POLÍTICA DE PROTEÇÃO DE DADOS DA AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO – AD Diper

2021

1) DEFINIÇÕES

Autoridade Nacional de Proteção de Dados (ANPD) - Autoridade Nacional de Proteção de Dados é órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Aviso de Privacidade - Instrumento pelo qual o Controlador fornece informações completas sobre as características essenciais do tratamento.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade ou Conselho (LGPD) - O Conselho Nacional de Proteção de Dados e da Privacidade é composto por representantes, titulares suplentes, dos órgãos: Poder Executivo Federal, Senado Federal, Câmara dos Deputados, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Comitê Gestor da Internet no Brasil, entidades da Sociedade Civil com atuação comprovada em proteção de dados pessoais, instituições científicas, tecnológicas e de inovação, entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais.

Compete ao Conselho propor diretrizes à Política Nacional de Proteção de Dados; elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; sugerir ações a serem realizadas pela ANPD; elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral, nos termos do art. 58-B da LGPD.

Consentimento - Consentimento deverá ser fornecido através de uma afirmação clara estabelecendo uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, tais como por consentimento escrito, incluindo meios eletrônicos, ou por declaração verbal, desde que mediante prova do seu consentimento.

Controlador - Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (Controlador), sozinho ou juntamente a outros Controladores (Co-Controladores).

Dado Pessoal - Dado Pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável, tais como nome, número de identificação, dados de localização, um identificador online ou a um ou mais dos elementos característicos de sua identidade física, fisiológica, genética, mental, econômica, cultural ou social (veja também Categorias especiais de dados pessoais).

Dados Pessoais Sensíveis (incluindo biométricos e referentes à saúde) - Categoria de 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. Esses dados são definidos pela LGPD como "Dados Pessoais Sensíveis":

a. "Dados genéticos": dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa física que fornecem informações unívocas sobre a fisiologia ou sobre a saúde de tal pessoa física, e que resultam designadamente da análise de uma amostra biológica da pessoa física em questão;

b. "Dados biométricos": dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa física que permitam ou confirmem a identificação única dessa pessoa, tais como foto, vídeo, imagens da face ou dados de impressão digital;

c. "Dados relativos à saúde": dados pessoais relacionados com a saúde física ou mental de uma pessoa física, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

Encarregado ou DPO (Data Protection Officer) -Pessoa natural encarregada de supervisionar e dar suporte ao Controlador ou ao Operador em todos os temas relacionados ao tratamento de Dados Pessoais. O DPO desempenha um papel consultivo, ele/ela supervisiona a conformidade à LGPD, pelo Controlador e o Operador, e é a referência e ponto de contato com a Autoridade Nacional e com os Titulares, de acordo com o que está previsto na LGPD e nesta Política.

Incidente de Segurança de Dados - O incidente de Segurança de Dados é uma violação de segurança que leva ao acesso, divulgação não autorizada, alteração, perda

ou destruição acidental ou ilegal de Dados Pessoais transmitidos, armazenados ou de outra forma tratados.

Legítimo Interesse - O legítimo interesse é uma das bases legais para tratar Dados Pessoais e é definido pela relação especial que une o Controlador ao Titular.

Lei Geral de Proteção de Dados ou LGPD - Lei Federal nº 13.709/18 que 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.

Medidas de Segurança - Medidas 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, de acordo como o Art. 46 da Lei Federal nº 13.709/18 e sua respectiva regulamentação.

Operador - Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Pseudonimização, anonimização e criptografia - A pseudonimização significa o tratamento de dados pessoais de forma que deixem serem atribuídos a um Titular específico, salvo se recorrer-se à informações suplementares, e desde que essas informações suplementares sejam mantidas arquivadas separadamente. Já a anonimização, é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Criptografia, por sua vez, o processo de transformar informação usando um algoritmo de modo a impossibilitar a sua leitura a todos exceto aqueles que possuam uma identificação particular, geralmente referida como chave.

Relatório de Impacto à Proteção de Dados Pessoais ou DPIA - Avaliação de risco destinada a (a) Descrever o projeto de tratamento do dado e suas finalidades; (b) Avaliar a necessidade e proporcionalidade do tratamento; (c) Avaliar os riscos para os direitos e liberdades do Titular decorrentes do tratamento; (d) Determinar e mitigar medidas; e (e) Quando considerado necessário pelo DPO, confrontar os resultados do DPIA com a Autoridade Nacional.

Titular dos Dados Pessoais - Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.Ele /Ela é entendido(a) como uma pessoa natural identificada ou identificável.

Transferência Internacional de Dados - Há transferência internacional de dados quando há transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento - 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.

2) ARGUMENTO LEGAL

Em conformidade com o art. 8º, inciso IV, da Lei Federal nº 13.303, de 30 de junho de 2016, a Diretoria e o Conselho de Administração da Agência de Desenvolvimento Econômico de Pernambuco – AD Diper subscrevem a presente Política de Divulgação de Informações, aprovada em suas reuniões realizadas nos dias 07 de maio de 2021 e 12 de maio de 2021, respectivamente.

3) IDENTIFICAÇÃO GERAL

CNPJ nº 10.848.646/0001-87

NIRE: 26300033534

Sede: Recife/PE

Tipo de estatal: Sociedade de Economia Mista

Acionista controlador: Estado de Pernambuco

Tipo societário: Sociedade anônima

Tipo de capital: Fechado

Abrangência de atuação: Internacional

Setor de atuação: Apoio Desenvolvimento Econômico e Social do Estado de Pernambuco; Promoção do desenvolvimento do Estado de Pernambuco por meio de ações indutoras e apoio aos setores industrial, energético, agroindustrial, comercial, de serviços, florestal e mineral, nos termos da legislação vigente, bem relacionados ao artesanato e à cultura pernambucana, promovendo programas de como articular a atração de novos investimentos; Exercício de atividades de pesquisa, exploração e aproveitamento de jazidas minerais no território nacional e Fomento à cultura estadual e ao artesanato, de acordo com os limites da legislação estadual vigente.

Membros da Unidade responsável pela Política:

Fabiana Freitas Wanderley

Maria de Fátima Vilaça de Souza Barbosa

Nathaly Scavuzzi Menezes Medeiros de Souza

Simone Medeiros

Conselheiros de Administração subscritores da Política:

Luciana Barbosa de Oliveira Santos – CPF: 809.199.794-91

Fernandha Batista Lafayette – CPF: 014.527.774-70

Marcelo Andrade Bezerra Barros – CPF: 652.895.104-78

Dilson de Moura Peixoto Filho – CPF: 123.301.914-72

André Longo Araújo de Melo – CPF: 768.999.934-49

Renato Xavier Thièbaut – CPF: 009.916.297-01

Eduardo Jorge de Albuquerque Machado Moura – CPF: 022.133.734-26

Diretores subscritores da Política:

Roberto De Abreu e Lima Almeida – CPF: 374.880.824-00 – Diretor Presidente;

Bruno Aurélio Santos Lira – CPF: 013.349.184-65 - Diretor de Incentivos Fiscais;

Janaína Cardoso Acioli – CPF: 963.320.854-87 - Diretora de Gestão;

José André de Lima Freitas da Silva – CPF: 029.566.434-79 - Diretor de Atração de Investimentos;

Márcia Maria da Fonte Souto – CPF: 318.185.954-00 - Diretora de Promoção do Artesanato;

Marcello Luis Rodrigues Araújo – CPF: 029.740.584-50 - Diretor de Infraestrutura.

Data de divulgação: Maio/2021

4) OBJETO E OBJETIVO DO DOCUMENTO

A LGPD estabelece regras e princípios para o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD define que a proteção de dados pessoais no Brasil tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A AD Diper reconhece o valor da privacidade e da proteção de dados como bem comum e boas práticas de negócios, promovendo sua implementação sistematicamente com a LGPD e a regulamentação aplicável.

A presente política tem o propósito de nortear as ações dos agentes públicos na prestação de informações corporativas objetivas, confiáveis e tempestivas, com qualidade, transparência, veracidade, completude, consistência, equidade e tempestividade, no relacionamento com acionistas, investidores, público e formadores de opinião e aplica-se à AD Diper no que diz respeito à sua atuação de acordo com as leis, regulamentos e normas de governança aplicáveis à Proteção de Dados Pessoais.

Busca-se, igualmente, divulgar com homogeneidade e simultaneidade, a gestão dos negócios, fatos ou atos de caráter político-administrativo, técnico, negocial ou econômico, capazes de afetar valor da empresa ou influenciar a decisão dos investidores ou a percepção da sociedade.

Como base legal para o presente instrumento, considerou-se a Constituição da República Federativa do Brasil de 1988 – art. 5, X ("CRFB"); a Lei Federal nº 8.078/1990 – Código de Defesa do Consumidor ("CDC"); a Lei Federal nº 12.965/2014 e seu Decreto Regulamentador 8.771/2018 – ("Marco Civil da Internet'); e a Lei Federal nº 13.709/2018 Lei Geral de Proteção de Dados – ("LGPD").

5) ESCOPO DE APLICAÇÃO

No que diz respeito ao escopo de aplicação, o art. 3º da Lei Federal 13.709/2018, estabelece que a LGPD recai sobre qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

a. A operação de tratamento seja realizada no território nacional;

b. A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

c. Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Portanto, o presente documento aplica-se a todas as operações da AD Diper que tratam dados pessoais. Este documento estende-se, também, às operações da AD Diper realizadas fora do território brasileiro que tratam dados pessoais coletados no Brasil, ou que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil.

6) PRINCÍPIOS GERAIS

A proteção de Dados Pessoais na AD Diper será baseada nos seguintes princípios fundamentais, majoritariamente previstos pela LGPD:

6.1. Princípio da Finalidade: A realização do Tratamento pela AD Diper deve se dar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de Tratamento posterior de forma incompatível com essas finalidades.

6.2. Princípio da Adequação: A AD Diper deve garantir a compatibilidade do Tratamento com as finalidades informadas ao titular, de acordo com o contexto do Tratamento.

6.3. Princípio da Necessidade: O Tratamento realizado pela AD Diper deve limitar-se 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. Assim, a coleta de Dados Pessoais pela AD Diper deve ser limitada ao indispensável.

6.4. Princípio de Livre acesso: A AD Diper deve garantir aos titulares consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como sobre a integralidade de seus dados pessoais.

6.5 Princípio da Qualidade dos dados: A AD Diper deve garantir aos titulares exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento.

6.6. Princípio da Transparência: A AD Diper deve garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do Tratamento e sobre os Controladores e Operadores nele envolvidos, observados os segredos comercial e industrial.

6.7. Princípio da Segurança: A AD Diper deve garantir a utilização de Medidas de Segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de Dados Pessoais.

6.8. Princípio da Prevenção: A AD Diper deve garantir a Adoção de medidas para prevenção da ocorrência de danos em virtude do Tratamento de dados pessoais.

6.9. Princípio da Não-discriminação: A AD Diper não deve realizar nenhum Tratamento para fins discriminatórios ilícitos ou abusivos.

6.10. Princípio da Responsabilização e Prestação de contas: A AD Diper deve garantir a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. A AD Diper, por meio de documentação e demonstração de processos internos, prestará contas às Autoridades e aos Colaboradores, e a quem mais entender relevante, quanto à observância das medidas que dão efeito aos princípios acima indicados.

Isto implica em uma atualização contínua para as melhores práticas de proteção de dados e um esforço correspondente para incorporá-las dentro da estratégia, da organização e dos negócios da AD Diper.

O princípio da responsabilização requer, também, uma utilização mais ampla das metodologias de avaliação de risco, a exemplo do Relatório de Impacto à Proteção de Dados Pessoais (DPIA) como um processo de tomada de decisão centrado nos interesses do Titular. Isto implica um dever do Controlador e do Operador de executar um DPIA não apenas nos tratamentos já em curso, mas também no desenho de nova organização, processo, plataforma digital e algoritmo, e assim por diante.

6.11. Princípio da *privacy by design* (desde a concepção) e *by default* (por padrão): Princípio não previsto expressamente pela LGPD, mas que é consolidado em todo o mundo e, segundo o qual, a AD Diper deve colocar em prática medidas técnicas e

organizacionais adequadas para garantir, e poder demonstrar, que qualquer tratamento de Dados Pessoais é desenvolvido considerando todos os requerimentos aplicáveis à proteção de dados pessoais, desde o início do projeto ou da operação. Estas medidas devem ser incluídas nos projetos desde o princípio, considerando o custo de implementação, a natureza, o escopo, o contexto e finalidade do tratamento, bem como a probabilidade e a gravidade do risco para os direitos e liberdades do Titular em virtude do tratamento ("privacy by design").

O Controlador deve assegurar que, por padrão (by default), apenas Dados Pessoais que sejam necessários para cada finalidade específica de tratamento sejam processados ("privacy by default"). Esta obrigação aplica-se a todos os Dados Pessoais coletados, à extensão de seu tratamento, o período de seu armazenamento e a sua acessibilidade.

Se necessário, essas medidas devem ser revistas e atualizadas, considerando-se a evolução das melhores práticas.

A contratação de terceiros para tratamento de dados deve ser desenvolvida e implementada de maneira a que este terceiro tenha nível apropriado de segurança equivalente aos padrões da AD Diper. Qualificação de fornecedores e cláusulas contratuais visam a proteção de dados pessoais.

7) TRATAMENTO DOS DADOS PESSOAIS

As áreas da AD Diper, com o apoio do encarregado, têm o dever de seguir as instruções emitidas pela Autoridade Nacional de Proteção de Dados, bem como as melhores práticas para garantir a privacidade e a Proteção de Dados dos Titulares.

No momento de tratar os dados é necessário atentar para algumas especificidades, tais como:

7.1. Anonimização

Tratamento de Dados Pessoais contempla as seguintes atividades: pesquisa, coleta através de qualquer instrumento ou sensor, escuta e gravação (foto, vídeo, voz etc.), identificação, uso, gerenciamento, manuseio, organização, estruturação, armazenamento (incluindo armazenamento físico e gerenciamento e manutenção de

servidor em que os Dados Pessoais são armazenados, mesmo que temporariamente), comparação, compilação, duplicação, perfilamento (profiling) conservação, adaptação, modificação, integração, correção, inspeção, uso, extração, consulta, comunicação, transmissão, disseminação, segregação de pontos de vista, eliminação, cancelamento, destruição; pseudonimização, anonimização e criptografia.

Os Dados Pessoais, após submetidos a processo efetivos de anonimização perdem a qualidade dos Dados Pessoais, salvo quando tais procedimentos forem revertidos ou reversíveis.

7.2. Consentimento

O consentimento deve ser dado por um claro ato afirmativo estabelecendo uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, o que pode ocorrer por uma declaração escrita ou oral, incluindo por meios eletrônicos, sempre mediante comprovação pelo Controlador.

Pode incluir a marca em *check box (opt-in)* ao visitar um site da AD Diper ou outra declaração ou conduta que indique claramente, neste contexto, a aceitação do Titular sobre o tratamento proposto de seus Dados Pessoais. O silêncio e a inércia do Titular diante de *check box* previamente marcadas/selecionadas não configuram consentimento.

O consentimento deve ser aplicado a todas as atividades de tratamento realizadas para a mesma finalidade. Se o tratamento tiver mais de uma finalidade, o consentimento deve ser fornecido para cada uma dessas finalidades, por exemplo, em caixas separadas. Conforme o § 2º do art. 9º da LGPD, se houver mudança da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente ao titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde com as alterações.

Se o consentimento do Titular for coletado por meio eletrônico, o pedido deve ser claro, conciso.

O Controlador, juntamente com o Operador, são responsáveis por coletar legalmente o consentimento do Titular e têm a obrigação de demonstrar perante a Autoridade

Nacional que a coleta de consentimento foi realizada legalmente e em total respeito aos regulamentos de privacidade e à LGPD.

Enquanto durar uma atividade de Tratamento baseada no consentimento do Titular, a obrigação de demonstrar esse consentimento existe. Após o término da atividade de Tratamento, a prova de consentimento deve ser mantida pelo tempo estritamente necessário para o cumprimento de uma obrigação legal ou para que a empresa possa exercer seus direitos ou defendê-los em demandas judiciais, administrativas ou arbitrais.

Para as atividades de Tratamento baseadas no consentimento do Titular, o compartilhamento de Dados Pessoais com terceiros apenas pode ser realizado mediante consentimento específico e em destaque, nos termos do § 5º do art. 9º da LGPD.

A fim de obter o consentimento informado de crianças e adolescentes, bem como para todas as pessoas vulneráveis, o Controlador deve explicar em linguagem clara e simples para as crianças como ele pretende tratar os dados que coleta. Os pais ou um representante legal da criança deve(m) consentir, de modo que um conjunto de informações será necessário para permitir que o(s) adulto(s) tome(m) uma decisão informada.

Como regra geral, se o consentimento for revogado, todas as operações de Tratamento que foram nele baseadas e ocorreram antes da retirada do consentimento permanecem legais.

7.3. Aviso de Privacidade

O aviso de privacidade deve ter um texto conciso, claro, simples e compreensível pelos vários públicos (ex: menores de idade, portadores de necessidades especiais, etc.) e ser fornecido ao Titular no momento da coleta dos Dados Pessoais, contendo:

- Informações gerais, identificação e de Contato do Controlador;
- Informações gerais e de contato do Encarregado – DPO;
- Objeto e modalidades do Tratamento;
- Finalidade e base legal do Tratamento;
- Fonte dos Dados Pessoais;

- Destinatários com quem os Dados Pessoais sejam compartilhados;
- Transferência de Dados Pessoais;
- Responsabilidades dos Agentes que realizam o tratamento (Controlador e do Operador);
- O período de armazenamento de Dados Pessoais;
- Qualquer uso de tomada de decisão automatizada;
- Os direitos dos Titulares e os meios para exercê-los.

O Encarregado é o responsável pela aprovação de qualquer Aviso de Privacidade na AD Diper e o documento deve ser revisto sempre que houver qualquer mudança no tratamento dos Dados Pessoais.

8) REGISTROS DOS TRATAMENTOS DE DADOS

Considerando as imposições legais impostas à Administração Pública, face ao Princípio Constitucional da Publicidade, a divulgação é a máxima. O acesso a documentos e informações públicas é a regra, sigilo é a exceção. Se a alta administração entender que a divulgação coloca em risco interesse legítimo da empresa, deve-se dar o tratamento adequado à informação, classificando-a e mantendo-a em sigilo.

A LGPD prevê que o Controlador e o Operador devem manter registro das operações de Tratamento que realizarem ("Registro " de forma independente um do outro). Para garantir o cumprimento da obrigação da LGPD, é primordial que haja um mapeamento dinâmico do tratamento e seu ciclo de vida.

O conteúdo mínimo do registro do Controlador deve apresentar:

- O nome e os dados de contato do Controlador e, quando aplicável, dos Controladores Conjuntos, do representante legal do Controlador e do Encarregado-DPO;
- As finalidades do tratamento;
- Descrição das categorias de Titulares e das categorias de Dados Pessoais;

- As categorias de destinatários para os quais os Dados Pessoais foram ou serão divulgados, incluindo destinatários em terceiros países ou organizações internacionais;

- Quando aplicável, as transferências internacionais de dados pessoais para outro país ou uma organização internacional, incluindo a identificação desse outro país ou organização internacional.

- Sempre que possível, os prazos previstos para o descarte das diferentes categorias de Dados Pessoais;

- Sempre que possível, uma descrição geral das medidas de segurança referidas no Art. 46 da LGPD.

9) RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RPID)

O Relatório de impacto à Proteção de Dados Pessoais ("RIPD") é a documentação do Controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Assim, o RIPD é um processo destinado a:

- Descrever o projeto ou o processo de Tratamento de Dados e sua finalidade;

- Avaliar a necessidade e proporcionalidade do Tratamento;

- Avaliar os riscos dos direitos e liberdades do Titular decorrentes do Tratamento;

- Determinar as medidas de mitigação, e;

- Quando considerado necessário, o DPO deverá apresentar os resultados da RIPD à Autoridade Nacional.

O risco deve ser entendido como um risco de impacto negativo nos direitos e liberdades do Titular.

A probabilidade e a gravidade do risco para os direitos e liberdades do Titular devem ser determinadas por referência à natureza, âmbito, contexto e finalidades do tratamento. O risco deve ser avaliado com base em uma avaliação objetiva, através da

qual se estabeleçam se as operações de tratamento de dados envolvem um risco ou um alto risco.

A LGPD não estabelece hipóteses nas quais a elaboração do RIPD é obrigatória, definindo apenas que a Autoridade Nacional pode determinar sua execução. Dispõe, no entanto, em seu Art. 37 que o Controlador e o Operador devem manter registro das operações de Tratamento que realizarem, especialmente quando baseadas em legítimo interesse. Assim, o Controlador e o Operador deverão registrar o Tratamento de forma que seja viável a elaboração do RIPD em todas as situações em que haja Tratamento.

10) ENCARREGADO (DATA PROTECTION OFFICER - DPO)

A LGPD exige que as organizações que realizam o Tratamento de Dados Pessoais nomeiem um Encarregado pelo tratamento de dados pessoais (DPO) que deve exercer as atividades previstas no § 2º do Art. 41 da lei.

O DPO é selecionado considerando sua experiência em privacidade e proteção de dados, suas características profissionais, sua habilidade para cumprir as tarefas que lhe sejam atribuídas. O DPO pode ser um funcionário da AD Diper ou um terceiro contratado para este serviço.

O Controlador e o Operador devem envolver o DPO em todas as questões relativas à proteção de Dados Pessoais e garantir sua independência na execução das funções, observando que sejam:

- Garantidos os recursos necessários para executar seus deveres;
- Assegurando que ele / ela não receba instruções, nem seja penalizado por suas decisões e por seus pareceres;
- Garantindo que o DPO não atue em situações de conflitos de interesse.

O DPO deve manter sua atividade em sigilo e confidencialidade, sendo responsável por:

- Garantir que haja o devido atendimento às reclamações e comunicações dos Titulares, que sejam prestados os esclarecimentos e adotadas as providências necessárias;

- Apoiar e aconselhar o Controlador e o Operador em relação às obrigações decorrentes da legislação e regulamentação de proteção de dados, especialmente em relação à LGPD e às normas editadas pela Autoridade Nacional.

- Projetar programas de conformidade e monitorar a implementação, definir governança de proteção de dados, avisos de privacidade padrão, cláusulas contratuais e boas práticas.

- Apoiar o Controlador e o Operador na negociação de contratos de proteção de dados, definir o fluxo de atendimento dos direitos dos Titulares; definir e implementar planos de treinamento e conscientização aos colaboradores;

- Fornecer, se necessário, uma opinião sobre a avaliação do impacto na proteção de dados e monitoramento de progresso;

- Cooperar e atuar como ponto de referência da Autoridade Nacional, recebendo comunicações e adotando providências;

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

11) O CONTROLADOR E O OPERADOR

11.1. Controlador

Quando estiver atuando como Controladora, a AD Diper tem o dever de consultar as instruções emitidas pela Autoridade Nacional e também as diretrizes e melhores práticas reconhecidas em matéria de proteção de dados pessoais.

O Controlador define a finalidade do tratamento de Dados Pessoais e deve implementar medidas técnicas e organizacionais apropriadas para assegurar a proteção de Dados Pessoais de acordo com a LGPD.

A AD Diper tem ainda o ônus de provar a conformidade com a LGPD e, com o suporte do DPO, deve:

- Planejar e executar as medidas adequadas de segurança, privacyby design e by default, aplicando as melhores práticas e os mais altos padrões de mercado;

- Treinamento contínuo aos seus próprios empregados e terceiros;

- Verificar o cumprimento da LGPD nos terceiros que tratam os dados em seu nome;

- Cooperar com a Autoridade Nacional nos cursos de suas iniciativas de investigação;

Os Controladores, quando Conjuntos, devem determinar de forma transparente, mediante acordo, suas respectivas responsabilidades em relação ao cumprimento das obrigações decorrentes da LGPD, em especial no que diz respeito ao exercício dos direitos pelos Titulares.

10.2. Operador

A AD Diper, quando estiver atuando como Operadora, tem o dever de consultar e atender às disposições da Lei Geral de Proteção de Dados e àquelas eventualmente emitidas pela Autoridade Nacional acerca de suas responsabilidades enquanto Operador.

As seguintes indicações são exemplificativas não exaustivas sobre o tema:

- Quando o Tratamento for executado em nome de um Controlador, não deve envolver outro Operador (Sub Operadores) nas atividades de Tratamento realizadas em nome de um Controlador sem autorização prévia específica ou geral por escrito do respectivo Controlador.

- Ao buscar um Operador para realizar tratamento de Dados em seu nome, a AD Diper deve garantir que o Operador siga as instruções e que seja estipulada de forma clara a natureza, a duração e a finalidade do tratamento, o tipo de Dados Pessoais Tratados, as categorias dos Titulares, as obrigações e os direitos do Controlador.

Ao estabelecer um acordo, a AD Diper, como Controlador, deve estabelecer que o Operador:

- Trate os Dados Pessoais somente em instruções documentadas do Controlador, incluindo com referência a transferência dos Dados Pessoais a um terceiro país ou organização internacional, a não ser que seja obrigado a fazê-lo pela legislação a qual o Operador esteja submetido; nestes casos o Operador deverá informar ao Controlador todos os requerimentos legais antes do Tratamento, a menos que a lei proíba tais informações;

- Assegure que as pessoas autorizadas a tratar os Dados Pessoais tenham a obrigação contratual ou legal de manter sigilo e confidencialidade;

- Adote todas as medidas de segurança exigidas nos termos do, bem como Art. 46 da Lei Geral de Proteção de Dados;

- Respeite as condições estabelecidas pela Lei Geral de Proteção de Dados para subcontratar outro Operador, com a obrigação de garantir que a transferência internacional de dados para fora do Brasil será executava apenas para países considerados adequados com a legislação de privacidade local, e um documento contratual adequado seja previamente assinado entre o Operador e o Suboperador para garantir o os direitos dos Titulares;

- Adote, considerando a natureza do tratamento, medidas técnicas e organizacionais apropriadas, na medida do possível, que permitam ao Controlador atender as requisições dos Titulares no exercício de seus direitos, conforme previstos no Capítulo III da Lei Geral de Proteção de Dados;

- Preste assistência ao Controlador para garantir a conformidade com obrigações relacionadas às medidas de Segurança (Capítulo VII da Lei Geral de Proteção de Dados), Notificação e Comunicação de Incidente de Segurança de Dados (Art 48 da Lei Geral de Proteção de Dados) e RIPD(Art. 38 da Lei Geral de Proteção de Dados);

- Elimine ou devolva, a critério exclusivo do Controlador, todos os Dados Pessoais ao término da prestação dos serviços relacionados, deletando cópias existentes, a não ser que disposto expressamente em contrário na legislação aplicável para o armazenamento dos Dados Pessoais objeto do respectivo Tratamento.

- Disponibilize ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas na Lei Geral de Proteção de Dados;

12) MEDIDAS DE SEGURANÇA

O Controlador tem o dever de consultar e atender às disposições contidas na Lei Geral de Proteção de Dados e àquelas que venham a ser emitidas pela Autoridade Nacional acerca das medidas de segurança aplicáveis às atividades de Tratamento.

Considerando as condições existentes, os custos de implementação, a natureza, âmbito, contexto e finalidades do Tratamento, bem como o risco e impacto perante os direitos e liberdades dos Titulares, o Controlador e o Operador devem implementar medidas técnicas e organizacionais destinadas a garantir um nível de segurança adequado, incluindo, entre outras, as medidas de *privacy by design* (desde a concepção) e *privacy by default* (por padrão). O Controlador e o Operador devem:

- Rever e proteger todos os sistemas, identificação de aplicações e infraestruturas e acesso lógico;
- Rever e gerir de forma segura os Dados Pessoais e Sensíveis, com o objetivo de garantir uma elevada qualidade de dados e de forma que o Tratamento se limite ao necessário e ao adequado;
- Segregar os Dados Pessoais e perfilar usuários que lidem com Dados Pessoais, limitando acesso e atribuições de acordo com o estritamente necessário para execução de suas tarefas.
- Pseudonimizar, anonimizar e criptografar Dados Pessoais e Sensíveis. A escolha entre as três opções deve ser a disponível ao Controlador e ao Operador;
- Assegurar permanentemente a confidencialidade, integridade, disponibilidade e resistência dos sistemas empregados nos Tratamentos;
- Restaurar prontamente o acesso e disponibilidade dos Dados Pessoais em caso de incidentes de segurança;
- Testar, verificar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Tratamento.

Ao avaliar o nível adequado de segurança, devem ser considerados os riscos apresentados pelo Tratamento, particularmente em caso de conduta ilegal ou acidental

que leve a destruição, perda, alteração, divulgação não autorizada ou ao acesso do Dado Pessoal transmitido, armazenado ou de outra forma Tratado.

A adesão a um código de conduta aprovado pela Autoridade Nacional ou a um mecanismo de certificação aprovado em linha com as boas práticas de Proteção de Dados LGPD pode ser utilizado como elementos para demonstrar a conformidade com a LGPD.

13) INCIDENTE DE SEGURANÇA DE DADOS E DIREITO DE AUDITORIA

A implementação de medidas de segurança no âmbito do art. 46 da LGPD, juntamente com as medidas previstas na Política de Segurança da Informação e no Plano de Resposta à Incidentes de Segurança, devem ser instrumentos apropriados para prevenir Incidentes de Segurança de Dados.

O Controlador terá o direito, a qualquer momento, durante a vigência do Contrato e/ou durante todo o período em que o Operador retiver os Dados Pessoais do Controlador, de realizar uma avaliação interna ou auditoria para confirmar que o Operador e/ou Sub Operador está agindo em conformidade com esta Política e a LGPD, mediante notificação do Operador com 10 (dez) dias úteis de antecedência.

O Operador deverá disponibilizar, a qualquer momento, todas as informações necessárias para demonstrar conformidade com esta Política e com o Contrato, e deverá permitir e contribuir com auditorias, incluindo verificações e inspeções periódicas, pelo Controlador ou por auditor enviado pelo Controlador, em relação ao Tratamento dos Dados Pessoais do Controlador. No caso de quaisquer problemas de segurança encontrados durante tais auditorias, o Operador deverá tomar, às suas próprias custas, todas as ações necessárias para resolver os problemas mencionados.

O Controlador terá o direito de notificar o Operador e/ou Sub Operador sobre qualquer possível risco de eventual ocorrência de Incidente de Segurança ou descumprimento com quaisquer Leis e Regulamentos de Proteção de Dados que constatar em sua auditoria, devendo o Operador e/ou Sub Operador, em até 30 (trinta) dias corridos, tomar as medidas necessárias, informando o Controlador que poderá, a seu critério, realizar nova auditoria. O Controlador e o Operador têm o dever de consultar e atender às instruções detalhadas na Lei Geral Proteção de Dados e aquelas que venham a ser emitidas pela Autoridade Nacional sobre notificação de incidente de dados pessoais.

14) OS DIREITOS DOS TITULARES

O direito à Privacidade e à Proteção de Dados Pessoais devem ser considerados face aos outros direitos fundamentais, de acordo com o princípio da proporcionalidade.

O Controlador tem que envidar seus melhores esforços, sem atrasos injustificados, para fornecer ao Titular, com uma interface fácil e prática, para o pleno exercício dos direitos de proteção de dados disciplinados pela Lei Geral de Proteção de Dados.

O prazo para uma resposta ao pedido do Titular do Dado é, para todos os direitos, imediato para respostas em formato simplificado, ou no prazo de até 15 (quinze) dias, contado da data do requerimento do titular, em caso de resposta clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida em formato gratuito e de sua escolha. A resposta ao pedido do Titular deve ser por escrito ou por meio de ferramentas eletrônicas, e deve ser clara, concisa e transparente.

O Controlador tem o ônus de provar o pedido manifestamente excessivo ou não fundamentado. Além disso, o exercício de direitos é realizado de forma gratuita ao Titular e é responsável do Controlador adotar medidas técnicas e organizacionais para processar o exercício dos direitos do Titular.

São direitos dos Titulares de Dados, de acordo com a LGPD:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Portabilidade dos dados;
- Eliminação dos dados pessoais tratados com o consentimento;
- Informação sobre entidades públicas e privadas com as quais foi realizado o uso compartilhado de dados;

- Informação sobre a possibilidade de não fornecimento do consentimento e sobre as consequências da negative;
- Revogação do consentimento; e,
- Revisão das decisões automatizadas tomadas com base no tratamento de dados pessoais.

14.1. Direito de Confirmação e Direito de Acesso

O Titular tem o direito de ser informado de que um tratamento de dados relativo aos seus próprios dados está em andamento e, em caso de resposta afirmativa, obter acesso aos seus Dados Pessoais e receber uma cópia destes.

A confirmação de existência ou o acesso a Dados Pessoais serão providenciados em formato simplificado, imediatamente ou dentro prazo de até 15 (quinze) dias por meio de declaração clara e completa, que indique: a origem dos dados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no, contado da data do requerimento do titular.

Os Dados Pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. As informações e os Dados Pessoais poderão ser fornecidos, a critério do Titular: por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa. A cópia dos Dados Pessoais é gratuita.

14.2. Direito de Correção

O Titular tem o direito de obter do Controlador a correção de Dados Pessoais que lhe dizem respeito e que estejam incompletos, inexatos ou desatualizados.

14.3. Direito de Revogação do Consentimento e Direito de Eliminação do Dado Pessoal

O Titular tem o direito de revogar o consentimento anteriormente manifestado a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado. A parte interessada também tem o direito de obter a eliminação dos Dados Pessoais tratados com o consentimento do Titular.

O Controlador deve eliminá-los considerando a tecnologia disponível e os custos de implementação adotando medidas apropriadas.

Devem ser deletados quaisquer links, cópias ou reproduções de seus Dados Pessoais. Exceções somente poderão ser realizadas na medida em que o tratamento seja necessário para:

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados disposto na LGPD
- Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

O Controlador deve informar outros Controladores envolvidos no mesmo tratamento de dados sobre a solicitação de eliminação.

14.4. Direito de Oposição

O Titular tem o direito de obter do Controlador a anonimização, bloqueio ou eliminação de Dados Pessoais:

- Desnecessários;
- Excessivos ou
- Tratados em desconformidade com o disposto na LGPD.

14.5. Direito à portabilidade dos dados

O Titular tem direito a receber de forma estruturada Dados Pessoais fornecidos a um Controlador e tem o direito de transmitir tais dados para outro Controlador, sem interferência do Controlador.

Ao exercer o direito à portabilidade de dados, o Titular tem o direito de obter a transmissão direta de Dados Pessoais, quando tecnicamente viável, de um controlador ou outro.

14.6. Direito de Informação

O Titular sempre tem direito a ser informado de maneira ampla sobre os Tratamento ao qual seus Dados Pessoais são submetidos. Em especial o Titular tem direito a ter informação:

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

- Sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

14.7. Direito à Revisão de Decisões Automatizadas

A parte interessada tem direito de solicitar a revisão de 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.

O Controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Em caso de não oferecimento dessas informações baseado na observância de segredo comercial e industrial, a Autoridade Nacional poderá realizar auditoria para verificação de aspectos discriminatórios em Tratamento automatizado de Dados Pessoais.

15) TEMPO DE RETENÇÃO

O período dos dados armazenamento é estabelecido pela Lei, na maioria casos. Se o Controlador decidir por um período mais longo de tempo de retenção, deverá ser registrado propriamente no Registro de Dados.

Nos casos em que a lei não forneça prazo mínimo para retenção, o Controlador deverá estar apto para justificar o período de retenção de acordo com os Princípios de Responsabilização e Prestação de Contas, Necessidade e Adequação.

Esta Política será revisada com periodicidade anual ou conforme o entendimento do DPO.

A presente política foi atualizada em 12 de maio de 2021.

AD Diper