uma base legal.

5. EXISTEM CATEGORIAS DE DADOS PESSOAIS?

Sim. Além de dados pessoais (em sentido amplo), a Lei orienta que maiores cuidados devem ser tomados quando do tratamento de dados pessoais de crianças e adolescentes (art. 14), bem como de dados pessoais sensíveis (art. 11).

5.1. Dados pessoais de menores de idade

Nos termos do art. 14 da LGPD, o tratamento dos dados pessoais de crianças e adolescentes há de ser realizado "em seu melhor interesse", ou seja, visando sempre o atendimento de suas necessidades e a preservação de seus direitos.

Adolescentes são, no sistema jurídico brasileiro, aqueles com idade compreendida entre 12 e 18 anos incompletos; e crianças, aqueles com até doze anos de idade incompletos[1] – para estes, ainda prevê a lei que seus dados somente poderão ser tratados "com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal".

Não há vedação a seu tratamento; porém, é altamente recomendado que, havendo a possibilidade de tratar-se dados pessoais de menores de idade, o cuidado seja redobrado, em especial quanto ao consentimento do responsável (estritamente necessário no caso das crianças).

Além disso, é importante assegurar-se que o tratamento a ser realizado seja compatível não só com as finalidades informadas, mas com o "melhor interesse" do menor.

5.2. Dados pessoais sensíveis

Ainda, a LGPD define como dados pessoais sensíveis todo "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" (art. 5º, II).

Em que pese pareça uma definição bem simples, em especial dado o rol aparentemente objetivo da lei, o tratamento de tais dados acontece com mais frequência do que se imagina: ao perguntar-se em um cadastro sobre a religião praticada pela pessoa; quando do registro e/ou armazenamento de um atestado médico de um colaborador; ou com o processamento da biometria utilizada para legitimação de uma operação (como as bancárias ou mesmo de marcação de ponto).

Mesmo imagens de um circuito interno de monitoramento, se utilizadas para a extração de informações, como com o emprego de uma solução de reconhecimento facial (biometria), ou ainda se inseridas anotações sobre os titulares com base nas imagens captadas (como

[1] Definições trazidas da Lei nº 8.069 de 13 de julho de 1990 (Estatuto da Criança e do Adolescente, ou ECA).

por exemplo sobre a cor da pele ou sobre traços físicos ou de vestes que possam indicar um alinhamento religioso ou político), podem ser consideradas dados pessoais sensíveis.

Novamente, não há problema em tratar-se tais dados pessoais – mas é necessária atenção, pois possuem regras diferentes para que possam ser tratados e exigem uma proteção especial.

Além disso, conforme orientação do art. 38 da LGPD, havendo tratamento de dados pessoais sensíveis, recomenda-se elaborar um Relatório de Impacto à Proteção de Dados Pessoais (*Data Protection Impact Assessment*, ou DPIA), o qual deverá conter, 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 a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

6. DADOS ANONIMIZADOS SÃO DADOS PESSOAIS?

Nos termos do art. 12 da LGPD, "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Ou seja, dados anonimizados são aqueles que recebem tratamento específico para que se tornem incapazes de identificar (ou potencialmente identificar) um titular – e, nesses casos, deixam de ser dados pessoais, não se submetendo às diretrizes protetivas da lei.

Um tipo de operação de anonimização é facilmente exemplificável:

Dados Pessoais:

Nome	CPF	CEP	Idade
José da Silva	123.456.789-00	06454-000	45

ANONIMIZAÇÃO

Dados Anonimizados (com exclusão **permanente** dos dados apagados / substituídos):

Nome	CPF	CEP	Idade
J.	XXX.XXX.XXX-XX	06454	40 > 50

É importante não confundir anonimização (irreversível) com pseudonimização, esta conceituada no art. 13, §4º da LGPD como "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

Ou seja, dados pseudonimizados, por serem aptos a serem associados a seu titular, seja por reversão do processo, seja por associação a outras informações, seguem sendo dados pessoais sob a ótica da lei.

7. QUEM É RESPONSÁVEL PELO TRATAMENTO DOS DADOS PESSOAIS?

A LGPD chama de "agentes de tratamento" aqueles atuantes nas operações de tratamento de dados pessoais, dividindo-os em dois – o Controlador e o Operador.

O Controlador[2] é o responsável por tomar as decisões relativas ao tratamento de dados pessoais, como quando realizá-la, o porquê de fazê-lo, mantê-los ou excluí-los - ou seja, por determinar o destino dos dados pessoais em todo o seu ciclo de vida. É o caso de toda empresa que coleta dados de seus clientes, em um cadastro, por exemplo, ou mesmo para emissão de Nota Fiscal.

Já o Operador[3] é aquele que, contratado por um Controlador, atua no tratamento de dados pessoais em nome e por conta deste. É, normalmente, alguém sub-contratado para executar uma função, um papel ou uma atividade de tratamento de dados pessoais em razão de sua

[2] A LGPD define o Controlador como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
[3] A LGPD define o Operador como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

especificidade ou de sua *expertise*. O exemplo mais clássico de um Operador é uma empresa que presta serviços de *mailing* – ela não decide o que fazer com os dados pessoais, apenas executa as diretrizes impostas pelo Controlador. Escritórios de contabilidade ou de advocacia são, também, via de regra, Operadores, em suas relações com pessoas jurídicas.

Quanto à responsabilidade civil sobre as operações de tratamento de dados pessoais, ela será primordialmente do Controlador, exceto se o Operador descumprir as diretrizes do Controlador quanto ao tratamento de dados pessoais ou, de qualquer forma, violar as disposições da LGPD – ocasião em que incide a previsão do artigo 42 da LGPD (responsabilidade solidária).

É importante destacar que, como visto, os papéis de Controlador e Operador não são definidos pelas partes da operação, mas sim decorrentes de uma análise do seu papel considerando o fluxo de dados da operação de tratamento de dados pessoais – e é por isso que os papeis devem estar claros no ato da contratação, e as obrigações e responsabilidades de cada parte devem ser adequadamente indicadas no instrumento contratual.

Um franqueado, por exemplo, é Controlador dos dados pessoais de seus colaboradores, mas pode ser Operador dos dados pessoais de seus clientes (caso estejam operacionalmente sob controle do franqueador).

Além dos papeis de Controlador e Operador, pode acontecer também de as partes figurarem na condição de Controladores em Conjunto (Co-controladores) ou mesmo de Controladores Independentes.

Quando um franqueado compõe sua base de dados com dados pessoais de seus clientes e eventualmente os compartilha com o franqueador, ambos podem figurar como Controladores dos dados pessoais, cada qual respondendo pelo tratamento de dados pessoais que realiza em sua esfera de atuação (Controladores Independentes).

Neste mesmo cenário, o franqueador pode desenvolver ações específicas de engajamento para as quais atuará juntamente com o franqueado, os quais tomarão, juntos, as decisões operacionais relativas aos dados pessoais – ocasião em que serão Co-controladores (ou Controladores em Conjunto).

E até mesmo o franqueador pode vir a ser Operador de seu franqueado, como, por exemplo, quando dispõe de um CSC (Centro de Serviços Compartilhados) que é utilizado pelo franqueado para operacionalização de tarefas administrativas e de gestão empresarial. O

franqueador, não sendo destinatário dos dados pessoais dos colaboradores do franqueado, ao operar a folha de pagamento do franqueado, atuaria como seu Operador.

É por isso que o mapeamento dos fluxos de dados pessoais no ambiente empresarial é de suma importância à plena conformidade com a LGPD: a correta percepção do papel dos agentes nas operações de tratamento de dados pessoais.

8. É POSSÍVEL COMPARTILHAR DADOS PESSOAIS?

Sim, o compartilhamento de dados pessoais sob a guarda do Controlador é possível, desde que observados os deveres de informação e de transparência em relação ao titular dos dados pessoais.

Para que um compartilhamento de dados seja legítimo, é necessário que o titular seja previamente comunicado acerca da possibilidade de compartilhamento, bem como de sua finalidade – ou, se o caso, que outorgue consentimento claro, específico e destacado para tal fim, nos termos do §5º do art. 7º da LGPD.

Além disso, é necessário que se observe os requisitos de segurança da informação para a realização operacional do compartilhamento, de modo que as boas práticas e os controles relevantes para o tratamento dos dados pessoais estejam assegurados, em especial garantindo uma transmissão segura entre emissor e receptor.

9. AFINAL, COMO LEGITIMAR O TRATAMENTO DE DADOS PESSOAIS?

As bases legais são as condições que autorizam o tratamento de dados pessoais pela LGPD. Importante destacar que a forma de interpretar a regulamentação é analisar se naquele fluxo específico para aquela determinada finalidade é possível enquadrar o tratamento em uma das bases legais previstas na lei.

São bases legais autorizadoras do tratamento de dados pessoais as seguintes:

- Quando o titular expressamente autorizar (consentimento), hipótese em que deve-se manter registro de sua concessão;
- Para cumprimento de um contrato (ou sua elaboração) junto ao titular;
- Para utilização em processo judicial, administrativo ou arbitral;
- Para o cumprimento de obrigações legais ou regulatórias;
- Visando a proteção do crédito;
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Para a proteção da integridade física do titular ou de outra pessoa;
- Quando em atendimento de serviços de saúde; ou
- Quando necessário com base no legítimo interesse do controlador ou mesmo de um terceiro.

O "legítimo interesse", vale destacar, não é amplo e irrestrito, mas depende de uma avaliação prévia criteriosa quanto aos requisitos que permitem enquadrar determinado tratamento em suas hipóteses – o que se chama de *Legitimate Interest Assessment* (ou LIA).

Pode ser considerado legítimo interesse da empresa, por exemplo, o envio de e-mail publicitário (*mailing*) aos clientes cadastrados em sua loja, porém não o será o mesmo tipo de envio a uma base de dados cadastrais comprada de terceiros para fins de prospecção – e é para essa diferenciação que o LIA se mostra importante.

Outrossim, como já dito, nenhuma base legal, por si só, basta à legitimação do tratamento, já que deve estar alinhada com a finalidade pretendida (o que se pretende fazer com tais dados pessoais). Para se estar em conformidade com a LGPD, a finalidade do tratamento deve ser específica e informada, e a operação deve se dar em uma base legal autorizadora.

Coletar dados pessoais de clientes, por exemplo, pode ter a finalidade de permitir a emissão de uma Nota Fiscal (que teria como base o cumprimento de obrigação legal) ou mesmo de garantir a entrega do produto ou a prestação dos serviços contratados (cumprimento de contrato).

Abrir a carteira de um cliente que passa mal dentro de uma loja à procura de seu RG, por outro lado, teria como finalidade a identificação da pessoa, baseada na proteção de sua integridade física.

Cada situação é uma, mas deve-se sempre ter em mente que qualquer tratamento que não tenha uma finalidade clara e previamente informada (ou que se desvie dessa finalidade) **ou**

que não se enquadre em uma das bases legais autorizadoras é, em sua essência, um tratamento irregular.

10. E SE UM TRATAMENTO FOR IRREGULAR, QUAL O IMPACTO DISSO?

Não só para um tratamento irregular, mas também em decorrência de um incidente envolvendo dados pessoais (falaremos mais disso adiante), a LGPD traz severas consequências.

Na seara administrativa (ou seja, de competência da Autoridade Nacional de Proteção de Dados – ANPD), o infrator pode ser sujeitado às seguintes penalidades:

- Advertência e fixação de prazo para adoção das medidas corretivas;
- Multa, que pode chegar a 2% do faturamento da pessoa jurídica, grupo ou conglomerado em seu último exercício (ou seja, no ano anterior ao da constatação) – limitado a R$50 milhões;
- Multa diária até a regularização da situação, também limitada a R$50 milhões;
- Determinação de bloqueio ou eliminação dos dados pessoais envolvidos;
- Suspensão parcialda utilização do banco de dados envolvido por 6 (seis) meses, prorrogável por igual período;
- Proibição de exercer atividades de tratamento de dados pessoais.

Em decorrência das disposições da Lei nº 14.010/2020, as multas administrativas em decorrência do descumprimento da LGPD somente poderão ser aplicadas a partir de 1º de agosto de 2021 – mas isso não impede ações promovidas por entes representativos, como o Ministério Público, o PROCON, etc..

Além disso, pode ser determinado que a ocorrência seja tornada pública, gerando grande impacto negativo à imagem da empresa – e, no caso das franquias, mesmo um incidente isolado em um franqueado pode ter alto impacto reputacional à marca e à própria franquia como um todo.

Além disso, órgãos de representação social ou de classe (como sindicatos, no caso de colaboradores; Ministério Público ou órgãos / instituições de proteção ao consumidor, no caso de consumidores; etc.)

podem, ainda, tomar ações específicas com base no incidente ou na violação, pleiteando danos morais coletivos, a assinatura de Termo de Ajustamento de Conduta, entre outras penalidades.

Tudo isso sem prejuízo das ações que o próprio titular, sentindo-se lesado, pode adotar.

11. COMO MITIGAR RISCOS DE UMA NÃO-CONFORMIDADE?

Como falamos anteriormente, o tratamento de dados pessoais é não só uma realidade, mas uma necessidade no dia a dia das empresas – seja porque os dados pessoais são importantes para utilização interna, seja porque algumas obrigações dependem deles.

Invariavelmente, a melhor forma de prevenção é a cautela.

Um ótimo início é entender o quanto os dados pessoais são importantes, estão presentes na operação e nela impactam, de forma direta ou indireta.

É interessante submeter a empresa a um processo de mapeamento dos fluxos de dados pessoais, em especial para definição clara de finalidades e bases legais autorizadoras tanto das operações de tratamento como das de compartilhamento de tais dados pessoais.

Mas, além de mapeamento e implementação de ferramentas de segurança tecnológica, é imprescindível dar atenção ao maior fator de vulnerabilidade das empresas: o fator humano.

Conscientização, informação e treinamento são essenciais não só para disseminar a cultura da proteção de dados pessoais, mas em especial para buscar que todos façam a sua parte.

Tais orientações podem partir inclusive da própria franqueadora, já que incidentes relacionados a dados pessoais possuem um alto impacto reputacional – mas devem contar sempre com a colaboração dos franqueados.

Além disso, normativos internos (como políticas de gestão de dados pessoais e de mesa limpa, por exemplo) colaboram para redobrar a atenção dos colaboradores, sem prejuízo dos BCRs (*Binding Corporate Rules*) que podem ser estabelecidos entre franqueador e franqueados visando estipular regras mais específicas (e, talvez, operacionalmente detalhadas) para o tratamento de dados pessoais, as respostas a incidentes e afins.

Sob o aspecto operacional, é bom ter em mente que as operações de tratamento de dados devem observar os princípios da adequação (de que os dados tratados sejam adequados para a finalidade pretendida) e da minimização (que prevê que não sejam coletados dados além dos necessários para aquela finalidade). E é altamente recomendado evitar ao máximo o tratamento de dados pessoais sensíveis.

Por fim, sendo responsável o Controlador pelas operações de tratamento de dados pessoais realizadas por si ou por sua conta e em seu nome (por Operadores, no caso), é importante assegurar que tais terceiros que venham a ter acesso aos dados pessoais se comprometam a observar as diretrizes da lei e a cumpri-las, o que deve ser reforçado por cláusulas contratuais específicas que prevejam não só os direitos e deveres de cada das partes mas, em especial, suas responsabilidades.

12. UM INCIDENTE: E AGORA?

Um incidente relacionado a dados pessoais é a ocorrência de quaisquer "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

A figura mais clássica do incidente (e altamente em debate atualmente) é a do vazamento de dados pessoais sob controle da empresa, o que pode ocorrer por um descuido de um colaborador que perde uma pasta com documentos até por um ataque de um terceiro mal intencionado que invade os sistemas da empresa para obter tais dados.

Mas a perda de tais dados pessoais ou mesmo sua adulteração, acidental ou não, são considerados também incidentes – e podem ensejar aquelas penalidades sobre as quais já falamos.

Em caso de incidente, algumas premissas básicas devem ser observadas:

- É essencial agir rapidamente: a primeira hora é crucial!
- O Comitê de Proteção de Dados ou o Comitê de Resposta a Incidentes (quando e se constituídos) devem, imediatamente, ser acionados ou, quando não, ao menos as equipes de administração (DPO, T.I e Segurança da Informação).

- Deve-se evitar qualquer manipulação da base de dados e/ou do sistema afetado que possa trazer prejuízos à ocorrência e destruir algum rastro. Para tanto, T.I e Segurança da Informação devem apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente, bem como para a coleta de evidências de forma legal e/ou preservação dos recursos de tecnologia de modo a não perder as informações do incidente.
- Em caso de incidentes, deve-se evitar fazer qualquer comentário, participar de entrevistas e/ou emitir declarações ou comentários sobre o incidente sem prévia autorização do Comitê responsável e/ou do Departamento de Comunicações da Empresa. Os colaboradores de todos os níveis devem ser orientados que, caso questionados, deverão responder que "a situação está sendo devidamente apurada e a empresa prestará as informações assim que possível".
- Desde o marco zero, devem ser mantidos registros de cada etapa de análise do incidente e de medidas tomadas visando sua apuração, a mitigação dos danos e/ou sua correção, de modo a assegurar a possibilidade de eventual auditoria dos eventos.

É importante que as empresas contem com uma política interna para a gestão de incidentes dessa natureza, o que envolve o cumprimento do dever de *report* à Autoridade Nacional de Proteção de Dados (ANPD). Esse comunicado deve ser feito pelo Encarregado (*Data Protection Officer*, ou DPO – como nos referiremos aqui), função de constituição obrigatória por todas as empresas.

O dever de *report* é do Controlador. Logo, se for identificado o incidente pelo Operador, cabe a ele informar o Controlador, devendo então o Controlador notificar a ANPD – e, se houver alto risco de dano relevante aos titulares, eles também devem ser comunicados.

O *report* à ANPD deve ser realizado "em prazo razoável" (art. 48, §1º da LGPD), o que, por analogia às normativas mundiais de proteção de dados pessoais, entende-se por 72 (setenta e duas) horas após a ciência do incidente.

Por isso, e em especial na relação entre franqueador e franqueado, é importante definir os papéis e o SLA para situações relacionadas à resposta a incidentes. Como a marca é o valor agregado de maior relevância nas operações de franquia, a recomendação é que eventuais comunicações relacionadas a incidentes partam do franqueador, estabelecendo-se, por contrato (ou mesmo por um BCR), a obrigação de o franqueado não só reportar-se ao franqueador, mas também fornecer-lhe as informações pertinentes sobre o incidente de modo a permitir-lhe fornecer as diretrizes ao franqueado ou, se o caso, a adoção das medidas necessárias.

13. FALANDO EM DPO...

Um DPO é uma pessoa (física ou jurídica) nomeada pela empresa para ser a ponte de comunicação entre a empresa, os titulares e a ANPD.

Ele não trabalha sozinho – pode ter toda uma equipe interna ou mesmo uma empresa ou escritório externo dando-lhe suporte, ou pode ser ele próprio um escritório ou uma empresa.

Além de ser o interlocutor entre os envolvidos no tratamento de dados pessoais, o DPO é também o responsável por orientar a empresa e seus colaboradores, parceiros e afins quanto às disposições relativas à proteção de dados pessoais, cabendo-lhe inclusive fiscalizar (internamente) a observância das normas e políticas da empresa e da própria LGPD tanto pela empresa quanto por seus colaboradores, parceiros, prestadores de serviço e afins e, ainda, manter o Programa de Governança em Privacidade da empresa.

À função do DPO devem ser asseguradas independência operacional e imparcialidade, além de acesso à alta direção da empresa (a quem deve se reportar, além de a seu próprio superior se o caso).

Em se tratando de colaborador interno, não há qualquer óbice legal com outras atribuições, porém não é recomendável, pois além de sobrecarregar, deve-se garantir que não haja no acúmulo eventual conflito de interesses (em caso recente, a Autoridade de Proteção de Dados Belga reconheceu que haveria conflito de interesses no acúmulo de funções de DPO por um *Chief of Compliance*, mas outros cargos denotam aparente conflito de interesses, como os operacionais ou de gestão de T.I).

O DPO poderá, ainda, ser um prestador de serviços externo, como um escritório ou uma empresa, bem como poderá não ser exclusivo (um mesmo DPO pode estar vinculado a mais de uma empresa como prestador de serviços).

Ainda que no escopo de uma franquia, deve ser assegurado que cada pessoa jurídica distinta possua um DPO próprio, que exerça suas funções em observância às diretrizes acima mencionadas.

E ainda que seja aparentemente coerente centralizar as operações na franqueadora, pois em muitos casos grandes marcas de franquia prestam o serviço de gestão de atendimento de reclamações de clientes até por conta de proteger efeitos reputacionais da marca,

operacionalmente tal centralização pode se tornar inviável, já que mesmo em uma rede de franquias, cada unidade franqueada possui características operacionais singulares (seja seu público-alvo, sejam ações publicitárias próprias, etc.). Nossa recomendação é analisar o modelo de negócio de cada sistema de franquias.

14. QUAIS SÃO OS DIREITOS DOS TITULARES?

Os titulares de dados pessoais têm direitos e garantias especificadas pela LGPD, cabendo à empresa garantir que tais direitos sejam passíveis de serem acessados e exercidos desde o início do processo de tratamento de dados e ao longo de toda a vida do processamento, inclusive no término. São eles, conforme os artigos 6º, 18 e 20 da LGPD:

- **Confirmação da existência de tratamento:** o Controlador tem o dever de, ante solicitação do titular, confirmar se trata dados pessoais do solicitante;

- **Acesso aos dados:** o Controlador tem o dever de, ante solicitação do titular, informar quais dados pessoais do solicitante está a tratar;

- **Correção dos dados incompletos, inexatos ou desatualizados:** constatando o titular que seus dados pessoais estão não estão corretos, ante sua solicitação, o Controlador tem o dever de retificá-los;

- **Anonimização, bloqueio ou eliminação (apagamento) dos dados desnecessários, excessivos ou tratados em desconformidade:** caso o titular constate que dados pessoais seus estão sendo tratados em desacordo com a finalidade informada pelo Controlador, ele pode solicitar seu apagamento (exclusão não de todos, mas do dado considerado desnecessário) ou seu bloqueio (o dado considerado desnecessário à finalidade informada pode permanecer armazenado, mas não pode ser tratado);

- **Portabilidade a outro fornecedor mediante requisição expressa:** em que pese dependa ainda de regulamentação pela ANPD (conforme art. 40 da LGPD), é o direito do titular de solicitar que seus dados sejam transferidos a outro Controlador (e, por conseguinte, apagados da base do alvo da solicitação);

- **Eliminação dos dados tratados com o consentimento (pedido de apagamento):** caso dados pessoais estejam sendo tratados sob consentimento do titular, ele poderá solicitar sua exclusão;

- **Informação das entidades com os quais houve compartilhamento dos dados pessoais:** como visto, o Controlador pode compartilhar dados pessoais do titular, seja com seus Operadores, seja com outros Controladores, e caso solicitado pelo titular, deverá informá-lo sobre com quem compartilhou tais dados pessoais;

- **Informação sobre consequências de não fornecer o consentimento:** em casos em que dados pessoais serão tratados com base no consentimento, o titular deve ser previamente informado sobre a consequência, em sua relação com o Controlador, em caso de não fornecer tal consentimento;

- **Revogação de consentimento:** para casos em que dados pessoais do titular sejam tratados com base no consentimento, deve ser assegurado ao titular o direito de revogar tal consentimento, a qualquer tempo, pelo mesmo meio em que o outorgou;

- **Revisão de decisões automatizadas:** em casos em que algoritmos sejam utilizados para a tomada de decisões baseada em dados pessoais do titular (ex. perfilhamento), ele tem o direito de solicitar a revisão da decisão final.

É importante ter em mente que, ainda que legítimo o tratamento, caso não haja atendimento dos direitos dos titulares, a Instituição fica sujeita a sanções, em razão do princípio da responsabilização e prestação de contas.

Assim, as empresas deverão disponibilizar canal(is) de atendimento para que o titular exerça seus direitos, podendo as solicitações serem recepcionadas por diversos meios (chat, fale conosco, ouvidoria, chatbot), mas sempre direcionadas ao DPO para que este, por sua vez, tome as providências adequadas.

Em que pese a LGPD não determine um prazo para atendimento a todas as solicitações dos titulares, considerando o prazo assinalado de 15 dias para a confirmação da existência de tratamento de dados pessoais (art. 19, II), é razoável, por analogia simples, atribuir-se ao atendimento das demais o mesmo prazo, o qual tem início após o procedimento de autenticação do titular.

Em um cenário de franquias (em especial quando há compartilhamento de dados pessoais entre franqueador e franqueado), é possível determinar, de forma antecipada, seja por previsão contratual específica, seja por BCR, quais os procedimentos serão adotados pelas partes para atendimento às solicitações dos titulares, inclusive para que sejam replicadas nas bases um de outro.

15. O QUE SÃO DECISÕES AUTOMATIZADAS E COMO REVISÁ-LAS?

Como visto, um dos direitos do titular de dados pessoais é o de ter revisadas "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade" (art. 20 da LGPD).

Em um mundo com exponencialmente crescentes quantidades de interações de toda natureza, e com o aprimoramento da tecnologia e das técnicas de programação, muitas decisões passaram a ser tomadas com amparo (por vezes exclusivo) de algoritmos preditivos e interpretativos, desde a concessão de crédito pessoal até a seleção prévia de candidatos em um processo seletivo.

Até mesmo forças policiais investigativas e instituições regulatórias têm se utilizado de ferramentas de processamento de dados em massa e de análises automatizadas, como as identificações de operações potencialmente fraudulentas e/ou de indícios de ocultação de patrimônio.

Porém, não é só a revisão da decisão final que é assegurada ao titular, mas também o direito de receber "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial" (art. 20, §1º) – a chamada "transparência do algoritmo".

O objetivo da previsão legal é assegurar aos titulares a não-ocorrência de tratamento discriminatório, de sorte que ante eventual negativa de abertura dos dados em razão de segredo comercial e industrial, a ANPD pode realizar auditoria para verificação de sua não-ocorrência.

16. QUANTO À SEGURANÇA...

A LGPD impõe aos agentes de tratamento (Controladores e Operadores) o dever de "adotar medidas de 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 qualquer forma de tratamento inadequado ou ilícito" (art. 46).

Apesar disso, a lei não traz definições ou diretrizes mais objetivas sobre quais seriam tais medidas, ou como deveriam ser implementadas.

Sob tal prisma, protocolos e padrões internacionalmente reconhecidos – as chamadas *soft laws*, como a ISO 27.001 e as diretrizes do NIST (*National Institute of Standards and Technology*, dos Estados Unidos da América) – são excelentes fontes de referência dos padrões ideais de medidas técnicas e administrativas de segurança.

Algumas práticas gerais são recomendadas: ser proativo e não reativo, buscando evitar eventos invasivos de privacidade antes que ocorram; ser preventivo e não corretivo, monitorando riscos e entregando soluções que excluam os riscos identificados; conceber as operações já tendo em mente a privacidade dos titulares; garantir a proteção dos dados pessoais durante todo seu ciclo de vida (desde a coleta até seu expurgo); garantir, sempre visibilidade e transparência ao titular quanto ao tratamento de seus dados pessoais.

Ao lado de tais práticas, que devem ser incorporadas ao âmago da operação, outras podem ser orientadas por políticas e normativos internos e assumem vital importância sob a ótica da governança de dados, como:

- Manter processo de ciclo de vida para criação, manutenção, revisão, aprovação e comunicação de política, normas e procedimento às partes relevantes;
- Manter um sistema de gestão de segurança da informação;
- Definir responsabilidades de segurança de colaboradores e terceiros;
- Manter procedimento para classificação e gestão de ativos;
- Implementar diretrizes relativas a dispositivos móveis e periféricos, como de BYOD (*Bring Your Own Device*) e gestão de dispositivos de armazenamento removíveis;
- Estabelecer diretrizes para o uso de repositórios digitais e serviços de nuvem (*cloud computing / storage*);
- Implementar e manter procedimentos para continuidade do negócio;

Utilizar os dados pessoais somente para as finalidades previamente declaradas ao titular;

- Restringir o acesso aos dados pessoais aos profissionais que deles dependam para exercer suas atividades.

É importante que tanto franqueador quanto franqueado formalizem entre si, juntos aos parceiros, fornecedores e colaboradores que realizam o tratamento de dados pessoais, regras fundamentais para assegurar a privacidade e a segurança das partes envolvidas, dentre as quais destacam-se, principalmente:

- Utilizar sempre softwares devidamente licenciados e manter as atualizações em dia;
- Manter, em todos os terminais, ferramenta *anti-malware* ("anti-vírus") devidamente configurada e atualizada;
- Implementar um NGFW (*Next-Generation Firewall*);
- Garantir que os sistemas empregados no tratamento de dados pessoais possuam recursos que permitam o pleno atendimento aos direitos do titular;
- Garantir que os sistemas empregados no tratamento de dados pessoais possuam técnicas que permitam a anonimização de dados pessoais;
- Testar novas versões das aplicações em ambientes de homologação sem conexão com o banco de dados ativo ou o emprego de dados pessoais de qualquer natureza;
- Implementar modelo de gestão de acessos, bem como criar controles de acesso individualizados, preferencialmente com credencial única sob duplo fator de autenticação para todas as funcionalidades empregadas;
- Incluir os sistemas que tratam dados pessoais nos procedimentos de gestão de mudanças da T.I;
- Estabelecer requisitos e rotinas de avaliação de segurança para aquisição e desenvolvimento de sistemas;
- Implementar processos periódicos de avaliação de vulnerabilidade nas aplicações ativas;
- Garantir a segurança física do datacenter, com controle de acesso, sistema de prevenção e combate a incêndios, videomonitoramento, monitoramento de ambiente (temperatura e umidade relativa do ar), bloqueio de portas físicas de conexão e de remoção de dispositivos, entre outras, bem como sua segurança lógica, com controle de acesso restrito a pessoal previamente autorizado e autenticado mediante duplo fator;
- Garantir a criptografia dos dados pessoais tanto no armazenamento (DES, 3DES, RC4, DESX, AES, etc.) quanto na transmissão (SSL, TLS);
- Implementar trilhas auditáveis de acesso que registrem o endereço IP e a porta lógica de conexão, bem como o *timestamp* (dia, mês, ano, hora, minuto, segundo e fuso-horário) da operação;

- Implementar trilhas auditáveis de transação que registrem o endereço IP e a porta lógica de conexão, bem como o *timestamp* (dia, mês, ano, hora, minuto, segundo e fuso-horário) da operação realizada, bem como as ações / alterações performadas;
- Garantir que os sistemas que tratam dados pessoais sejam submetidos a procedimentos de backup que observem a natureza e a criticidade dos dados tratados, bem como a volumetria da base, preferencialmente por duas ou mais modalidades distintas, garantindo-se a segurança dos backups (se em fita, por armazenamento a mais de 50km do datacenter; se por RAID, com designação de controle de acesso ao disco secundário; se em nuvem ou em disco, encriptando o backup;
- Garantir que os sistemas que tratam dados pessoais estejam inseridos no plano de continuidade do negócio;
- Implementar soluções específicas de DLP;
- Assegurar o descarte adequado dos dados pessoais, sempre nas dependências da empresa – se em meios lógicos, com procedimento de sanitização dos dados (*wipeout*); se em meios físicos, por fragmentação (trituração) e descarte segmentado;

17. E QUANDO OS DADOS PESSOAIS ESTÃO COM TERCEIROS CONTRATADOS?

Se manter os requisitos de governança e segurança acima apontados é tarefa difícil, assegurar-se que terceiros contratados os mantenham pode ser ainda mais.

Por isso, é importante que as empresas desenvolvam um procedimento específico para a execução de auditorias de controles de segurança da informação no tratamento de dados pessoais por terceiros, as quais devem ser realizadas antes mesmo da contratação (e, se consumada, durante a vigência da relação) para assegurar a conformidade do terceiro com a LGPD e os padrões adequados de segurança dos dados pessoais.

Em tal procedimento, devem ser analisados eventuais normativos internos, bem como os indicadores de conformidade operacional do terceiro para com a Lei. Além disso, devem ser analisados eventuais Relatórios de Impacto à Proteção dos Dados pessoais (RIPD ou, em sua sigla em inglês, DPIA) emitidos pelo terceiro, além da coleta de informações para preenchimento de um questionário de prontidão de segurança da informação e governança de dados.

Os riscos relevantes quanto aos dados pessoais e os controles mitigatórios empregados são, assim, percebidos e, por conseguinte, avaliados para fins de viabilização ou não da contratação – ou, no caso de uma relação vigente, de sua manutenção.

As condições mínimas de satisfação tanto dos níveis de conformidade quanto dos níveis de segurança dos dados pessoais devem ser previstas em contrato como dever do terceiro contratado, de forma que eventual violação (não-conformidade) permita não só a rescisão contratual, mas também a punição do infrator.

18. QUANDO PODE OCORRER A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS?

A LGPD traz em seu art. 33 condições específicas para que a transferência internacional de dados possa ocorrer, as quais visam garantir aos titulares a proteção adequada a seus dados pessoais e o respeito à sua privacidade.

É considerada transferência internacional não só o compartilhamento com empresa do grupo que esteja situada fora do país (ex. franqueador estabelecido nos EUA, franqueado no Brasil), mas mesmo o uso de tecnologia de armazenamento e processamento em nuvem executada em servidores fora do território nacional – seja um software (como um CRM ou um ERP em nuvem), seja um serviço de infraestrutura (como uma Azure ou uma AWS).

Tais transferências apenas podem ocorrer se:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei, sendo que o reconhecimento como tal depende de ato deliberativo da ANPD (art. 34 da LGPD);

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência, que prevejam a proteção e o atendimento aos direitos dos titulares tais quais previstos na LGPD, além das sanções em decorrência de seu descumprimento, que dependem de validação pela ANPD (art. 35 da LGPD);

b) cláusulas-padrão contratuais (*Standard Contractual Clauses*, ou SCC), documento a ser editado pela ANPD visando padronizar os aspectos mínimos a serem observados pelo agente

de tratamento ao qual remetidos internacionalmente os dados, que devem ser futuramente definidas pela ANPD (art. 35 da LGPD);

c) normas corporativas globais – os já citados BCRs –, quando internamente ao grupo econômico, e que prevejam os direitos e obrigações comentados neste Manual, que dependem de validação pela ANPD (art. 35 da LGPD);

d) selos, certificados e códigos de conduta regularmente emitidos, também a serem regulamentados e homologados pela ANPD (art. 35 da LGPD);

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, ato privativo do Poder Público;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, via de regra em cenários médico-hospitalares;

V - quando a autoridade nacional autorizar a transferência, ato de "consulta prévia" ainda a ser regulado pela ANPD, que avaliará não só os aspectos operacionais mas também os níveis de proteção oferecidos pelo país de destino;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional, ato privativo do Poder Público;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei, ato privativo do Poder Público;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades, para o que importante observar os requisitos de (1) consentimento específico, (2) em destaque e (3) com informação clara sobre a operacionalização internacional; e

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei, especificamente o cumprimento de obrigações regulatórias pelo controlador, quando da execução de contrato ou de exercício de direito em processo judicial, administrativo ou arbitral.

Como visto, muitos dos atos dependem de regulamentação prévia, homologação ou deliberação da ANPD; e, em um cenário atual em que a Autoridade ainda não se encontra em pleno funcionamento, o estabelecimento de operações baseadas em ato da Autoridade podem representar riscos operacionais ao Controlador em virtude de uma possível vedação futura.

19. ENFIM: QUAL O EFETIVO IMPACTO DA LGPD NAS OPERAÇÕES DOS ASSOCIADOS DA ABF?

Isso vai depender muito da natureza da operação sob análise, mas em um plano mais generalista, é possível dizer que todo e qualquer associado da ABF é impactado: no mínimo, por tratar dados pessoais de seus próprios colaboradores; mas também por manter registro dos dados pessoais de seus franqueados, ou ainda por tratar, em um plano geral, os dados pessoais dos clientes finais da rede.

Assim, reiterando, é altamente recomendado que as empresas busquem realizar o mapeamento de seus fluxos de dados pessoais, bem como reavaliem os sistemas que utilizam e, se o caso, aprimorem as medidas de segurança técnica empregadas.

Em especial em um cenário de franquias, além do mapeamento dos fluxos de dados pessoais tanto no franqueador quanto no franqueado, eventualmente referidos fluxos vão coincidir (ex. quando a franquia toda compartilha de um único CRM).

A implementação de medidas técnicas e administrativas adequadas para garantir a segurança dos dados pessoais é imprescindível, sendo crítico elemento de controle e avaliação do grau de comprometimento com a proteção de dados pessoais.

O investimento em capacitação e treinamento dos colaboradores para que passem a atuar em acordo com a lei também é de suma importância, e pode ser reforçada com a adoção de políticas e normativas internas sobre o tema.

Por fim, a empresa tem de estar apta a atender, quando necessário (e pertinente), os direitos do titular – e, para tanto, deve constituir um DPO.

No fim do dia, adequação não é só um simples indicador de conformidade legal, mas um item de ética e respeito para com os titulares, sejam clientes, sejam colaboradores, além de

reforçar a integridade operacional e jurídica da empresa – um diferencial relevante no mercado.

20. COMO ASSEGURAR A CONFORMIDADE COM A LGPD?

A realidade operacional de cada empresa, ainda que inserida em uma rede de franquias, torna cada plano de adequação único, exigindo que seja conduzido por profissionais capacitados e, em especial, aptos a compreenderem a fundo as particularidades de cada entidade.

Todavia, alguns elementos podem ser considerados essenciais a um projeto de adequação à LGPD:

- Mapeamento dos fluxos de dados pessoais na empresa;
- Identificação das finalidades específicas de cada operação de tratamento;
- Identificação das bases legais autorizadoras do tratamento de dados pessoais;
- Revisão da base legada e validação da legitimação do tratamento de dados pessoais ou expurgo dos dados legados;
- Avaliação dos sistemas empregados pela empresa para análise da operacionalização do atendimento dos direitos dos titulares e dos requisitos de segurança da informação;
- Revisão das plataformas tecnológicas da empresa e adequação dos documentos pertinentes (Termos de Uso e Política de Cookies);
- Constituição de uma Política de Privacidade;
- Proceder com ajustes na cultura interna da empresa, em especial visando a incorporação das diretrizes da Lei Geral de Proteção de Dados, através da constituição de políticas e normativos internos regulando o tratamento de dados pessoais;
- Implementação de procedimentos para atendimentos às requisições dos titulares;
- Implementação de procedimentos de Avaliação de Legítimo Interesse (*Legitimate Interest Assessment*, ou LIA);
- Emissão de Relatório de Impacto à Proteção dos Dados Pessoais (*Data Protection Impact Assessment*, ou DPIA);
- Revisão dos contratos com fornecedores, parceiros e clientes para inclusão de previsões específicas sobre a proteção de dados pessoais;
- Constituição de um Encarregado pela proteção de dados pessoais (DPO);

- Treinamento e capacitação de colaboradores para conscientização sobre as diretrizes da LGPD e de segurança da informação.

Não se busca, aqui, o esgotamento das medidas necessárias à adequação e à conformidade com a Lei Geral de Proteção de Dados, mas sim os aspectos mais essenciais de sua implementação. Como dito anteriormente, a realidade operacional de cada empresa é item essencial de análise para melhor compreensão das necessidades.

Ademais, não basta uma adequação estrita do ponto de vista jurídico, ou do ponto de vista técnico: é necessária a implementação de medidas tanto técnicas quanto organizacionais para fins de conformidade.

É importante sempre lembrar que não há “fórmula mágica”que leve à adequação perante a Lei – uma avaliação profunda da operação, customizada, que pondere tanto os aspectos técnicos quanto os organizacionais, certamente refletirá em um robusto plano de ações que certamente mitigará de forma eficaz os principais riscos de não-conformidade.