fundação podemos
político para todos

Conformidade e Governança *no setor público*

Parte 3

Conformidade na Lei Geral de Proteção de Dados Pessoais

Março 2024 | São Paulo - SP

Parte I: Conceitos da LGPD

1. Objeto e os Fundamentos da LGPD

O objetivo da Lei Geral de Proteção de Dados (LGPD) é disciplinar o tratamento de dados pessoais.

A LGPD se aplica ao tratamento de dados quer ele ocorra em meios digitais ou em meios físicos. Se aplica também seja o tratamento realizado por pessoa física ou jurídica, de direito privado ou público.

O objetivo da Lei é a proteção dos direitos fundamentais, da liberdade e da privacidade dos titulares de dados pessoais. Também se protege o livre desenvolvimento dos indivíduos, incluindo crianças e adolescentes.

São fundamentos da LGPD:

1. A privacidade;
2. A autodeterminação informativa;
3. A liberdade tanto de expressão, de informação, de comunicação e de opinião quanto a livre iniciativa e a livre concorrência;
4. A defesa do consumidor;
5. A inviolabilidade da intimidade, da honra e da imagem;
6. O desenvolvimento econômico e tecnológico;
7. O estímulo à inovação;
8. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania.

1.1. O que são dados pessoais?

De acordo com a LGPD o **dado pessoal** é toda informação que identifique ou possa identificar - por meio da combinação de vários dados - um indivíduo. Portanto, nome, sobrenome, e-mail, telefone, data de nascimento, CPF, RG, interesses, hábito de consumo, são todos exemplos de dados pessoais.

O CPF de um indivíduo é informação que permite que a pessoa natural (titular dos dados pessoais) seja identificada. Isso significa que, por meio do tratamento dos dados pessoais, poderão ser extraídos elementos distintivos que permitam identificar quem é o titular. A mera possibilidade de identificação é suficiente para tornar o dado um "dado pessoal", não havendo necessidade de que o dado aponte expressamente a identidade da pessoa.

Já o **dado sensível** significa o dado pessoal dotado de maior "sensibilidade", já que o seu titular pode vir a ser alvo de discriminação. Os dados sensíveis são sujeitos, portanto, a um regime legal mais rigoroso. São dados sensíveis aqueles que implicam ameaça a direitos fundamentais dos indivíduos, os quais incluem dados relacionados à raça, opinião política, religião, vida sexual, saúde, informação genética e biometria. Os dados pessoais sensíveis são classificados a partir de critérios objetivos.

Vale falar também no conceito de **dados anonimizados**: são dados "embaralhados" e que não permitem a identificação da pessoa natural a que se referem.

A identificação, nesse caso, é impossível do ponto de vista dos meios tecnológicos razoáveis (relação custo-benefício da reidentificação) e que estejam disponíveis no tempo em que o tratamento é realizado.

Importante notar que, por não permitirem a identificação de seu titular, os dados anonimizados **não são considerados dados pessoais** e, portanto, não estão sujeitos às normas da LGPD, ressalvadas as hipóteses nas quais é possível a reversão da anonimização, considerando-se a tecnologia existente no momento e a razoabilidade (custo-benefício, proporcionalidade etc.) do procedimento de reversão da anonimização.

1.2. Princípios norteadores da LGPD

A LGPD é norteada por alguns princípios que dão sustentação às suas normas e norteiam a sua interpretação.

Os princípios norteadores da LGPD são os seguintes:

Finalidade

Só pode haver coleta de dados pessoais para uma finalidade determinada, explícita e legítima. Não é possível que os dados pessoais sejam tratados para fins diversos da finalidade originalmente prevista.

O tratamento dos dados deverá ser motivado e vinculado a uma finalidade específica e legítima, que deve ser explícita e informada ao titular dos dados pessoais.

Adequação

Adequação é a correspondência entre os meios empregados no tratamento e as finalidades perseguidas. Devem ser consideradas apenas as finalidades informadas explicitamente ao titular dos dados pessoais.

Necessidade (Minimização)

Necessidade é o princípio de que o tratamento deve se restringir ao mínimo, ao indispensável para a realização da finalidade perseguida e explicitamente informada ao titular. Com base nesse princípio, a coleta deve ser limitada aos dados estritamente necessários e nunca excessiva.

Livre Acesso

O princípio do livre acesso é mais um dos princípios que servem de garantia para o titular de dados pessoais. Isto porque resguarda-se o direito do titular a uma "consulta facilitada e gratuita". O titular deve ser capaz de acessar, fácil e gratuitamente, a totalidade dos dados que lhe digam respeito.

Qualidade

A qualidade dos dados envolve a exatidão, a clareza, a relevância e a atualização dos dados, na medida da necessidade para o cumprimento de suas finalidades.

Transparência

A transparência é muito semelhante ao princípio do livre acesso, garantindo, ainda, a facilidade de acesso a informações sobre o tratamento de dados e os respectivos agentes de tratamento. A limitação a esse acesso somente pode ocorrer em casos de segredos comercial e industrial.

Segurança

Os dados pessoais devem ser tratados com a segurança adequada, suficiente e apropriada. Isso significa que os agentes de tratamento precisam adotar medidas técnicas e administrativas para proteção dos dados de acessos não autorizados, bem como de situações acidentais e ilícitas de perda, destruição ou difusão dos dados.

As medidas de segurança da informação devem se referir tanto aos suportes digitais quanto aos suportes físicos, assim como devem acompanhar o estágio atual da tecnologia, dentro dos limites da razoabilidade, o que gera um dever constante de atualização para os agentes de tratamento.

Prevenção

O princípio da prevenção orienta que devem ser adotados mecanismos que sejam capazes de, ex ante, impedir que o tratamento de dados pessoais resulte em dano. Muitas medidas de prevenção são exatamente as que integram também a satisfação do princípio da segurança.

Não-discriminação

O princípio de não-discriminação é um princípio essencialmente negativo. São proibidos os tratamentos que persigam finalidades discriminatórias, ilícitas ou abusivas. A discriminação abrange o tratamento desigual segundo determinado critério para uma finalidade proibida. Quando, porém, a finalidade é a de garantir a isonomia entre os indivíduos ou outras finalidades lícitas e legítimas, determinados critérios que, em outras situações seriam discriminatórios, podem ser autorizados. Por esse motivo não há discriminação na diferenciação entre homens e mulheres para a concessão de licença-maternidade ou no processo seletivo para os responsáveis pela realização de revistas íntimas. Como já decidido pelo STF, também não há discriminação na adoção de quotas socioeconômicas, raciais ou outras.

Responsabilização e prestação de contas *(Accountability)*

O controlador dos dados pessoais deverá agir de forma responsável. Deverá também ser capaz de provar que

age em conformidade com os princípios enumerados até agora. Nesse sentido, é importante que seja elaborado um programa de compliance específico para o tema da proteção de dados e a segurança da informação, no que se refere à privacidade e proteção de dados e segurança da informação.

1.3. Das Bases Legais

A LGPD estabelece requisitos para o tratamento de dados pessoais. São 10 as hipóteses de tratamento de dados pessoais (comumente chamadas "bases legais"), não sendo admitidas bases legais distintas das previstas em lei.

O conjunto de bases legais para o tratamento de dados pessoais e dados pessoais sensíveis divergem em alguns aspectos.

1.3.1. Das bases legais relativas a dados pessoais

O tratamento de dados pessoais pode ser baseado em uma das seguintes bases legais:

1. **Consentimento:** o consentimento do titular de dados pessoais. O consentimento deve ser livre (não pode haver coação), expresso, específico e informado (a pessoa deve ser informada a respeito do consentimento e de suas consequências). Deverá se dar **por escrito** ou por outro meio capaz de demonstrar a manifestação de vontade do titular. O consentimento deverá se referir à **finalidade específica** do tratamento de dados pessoais, de forma que as autorizações genéricas para o tratamento de dados são nulas. Por fim, o consentimento poderá ser revogado a qualquer momento.

2. **Cumprimento de obrigação legal ou regulatória:** o controlador pode tratar dados pessoais com o objetivo de cumprir obrigações impostas por força de lei ou por força de regras estabelecidas pela autoridade regulatória.

3. **Políticas públicas:** a administração pública poderá tratar e fazer o uso compartilhado de dados pessoais para a realização de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos ou convênios.

4. **Realização de Estudos:** órgãos de pesquisa poderão tratar dados para a realização de estudos. Os dados devem ser, sempre que possível, anonimizados.

5. **Execução de contrato:** poderá haver tratamento de dados quando o tratamento for necessário para a execução das obrigações contratuais. A base legal não se refere apenas aos contratos,

mas também aos procedimentos preliminares, antes da celebração definitiva do contrato.

6. Exercício Regular de Direitos: pode haver tratamento de dados para que direitos sejam exercidos regularmente para o processo judicial, administrativo ou arbitral.

7. Proteção da vida ou da incolumidade física: pode haver, ainda, tratamento de dados para proteção da vida ou da incolumidade física do titular.

8. Tutela da Saúde: poderá haver tratamento de dados para a tutela da saúde do titular de dados pessoais. Essa hipótese, porém, se limita a procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

9. Legítimo interesse: poderá haver tratamento de dados pessoais para entender um interesse legítimo do controlador ou de terceiros. Trata-se de uma base legal ampla, que deverá ser restringida em face de direitos e liberdades fundamentais que digam respeito à proteção de dados pessoais. Por esse sentido, **o legítimo interesse não pode ser utilizado para justificar o tratamento de dados sensíveis.**

10. Proteção de Crédito: a proteção do crédito é outra hipótese que se presta a fundamentar o tratamento de dados pessoais. **Trata-se de uma das bases legais que não serve para justificar o tratamento de dados pessoais.**

1.3.2. Das bases legais relativas a dados pessoais sensíveis

Os dados pessoais sensíveis, por sua vez, são cobertos por um menor número de bases legais, sendo elas:

1. Consentimento: o consentimento do titular de dados pessoais sensíveis deverá ser dado de forma específica, destacada e vinculada a uma finalidade específica.

2. Cumprimento de obrigação legal ou regulatória: o controlador pode tratar dados pessoais com o objetivo de cumprir obrigações impostas por força de lei ou por força de regras estabelecidas pela autoridade regulatória.

3. Políticas públicas: a administração pública poderá tratar dados pessoais para a realização de políticas públicas. A administração poderá se valer do uso compartilhado de dados. As políticas devem estar previstas em leis ou regulamentos.

4. Realização de Estudos: órgãos de pesquisa poderão tratar dados para a realização de estudos. Os dados devem ser, sempre que possível, anonimizados.

5. Exercício Regular de Direitos: pode haver tratamento de dados para que direitos sejam exercidos regularmente em contratos e para fins de processo judicial, administrativo ou arbitral.

6. Proteção da vida ou da incolumidade física: pode haver, ainda, tratamento de dados para proteção da vida ou da incolumidade física do titular.

7. Tutela da Saúde: poderá haver tratamento de dados para a tutela da saúde do titular de dados pessoais. Essa hipótese, porém, se limita a procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

8. Prevenção à fraude e à segurança do titular: poderá ocorrer o tratamento de dados pessoais sensíveis nos processos de identificação de autenticação de cadastro em sistemas eletrônicos, com o intuito de prevenir fraudes e garantir a segurança ao titular. A base legal não é aplicável quando entrar em conflito com direitos ou liberdades fundamentais do titular de dados pessoais.

Há um tratamento diferenciado para os dados de crianças e adolescentes. As noções de criança e adolescente são as presentes no Estatuto da Criança e do Adolescente (ECA):

Criança: pessoa que tenha até doze anos incompletos.

Adolescente: pessoa que tenha entre 12 anos completos e 18 anos incompletos.

Há particularidades para o consentimento de crianças e adolescentes. Devem ser observadas as particularidades da condição da criança ou adolescente, especialmente quanto à finalidade perseguida.

Há também deveres para o controlador que tratam dados de menores. Há um dever especial de simplicidade, clareza e acessibilidade. Deve ser levada em consideração a capacidade mental típica da idade.

Há ainda algumas regras específicas sobre o tratamento de dados de crianças e adolescentes. São elas:

Consentimento: o tratamento de dados pessoais de crianças exige o consentimento específico e em destaque de um dos pais ou do responsável legal. Pode haver a coleta sem o consentimento quando a coleta de dados for necessária para contatar os pais ou o responsável legal, caso em que esses dados não poderão ser armazenados ou utilizados

mais do que uma única vez. Também pode haver coleta de dados para a proteção da criança ou do adolescente. Em ambos os casos os dados não poderão ser repassados sem o consentimento. O **controlador** deve fazer todos os esforços razoáveis, considerando-se as tecnologias disponíveis, para verificar que o consentimento foi dado efetivamente pelos pais ou pelo responsável legal.

Transparência e exercício de direitos: deve haver publicidade ainda mais ampla a respeito dos tipos de dados de crianças e adolescentes que são coletados, assim como a forma de utilização desses dados e os procedimentos para que sejam exercidos os direitos previstos.

Deveres dos controladores: o controlador de dados pessoais de crianças ou adolescentes deverá ser ainda mais cauteloso e não condicionar o fornecimento de dados pessoais em contrapartida ao acesso a aplicações na Internet ou outros serviços, ressalvados os dados que são estritamente necessários para o fornecimento desse serviço ou aplicação.

Clareza e Simplicidade: a criança ou adolescente que for titular de dados pessoais deverá ser informada sobre o tratamento. As informações devem ser fornecidas levando-se em consideração as particularidades de compreensão de crianças ou adolescentes, isto é, de forma simples, clara e acessível. Elas devem ser informadas também de forma clara sempre que aplicações e serviços não sejam destinados à sua faixa etária e/ou que o acesso a estes exigir o prévio consentimento de um responsável legal.

Funções relevantes para a LGPD

Controlador: é a pessoa natural ou jurídica, de direito público ou privado, que efetivamente toma as decisões referentes ao tratamento de dados.

Operador: O operador é a pessoa natural ou jurídica, de direito público ou privado, que é responsável pela realização do tratamento dos dados pessoais. Se o controlador é quem **decide,** operador é quem **realiza** o tratamento dos dados, tratamento esse que ocorre em nome do controlador.

Encarregado: o Encarregado é designado pelo controlador e sua responsabilidade é servir como intermediário no diálogo entre o controlador, os titulares dos dados pessoais tratados e a agência regulatória, a Agência Nacional de Proteção de Dados

("ANPD").

Titular de dados pessoais: pessoa natural a quem se referem os dados. É o elo fraco, cujos direitos à identidade, intimidade e privacidade estão vulneráveis a violações e cujos direitos se protegem.

Tratamento: tratamento é a designação dada para qualquer operação realizada que envolva dados pessoais.

Banco de dados: trata-se de um conjunto de dados reunidos, desde que esses dados sejam estruturados e fixados em um ou em vários locais. O banco de dados poderá contar com um suporte, que tanto pode ser eletrônico como pode ser físico

Bloqueio: o bloqueio consiste numa indisponibilidade temporária do acesso aos dados pessoais. Há interrupção das atividades do tratamento de dados. O efeito não é terminativo, mas suspensivo.

Responsabilização

O controlador ou o operador que causarem dano decorrente de atividade irregular de tratamento respondem pelos danos causados em violação à LGPD, nos termos do art. 42, ficando obrigados a indenizar os titulares.

A responsabilidade dos referidos agentes de tratamento é **solidária** quando, de um lado, o operador descumprir obrigações previstas na LGPD ou deixar de atender instruções lícitas do controlador ou, por outro lado, o controlador estiver diretamente envolvido no tratamento do qual se originou o dano.

Além de ações individuais, são cabíveis ações de reparação por danos coletivos contra os agentes de tratamento.

Exclusão da Responsabilização

A lei prevê três hipóteses nas quais a responsabilidade do controlador ou do operador será afastada. As hipóteses são:

1. Quando provarem que não realizaram os tratamentos de dados pessoais em questão;
2. Quando provarem que, embora tenham realizados o tratamento, não houve violação à legislação de proteção de dados pessoais;
3. Quando provarem que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Parte II: A LGPD na prática

1. Adequação à LGPD

Diversos são os deveres atribuídos ao controlador e ao operador de dados e os direitos dos titulares reconhecidos e protegidos pela LGPD.

Os agentes de tratamento devem, assim, buscar a adequação de seus projetos, produtos, serviços e atividades à LGPD, de forma efetiva.

Uma medida para conferir efetividade à LGPD é o engajamento do agente de tratamento em um projeto de adequação à lei rumo a estabelecer um programa de governança em proteção de dados pessoais e segurança da informação e sua melhoria contínua.

O passo a passo em um projeto de adequação à LGPD pode ser descrito da seguinte forma:

1. O engajamento e a demonstração de que a alta administração da instituição assume compromissos com o tema da proteção de dados e a segurança da informação;

2. Mapeamento das atividades e todo o fluxo de dados (data flow), isto é, o trajeto que os dados pessoais percorrem em cada processo dos diversos departamentos;

3. O apontamento de gaps e as recomendações de adequação macro e fluxo a fluxo;

4. A criação de um plano de ação apontando as prioridades, os responsáveis e o cronograma;

5. Designação de um profissional, o Encarregado, que seja responsável pelo recebimento de reclamações dos titulares; notificações da ANPD e outras autoridades competentes, por recomendar ações de adequação e mitigação de riscos para a instituição; por ações de conscientização e pelo treinamento de funcionários e fornecedores;

6. Elaboração de políticas, avisos, termos e demais instrumentos de transparência ao titular;

7. Implementação das medidas de boa governança.

2. Contratos

Também deverá ocorrer a revisão dos contratos empresariais, que devem ser readequados de forma a atender os requisitos fixados pela lei.

A instituição deverá, nesse sentido, realizar um levantamento que aponte os contratos nos quais há compartilhamento de dados pessoais com parceiros, fornecedores e prestadores de serviços e firmar, junto a estes, aditivos contratuais contendo cláusulas referentes aos direitos e obrigações das partes no contexto do tratamento dos dados pessoais, à luz da LGPD. Deverá ser conferida atenção especial para os contratos que envolverem o tratamento de dados sensíveis ou dados de menores de idade, exigindo-se das partes um nível de proteção ainda mais robusto.

Portanto, quando houver tratamento de dados, os contratos deverão prever:

Conformidade com a LGPD: o contrato deverá prever que as

partes observarão a LGPD, assim como cumprirão normas internas de privacidade e proteção de dados.

Operador: nos contratos entre controlador e operador, deverá ser previsto que o operador tratará os dados em nome e conforme as instruções do controlador.

Exclusão dos dados: o contrato deverá prever que, após o final do tratamento dos dados, deverá haver a devolução e exclusão dos dados pessoais da base de dados do operador.

Padrões de segurança: o operador ou ambos os agentes de tratamento deverão adotar determinados padrões de segurança, que normalmente deverão constar em termos anexos.

Cooperação: poderá, ainda, haver cláusulas que prevejam que os diferentes agentes envolvidos no tratamento de dados irão cooperar, por exemplo, na forma de auxílio mútuo no caso, quando houver ameaças ou incidentes com dados pessoais, requisições pela ANPD ou outras autoridades competentes e requisições de titulares.

3. Instrumentos de Transparência

As políticas, avisos, termos e demais instrumentos de transparência devem informar, de forma clara ao titular de dados pessoais:

Dados coletados ou tratados: o titular deverá ser informado a respeito dos dados coletados ou tratados.

Finalidade específica do tratamento: o titular deve ser informado, de forma explícita e específica a respeito das finalidades do tratamento de seus dados.

Forma e duração do tratamento: o titular deve ser informado sobre o tempo que os dados pessoais ficam armazenados (período de retenção) e a forma de armazenamento desses dados pessoais.

Identificação do controlador: o titular de dados pessoais deverá ser informado sobre quem efetivamente toma as decisões referentes a seus dados pessoais.

Informações sobre uso compartilhado: o titular deve ser informado se seus dados pessoais são compartilhados e, se sim, qual é a finalidade perseguida pelo compartilhamento de dados.

Direitos do Titular e identidade do Encarregado: o titular de dados pessoais deve ser informado sobre quais são seus direitos, quais os meios para exercê-los. Também deverá ser informado sobre o canal de contato do encarregado e quem é o encarregado.

4. Relatório de Impacto à Proteção de Dados

Trata-se de relatório que poderá ser solicitado pela ANPD. Ele deverá conter a descrição de que tipos de dados são coletados, a metodologia empregada na coleta, a metodologia empregada para a segurança das informações e uma análise feita pelo controlador a respeito das medidas e mecanismos internos de mitigação de risco.

5. Término do Tratamento

O tratamento dos dados pessoais deverá chegar ao seu fim quando:

1. A finalidade perseguida pelo tratamento tiver sido atingida;
2. O tratamento tiver sido planejado para um período determinado e esse período chegar ao seu fim;
3. A pedido do titular dos dados pessoais (por exemplo, quando o titular revoga o consentimento);
4. Por determinação de autoridade.

6. Eliminação dos dados pessoais

Após o término do tratamento dos dados pessoais, deverá ocorrer a eliminação dos dados pessoais que até então estiverem retidos sob poder do controlador ou do operador. Poderá haver a retenção dos dados pessoais após o término do tratamento nas seguintes hipóteses:

1. Cumprimento de obrigação legal ou regulatória;
2. Estudo por órgãos de pesquisa (nestes casos, deverá ocorrer a anonimização dos dados sempre que possível);
3. Quando houver transferência para terceiro;
4. Uso exclusivo do controlador de dados anonimizados, sendo proibido o acesso a esses dados por terceiros.

A eliminação produz efeitos definitivos. Os efeitos da eliminação são terminativos. Há suspensão definitiva do tratamento.

7. Vazamento de dados pessoais e outros incidentes

Os vazamentos de dados pessoais e outros incidentes deverão ser comunicados à ANPD e ao titular dos dados pessoais sempre que o incidente possa acarretar dano ou

risco relevante ao titular.

Nessas hipóteses, a comunicação deverá ocorrer em prazo razoável, tendo a ANPD recomendado 2 dias úteis a contar da data do conhecimento do incidente.

A comunicação deverá conter:

1. Descrição de qual foi a natureza dos dados pessoais afetados;
2. Informação sobre quais titulares foram envolvidos;
3. Indicação das medidas técnicas e de segurança da informação utilizadas para a proteção dos dados;
4. Caso a comunicação não tiver sido imediata, deverão ser indicados os motivos da demora;
5. Indicação das medidas adotadas para remediar ou mitigar os efeitos do incidente.

A ANPD, nesses casos, poderá determinar a adoção de determinadas medidas pelo controlador. Essas medidas incluem a ampla divulgação do fato nos meios de comunicação, de forma a garantir que os titulares sejam informados a respeito do evento. A ANPD também poderá determinar medidas específicas a serem adotadas pelo controlador para a mitigação ou reversão do dano.

O VAZAMENTO DE DADOS DA ENEL EM OSASCO

Em 2020, 4% da base de clientes da ENEL em Osasco foram afetados por um vazamento de dados pessoais. No fim, quase 290 mil clientes foram afetados. Os dados vazados supostamente incluíam nome, gênero, CPF/CNPJ, RG, data de nascimento, números de telefone, e-mail, endereço postal, conta bancária, forma de pagamento, código da instalação, código e tempo de contrato, média de consumo energético e carga instalada.

Ocorrido o vazamento, a ENEL passou a comunicar os titulares de dados pessoais mediante carta e e-mails, assim como informou a respeito do perigo de fornecimento de senhas a terceiros, isto é, a ENEL adotou medidas preventivas para a prática de phishing, que poderia alcançar um pico após o vazamento.

Remédios

Algumas cláusulas poderão ser previstas como remédios ou mitigadoras para os riscos de privacidade e proteção de dados. São essas cláusulas, a depender do caso:

1. Termo de consentimento;
2. Cláusula que explicite a finalidade do tratamento;
3. Cláusula com informações sobre a segurança do tratamento;
4. Cláusula com informações

sobre os dados que serão tratados;

Para conferir efetividade à LGPD, devem ser observados os deveres de Informação e comunicação. Além disso, deverão ser elaborados relatórios informativos e preventivos. Na hipótese de não haver adoção imediata das providências devidas, deverá ser fornecida a justificativa cabível.

8. As requisições de titulares

Os titulares são os donos de seus dados e têm assegurada pela LGPD o exercício de direitos explícitos a respeito destes.

Cabe ao titular a solicitação perante o controlador do exercício dos seguintes direitos:

1. Obter confirmação de que o tratamento de dados pessoais existe;

2. Acesso facilitado aos dados pessoais que se referem a si próprio, ou seja, ao titular dos mencionados dados pessoais. Também há o direito de informação a respeito das entidades públicas e privadas com as quais o controlador tenha realizado uso compartilhado.

3. Ver corrigidos ou corrigir os dados incompletos, inexatos ou desatualizados;

4. Quando os dados forem desnecessários ou excessivos para a finalidade do tratamento, o titular de dados pessoais poderá solicitar a anonimização, o bloqueio ou a eliminação desses dados;

5. O titular deverá ter direito e garantia de poder transferir os dados a outro fornecedor de serviço ou produto. Isto é: os dados devem ser passíveis de portabilidade.

6. O titular tem direito à eliminação dos dados pessoais;

7. O titular tem direito a ser informado sobre a possibilidade de não fornecer o seu consentimento, quando este for aplicável, e das consequências que decorrem dessa negativa;

8. Sendo aplicável e tendo sido concedido, o titular de dados pessoais poderá revogar seu consentimento a qualquer momento.

Parte III - O imprescindível levantamento de informações

A fim de mapear as atividades de tratamento de dados pessoais da instituição, o responsável pelo tratamento de dados pessoais deverá levantar informações tais como listadas a seguir, o que permitirá

determinar medidas de adequação cabíveis:

Passo 1: Há tratamento de dados pessoais? Os dados pessoais são dados sensíveis ou anonimizados?

a. Se há tratamento de dados anonimizados, há possibilidade de reversão da anonimização?

Passo 2: Qual a base legal para o tratamento de dados pessoais?

b. Se a base legal for o consentimento, foi recolhido o consentimento específico, informado, sem vícios e para a finalidade específica?

c. Qualquer que seja a base legal, o titular foi ou será informado a respeito do tratamento de seus dados?

Passo 3: Há tratamento de dados de crianças ou adolescentes? Há transferência internacional de dados?

d. A base legal é compatível?

e. Se o consentimento, este foi ou será coletado?

f. Se sim, os requisitos específicos dessas modalidades de tratamento foram atendidos?

Passo 4: Qual a finalidade do tratamento dos dados pessoais? Os dados são tratados exclusivamente para atingir essa finalidade? Há outro propósito para o tratamento dos dados?

Passo 5: Onde os dados são armazenados?

g. Trata-se de ambiente seguro?

Passo 6: Por quanto tempo os dados ficam armazenados/retidos?

h. Qual o propósito e/ou justificativa legal para tal prazo?

Passo 7: Há exclusão dos dados após um período determinado? Se não, a justificativa é suficiente para os fins da LGPD?

i. Qual a forma do descarte? A forma de descarte é segura?

Passo 8: Os meios de segurança da informação são suficientes, considerando a tecnologia atual e parâmetros razoáveis?

j. São suficientes?

Passo 9: Em caso de vazamento ou outros incidentes com risco ou dano considerável, há ciência de que existe um dever de comunicar a ANPD e os titulares dos dados pessoais, em determinadas circunstâncias?

k. Existe um procedimento por escrito, aprovado e treinamento dos responsáveis?

Biografia

André Castro Carvalho

Bacharel (2007), Mestre (2010) e Doutor (2013) pela Faculdade de Direito da Universidade de São Paulo, tendo sua tese de doutorado recebido o Prêmio CAPES de Tese 2014 na área do Direito. Realizou estudos de pós-doutorado como visiting researcher no Massachusetts Institute of Technology - MIT (2016), sendo bolsista do Programa Estratégico - DRI (Estágio Pós-Doutoral) da CAPES, e concluiu o Programa de Pós-Doutorado realizado no Departamento de Direito Econômico, Financeiro e Tributário da Faculdade de Direito da Universidade de São Paulo (2018). Foi bacharelando (incompleto) em Economia pela Faculdade de Economia, Administração e Contabilidade - FEA da Universidade de São Paulo, tendo iniciado os estudos em 2011 e interrompido em 2012. Foi visiting researcher na Karl Franzens Universität Graz, na Áustria (2013), pelo Coimbra Group Scholarship Programme for Young Professors and Researchers from Latin America, e visiting scholar and professor na Nankai University (Tianjin) e JiLin University (Changchun), ambas na China (2012-2013), durante o período de doutorado. Possui certificação em treinamento corporativo em AML/CTF para uma instituição financeira emitido pela International Compliance Association - ICA em conjunto com a Manchester Business School (2014-2015), e é certificado em AML pela ACAMS (2019). É professor na pós-graduação no Ibmec-SP; professor regular na educação executiva em Compliance e no curso de LL.M do Insper; professor do MBA ESG/Exame e do MBA em Data Science da Trevisan Escola de Negócios. Também atua (ou atuou) como professor convidado em outros programas de extensão e de pós-graduação de diversas instituições de ensino, como PUC-SP, FIA, FIPE, FEA-USP, FD-RP, UFSCar, Unifor, EPM, ESA-DF, ABBC Educacional, Instituto Brasileiro de Ciências Bancárias - INFI e Associação Brasileira de Câmbio (ABRACAM). Foi professor de graduação de Direito Administrativo da Faculdade de Direito de São Bernardo do Campo (2011-2013), de Direito Econômico da Universidade Ibirapuera (2014) e de Direito Financeiro da Faculdade Autônoma de Direito - FADISP (2010).

Rua Fernandes Moreira, 507, Chácara Santo Antônio, São Paulo | @fundacaopodemos | fundacaopodemos.org.br