Série Proteção de Dados

14 PROTEÇÃO DE DADOS NA AMÉRICA LATINA

VEIRANO ADVOGADOS



Este é o décimo quarto capítulo da Série Proteção de Dados. Clique aqui para acessar o cap. 13.



Em 2023, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD") completa 5 anos de sua publicação – agora também com a possibilidade de aplicação das sanções administrativas pela ANPD, que se estende desde agosto de 2021. A Autoridade Nacional de Proteção de Dados ("ANPD") tem atuado ativamente para fomentar a discussão e disseminar os conceitos, práticas e princípios de privacidade e proteção de dados, com a publicação de diversos materiais para conscientização e regulamentação da LGPD desde a sua criação.

O Veirano Advogados tem acompanhado e participado das discussões relacionadas a estes temas. Por isso, nosso time de Proteção de Dados & Privacidade preparou a **Série Proteção de Dados**, na qual serão realizadas publicações periódicas sobre diferentes temas relacionados à privacidade, trazendo não somente os conceitos da LGPD, mas também publicações da ANPD sobre o tema, considerações relevantes, dentre outros conteúdos.



1. Brasil

Lei Aplicável: Lei nº 13,709/2018 ("LGPD"). Entrou em vigor em 18 de setembro de 2020, com exceção das sanções administrativas, que se tornaram exequíveis a partir de 1º de agosto de 2021. O panorama jurídico brasileiro de privacidade e proteção de dados é complexo e conta com leis setoriais específicas, ou seja, a LGPD deve ser entendida e interpretada como parte de um sistema e não como uma lei isolada. Exemplos de leis complementares à interpretação da LGPD são: o Código de Defesa do Consumidor (Lei n° 8.078/1990); a Lei de Interceptação Telefônica (Lei n° 9.296/1996); a Lei do Habeas Data (Lei n° 9.507/1997); a Lei de Telecomunicações (Lei n° 9.472/1997); a Lei de Sigilo Bancário (Lei Complementar n° 105/2001); a Lei do Cadastro Positivo (Lei n° 12.414/2011); Lei de Acesso à Informação (Lei n° 12.527/2011 e Decreto n°7.724/2012); o Marco Civil da Internet (Lei n° 12.965/2014 e Decreto n° 8.771/2016); Código de Ética Médica (Resolução n° 2.217/2018 do Conselho Federal de Medicina; o Marco Legal da Inteligência Artificial (Projeto de Lei nº 2.338/2023); Resoluções CMN n° 4.893/2021 e CMN n° 85/2021 do Banco Central do Brasil; e a Lei nº 14.289/2022.

Localização dos Dados: Embora não existam obrigações gerais de armazenamento/localização de dados, é possível que existam requisitos de armazenamento/localização quando forem tratadas informações confidenciais do Estado (não limitadas a dados pessoais) ou dados relacionados à Administração Pública Federal. Além disso, as Resoluções do Banco Central nº 4.893/2021 e nº 85/2021 estabelecem certos requisitos de transferência de dados para provedores de serviços em nuvem.

Nomeação de um DPO: Até que a ANPD forneça instruções mais detalhadas sobre o assunto, presume-se que toda empresa (pública ou privada) deve nomear um DPO. Essa obrigação geral se estende a todos os tipos de atividade e volumes de tratamento de dados sujeitos à LGPD (conforme estabelecido no "Guia de Orientação sobre Agentes de Tratamento e DPO" publicado pela ANPD em maio de 2021). A referida obrigação não se aplica aos agentes de tratamento de pequeno porte, que são autorizados a apenas fornecer um canal de comunicação com o titular dos dados, nos termos da Resolução CD/ANPD n° 2/2022.

Autoridade Reguladora:
Autoridade Nacional de Proteção de Dados - ANPD.

Notificação de Incidente: O controlador deve comunicar à ANPD e ao titular dos dados dentro de um prazo razoável se a violação for suscetível de resultar em risco ou dano relevante aos titulares dos dados. A própria LGPD não estabelece um prazo específico para notificar a ANPD em caso de incidentes de segurança. No entanto, de acordo com orientação publicada pela ANPD em 22 de fevereiro de 2021, a comunicação deve ser feita em até 2 (dois) dias úteis, contados a partir da data do conhecimento do incidente. Além disso, de acordo com essa orientação, a empresa ou responsável pelos dados deve avaliar internamente o incidente e apurar a natureza, a categoria e o número de titulares de dados afetados. A ANPD deve ser comunicada por meio de formulário disponível na página da ANPD (disponível aqui). Os agentes de tratamento de dados de pequeno porte poderão cumprir a obrigação de Notificação de Incidente em procedimento simplificado e com prazos flexíveis a serem disponibilizados pela ANPD nos termos da Resolução CD/ANPD N° 2/2022.

Multas: Os agentes de tratamento de dados que cometerem infrações podem estar sujeitos a sanções administrativas, de forma gradual, única, ou cumulativa, incluindo multa simples ou diária de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, até o limite de R$ 50 milhões por infração.

Atualizações legislativas: O Projeto de Lei nº 2.338/2023, que visa regulamentar os sistemas de inteligência artificial no Brasil, está em análise no Senado Federal e estabelece direitos para as pessoas afetadas por seu funcionamento, penalidades para violações, bem como informações sobre o órgão fiscalizador. A ANPD já publicou uma análise preliminar (disponível aqui) indicando os pontos de convergência e conflito entre o Projeto de Lei e a LGPD.



2. Uruguai

Lei Aplicável:
Lei nº 18.331/2008 (Ley de Proteccion de Datos Personales) e seu Decreto Regulatório No. 414/009; Lei nº 19,670/2018 (Accountability Act and Balancing of Budget Execution of the Exercise 2017) e seu Decreto Regulatório No. 64/2020.

Localização dos Dados:
Nos termos do Decreto nº 92/2014, os sistemas informáticos da Administração Central devem estar localizados em centros de dados seguros no Uruguai, exceto nos casos em que não haja risco para a entidade pública, de acordo com determinadas orientações incluídas no referido decreto. Assim, exceto nos casos em que não exista risco, as entidades públicas da Administração Central devem manter os seus dados no país. Algumas limitações adicionais para manter os dados no exterior podem aplicar-se tanto a entidades privadas como públicas, dependendo da atividade da empresa que encomenda o serviço de armazenamento (responsável pelo tratamento de dados). Por exemplo, as instituições reguladas pelo Banco Central do Uruguai (BCN) podem necessitar de autorização prévia do BCN no caso de se considerar que o armazenamento de informações se enquadra no conceito de tratamento de dados do ponto de vista da legislação bancária. Nesses casos, seria necessário analisar se o tratamento de dados no estrangeiro é ou não substancial.

Nomeação de um DPO:
Obrigatório nos seguintes casos: (i) entidades públicas estatais ou não estatais; (ii) entidades privadas ou parcialmente estatais; (iii) entidades privadas que tratam dados sensíveis como atividade principal; e (iv) entidades privadas que tratam grandes volumes de dados. O Decreto nº 64/2020 esclarece que por grande escala de dados entende-se o tratamento de dados de mais de 35.000 titulares.

Autoridade Reguladora: Unidade de Regulamentação e Controle de Dados Pessoais (*Unidad Reguladora y de Control de Datos Personales* - URCDP). É uma entidade autônoma da Agência para o Desenvolvimento do Governo Eletrônico e da Sociedade da Informação (*Agencia para el Desarrollo del Gobierno de Gestión Eletrónica y la Sociedad de la Información y del Conocimiento* - AGESIC).

Notificação de Incidente: As violações e incidentes envolvendo dados devem ser comunicados à URCDP e aos titulares dos dados. Assim que o DPO ou o responsável pelo tratamento dos dados confirmar a ocorrência de uma violação da segurança, esta deve ser notificada à URCDP no prazo de 72 horas (disponível aqui). A notificação aos titulares dos dados deve ser feita quando seus direitos tiverem sido significativamente afetados, assim que o DPO ou o controlador de dados confirmar a ocorrência de uma violação de segurança. A Lei nº 18.331/2008 exige que a notificação seja feita "logo que possível", mas não define um prazo exato para essa notificação. Após a primeira notificação ao regulador nas primeiras 72 horas após a violação, uma segunda comunicação deve ser feita pelo DPO ou pelo controlador de dados à URCDP. A segunda comunicação deve indicar todos os detalhes do que aconteceu e as medidas que foram adotadas e executadas para que essa violação/incidente tenha sido mitigada e não volte a ocorrer. A lei não estabelece um prazo para a execução da segunda comunicação.

Multas: Advertência, aviso, multas até 60.000 USD, suspensão da base de dados durante cinco dias e encerramento da base de dados.

Atualizações legislativas: O Decreto de 2020 estabeleceu novas obrigações relacionadas a notificações de violação, *Privacy by Design*, nomeações de DPO, avaliações de impacto de proteção de dados e medidas de segurança. A Lei nº 20.075/2022 entrou em vigor em 1º de janeiro de 2023 e altera o sistema de proteção de dados do Uruguai, introduzindo alterações que incluem a divulgação aos titulares dos dados, bem como os poderes da URCDP.



3. Argentina

Lei Aplicável:
Lei de Proteção de Dados Pessoais nº 25.326/2000; Decreto Regulatório de Proteção de Dados Pessoais No. 1558/2001; Diretiva de Transferência Internacional de Dados Pessoais No. E-60/2016; Resolução nº 47/2018, que dispõe sobre as medidas de segurança recomendadas para o tratamento e a conservação de dados pessoais em meios informatizados e não informatizados; Resolução nº 4/2019, que dispõe sobre as diretrizes de interpretação da Lei de Proteção de Dados Pessoais nº 25.326/2000; Resolução nº 332/2020, que regulamenta os aspectos legais e técnicos envolvidos nas auditorias realizadas pela Agência Argentina de Acesso à Informação Pública.

Localização dos Dados:
De acordo com a Lei de Proteção de Dados Pessoais nº 25.326, não há requisitos específicos. No entanto, outros regulamentos preveem requisitos de localização dos dados (por exemplo, a Comunicação "A" 6354 emitida pelo Banco Central Argentino ("BCRA") permite que as entidades financeiras subcontratem serviços de tecnologia da informação ("ITS") (por exemplo, migração para a nuvem), desde que não contenham informações de clientes e/ou do público em geral. A comunicação prevê que determinada documentação deve ser armazenada na Argentina (por exemplo, cópias originais de livros e registros contábeis e perfis de devedores de acordo com os regulamentos de gestão de crédito).

Nomeação de um DPO:
Em geral, não existe um requisito específico para nomear um responsável pela proteção de dados. Em determinadas circunstâncias, em que se aplicam normas de segurança especiais, pode ser necessário nomear um responsável pela segurança dos dados.

Autoridade Reguladora:
Agência de Acesso à Informação Pública (*Agencia de Acceso a la Información Pública*, AAIP)

Notificação de Incidente: Não é especificamente exigido pela legislação de proteção de dados, a menos que a Agência de Acesso à Informação Pública solicite especificamente informações sobre violações de dados. Por esse motivo, a pessoa responsável pelos dados deve manter registos sobre as violações de segurança, uma vez que esses registos podem ser solicitados pela Agência de Acesso à Informação Pública. A ausência de notificação de uma violação da segurança dos dados não constitui, por si só, uma violação do regime de proteção de dados, mas pode influenciar os efeitos da violação da segurança, especialmente se a ausência dessa notificação resultar em outras violações da segurança ou danos.

Multas: Advertências, suspensões, Multas de AR$ 1.000 a AR$ 100.000 (aproximadamente de USD 10 a USD 1.000 no câmbio oficial atual), encerramento ou cancelamento dos arquivos, registros ou banco de dados. Além disso, a Resolução nº 71/2016 da AAIP estabelece que, em caso de reincidência, as Multas aplicáveis podem ser aumentadas para até AR$ 5 milhões (aproximadamente USD 45.000 pela taxa de câmbio oficial atual), se a violação for qualificada como uma infração muito grave. A violação das regras de proteção de dados pode constituir um crime sujeito a penas de prisão impostas pelos tribunais penais.

Atualizações legislativas: Após uma consulta pública em setembro de 2022, a AAIP publicou, em 10 de novembro de 2022, o Projeto de Lei 87/2023 - atualmente em análise pelo Congresso Argentino - que visa atualizar a Lei e promover uma estrutura que equilibre a proteção de dados pessoais com a inovação tecnológica e o crescimento econômico. Além disso, a AAIP emitiu a Resolução 4/2019, que prevê diretrizes para a aplicação da Lei e aborda tópicos como vigilância por vídeo, tratamento automatizado de dados, consentimento e dados biométricos. Além disso, a AAIP emitiu, em 1º de dezembro de 2022, a Resolução 240/2022, que altera a Disposição nº 9, de 19 de fevereiro de 2015, sobre a Direção Nacional de Proteção de Dados Pessoais e nº 13, de 10 de março de 2015, que estabelece a classificação das infrações como leves, graves e muito graves, juntamente com a graduação das sanções. Por fim, a AAIP emitiu, em 16 de dezembro de 2022, a Resolução nº 255/2022, referente ao tratamento de dados genéticos nos termos da Lei.



4. Chile

Lei Aplicável:

Lei nº 19.628/1999 (*Ley Sobre Proteccion de La Vida Privada*), alterada pela Lei nº 21.214/2020; A Lei nº 20.575/2012 estabelece o "princípio da finalidade" para o tratamento de dados pessoais de natureza econômica, financeira, bancária ou comercial, bem como diversas regras que se aplicam ao tratamento de dados pessoais referentes a informações financeiras, econômicas, bancárias ou comerciais; a Lei nº 19.223/1993 estabelece sanções penais para determinadas condutas específicas relacionadas a furto, destruição, obstrução, modificação e acesso e divulgação ilegais de informações contidas em sistemas de tratamento de dados. No entanto, não se refere especificamente a dados pessoais. A Lei nº 20.584/2012 estabelece que todas as informações contidas em prontuários de pacientes ou documentações de tratamentos médicos são dados sensíveis, e estabelece a obrigação dos profissionais de saúde de manter os dados dos pacientes em sigilo e de observar o princípio da limitação da finalidade, além de incluir alguns casos específicos em que tais dados podem ser apresentados, parcial ou totalmente, ao titular dos dados e a outras pessoas ou entidades. Existem várias outras disposições sobre a privacidade dos dados dispersas por vários corpos legislativos, incluindo, por exemplo, o Código do Trabalho chileno, o Código Sanitário chileno, o Decreto-Lei nº 1 do Ministério da Saúde chileno, de 2006, relativo aos seguros de saúde, a Lei 19.799 relativa às assinaturas eletrônicas, o Decreto-Lei 3.500 do Ministério do Trabalho e da Segurança Social, de 1980, relativo ao sistema de pensões, o Decreto-Lei nº 3 do Ministério das Finanças chileno, de 1997, relativo aos bancos, a Compilação atualizada de normas da Comissão do Mercado Financeiro chilena, etc.

Localização dos Dados:

Os requisitos de Localização dos Dados só existem em casos muito específicos do setor bancário, em que os bancos locais autorizados são obrigados a ter cópias locais dos dados.

Nomeação de um DPO:

A lei chilena sobre a proteção de dados e privacidade, não exige a nomeação de um DPO.

Autoridade Reguladora:

Não existe nenhuma autoridade especial dedicada à supervisão de questões relacionadas com a proteção de dados no que se refere a atividades de tratamento realizadas por pessoas ou entidades privadas. A Lei 20.285/2008 sobre o acesso à informação pública prevê que o Conselho Chileno para a Transparência (Consejo para la Transparencia - CPLT, o órgão de controle para garantir o cumprimento da referida lei que prevê os direitos à transparência e ao acesso à informação da administração do Estado) deve garantir o cumprimento adequado da lei de proteção de dados pelos órgãos da administração do Estado, no entanto, o Conselho para a Transparência não tem poderes para impor multas. Desde 24 de dezembro de 2021, devido a uma disposição da recém-adotada Lei Pró-Consumidor (Lei 21.398/2021), o órgão de defesa do consumidor (Servicio Nacional del Consumidor - SERNAC) tem competência para controlar o cumprimento das disposições da lei de proteção de dados em matéria de consumo. O SERNAC não pode impor multas, mas pode instaurar e participar em processos judiciais e em processos voluntários coletivos. É a primeira vez que o tratamento de dados pessoais (dos consumidores) por parte de responsáveis privados está sujeito a um controle regulamentar. O projeto de lei prevê a criação de uma autoridade especial de proteção de dados que regula a proteção e o tratamento de dados pessoais e cria a Agência para a Proteção de Dados Pessoais (Boletim 11.144-07, consolidado com o Boletim 11.092-07). Até o momento, não existe um calendário claro para a aprovação deste projeto de lei

Notificação de Incidente:

Não há obrigação de comunicar um incidente de dados.

Multas:

Considerando que não existe uma autoridade especial de proteção de dados no Chile, as violações da proteção de dados têm de ser contestadas através de uma Ação Protetiva Constitucional com base numa alegada violação do direito constitucionalmente garantido à proteção de dados pessoais, ou através de uma ação perante os tribunais civis comuns. Além disso, a lei chilena sobre a privacidade dos dados prevê um tipo especial de ação no caso de um responsável pelo tratamento não responder atempadamente a um pedido para fazer valer os direitos da pessoa em causa ("Habeas Data"). Com a entrada em vigor da Lei Pró-Consumidor e a competência assim atribuída ao SERNAC, os consumidores podem apresentar queixas a esta autoridade alegando a violação da lei de proteção de dados. O SERNAC não pode impor Multas, mas pode instaurar e participar em processos judiciais e em processos voluntários coletivos.

Atualizações legislativas:

O Projeto de lei nº 11.144-07, que regulamenta o tratamento e a proteção de dados pessoais e cria a Autoridade Chilena de Proteção de Dados Pessoais, está sendo discutido no Senado chileno e se inspira no GDPR. Em particular, o projeto de lei alinharia o Chile aos padrões internacionais ao estabelecer direitos de acesso, retificação, cancelamento ou exclusão de dados pessoais e portabilidade de dados, além de introduzir novas bases legais para o tratamento de dados e categorias especiais de dados pessoais. O Projeto de Lei nº 14.847-06 estabelece os parâmetros sobre Segurança Cibernética e Infraestrutura de Informações Críticas que regulamenta as instituições públicas e privadas que possuem infraestrutura de informações críticas e estabelece requisitos associados a respostas a incidentes de segurança cibernética e está atualmente em discussão no Senado chileno.





5. Colômbia

Lei Aplicável:

Lei Estatutária nº 1.266/2008 regulamenta o tratamento de dados financeiros, de registos de crédito e de informações comerciais recolhidos na Colômbia ou no estrangeiro, estabelece termos gerais sobre o habeas data e estabelece princípios básicos de tratamento de dados, direitos dos titulares dos dados, obrigações do controlador de dados e regras específicas para dados financeiros. A Lei 1.266 foi alterada pela Lei nº 2,157/2021. O Decreto nº 1.377/2013 regula todo o tratamento de dados pessoais, bem como as bases de dados, e categorias especiais de dados pessoais, incluindo dados sensíveis e dados recolhidos de menores, regula a obtenção de autorização para tratar dados pessoais e os procedimentos para o tratamento de dados, e cria o Registo Nacional de Bases de Dados ("NRDB"). O Decreto nº 1.377/2013 é um ato de regulamentação secundária relacionado à Lei nº 1.581 que estabelece requisitos para os bancos de dados pessoais e domésticos no que diz respeito à autorização de uso e coleta de dados pessoais, limitações ao tratamento de dados, transferência transfronteiriça de bancos de dados e avisos de privacidade e exige que os controladores e operadores adotem uma política de privacidade e um aviso de privacidade. O Decreto nº 886/2014 e o Decreto n.º 090/2018 emitidos pelo Ministério do Comércio, Indústria e Turismo, bem como a Resolução 090 de 2018 emitida pela Superintendência da Indústria e do Comércio, regulamentam o NRDB e estabelecem prazos para o registo das bases de dados existentes na Colômbia.

Localização dos Dados:

Não existem obrigações gerais de armazenamento/localização de dados.

Nomeação de um DPO:

As empresas são obrigadas a nomear uma pessoa específica ou um grupo designado dentro da empresa para ser responsável pelas questões de dados pessoais, especificamente o tratamento dos direitos dos titulares dos dados e dos pedidos de privacidade.

Autoridade Reguladora:

De acordo com a Lei nº 1.266, existem duas autoridades diferentes em matéria de proteção e privacidade de dados. A primeira delas, que atua como autoridade geral, é a Superintendência de Indústria e Comércio (*Superintendencia de Industria y Comrecio* - SIC). A segunda autoridade é a Superintendência das Finanças (*Superintendencia Financiera de Colombia* - SOF), que atua como supervisor de instituições financeiras, agências de crédito e outras entidades que administram dados financeiros ou registros de crédito e verifica a aplicação da Lei nº 1.266. No entanto, de acordo com a Lei nº 1.581, o SIC é a autoridade máxima em matéria de proteção de dados pessoais e privacidade de dados, uma vez que tem poderes para investigar e impor sanções às empresas pela coleta, armazenamento, uso, transferência e eliminação inadequados de dados pessoais.

Notificação de Incidente:

Tanto o responsável pelo tratamento de dados como o subcontratante devem notificar o SIC em caso de violação da segurança, de risco de segurança ou de risco para a administração dos dados.

Multas:

O SIC está autorizado a investigar (como acima referido), solicitar informações, iniciar ações contra entidades privadas e impor multas até cerca de 534.000 USD, bem como ordenar ou obter a execução temporária ou permanente da empresa, entidade ou negócio. Além disso, o Código Penal da Colômbia estabelece, no artigo 269F, que quem, sem autorização, com o objetivo de obter vantagens pessoais ou para terceiros, obtiver, compilar, subtrair, oferecer, vender, trocar, enviar, comprar, interromper, divulgar, modificar ou utilizar códigos ou dados pessoais contidos em bases de dados ou plataformas semelhantes será punido com 48 a 96 meses de prisão e uma multa de aproximadamente 26.700 a 267.000 USD.

Atualizações legislativas:

Não há atualizações legislativas relevantes.



6. Mexico

Lei Aplicável: Lei federal sobre a proteção de dados pessoais detidos por entidades privadas (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), que entrou em vigor em 6 de julho de 2010. Posteriormente, o Poder Executivo também emitiu o Regulamento da Lei Federal sobre a Proteção de Dados Pessoais detidos por Partes Privadas (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), que entrou em vigor em 22 de dezembro de 2011; as Diretrizes de Aviso de Privacidade (*Guía para Elaborar el Aviso de Privacidad*), que entrou em vigor em 18 de abril de 2013; as Recomendações sobre a Segurança dos Dados Pessoais, em 30 de novembro de 2013; os Parâmetros de Auto-Regulação em matéria de dados pessoais, que entraram em vigor em 30 de maio de 2014; e a Lei Geral de Proteção de Dados Pessoais na posse de sujeitos obrigados (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), que entrou em vigor em 27 de Janeiro de 2017.

Localização dos Dados: Existem dispositivos de segurança nacional que estabelecem que as informações tratadas pelas entidades governamentais classificadas como informações de segurança nacional e informações públicas devem ser armazenadas nas instalações das entidades públicas em causa.

Nomeação de um DPO: Todos os responsáveis pelo tratamento de dados são obrigados a designar um responsável ou departamento de dados pessoais (cada um, um Responsável pela Proteção de Dados) para tratar os pedidos dos titulares de dados que exercem os seus direitos ARCO (acesso, retificação, cancelamento ou objeção) ao abrigo da lei. Os DPO são também responsáveis por supervisionar e aconselhar sobre a proteção de dados pessoais nas suas organizações.

Autoridade Reguladora: O Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) e o Ministério da Economia (*Secretaría de Economía*) são as autoridades mexicanas responsáveis pela proteção de dados.

Notificação de Incidente:
As violações de segurança que ocorram em qualquer fase do tratamento e que afetem materialmente os direitos patrimoniais ou morais da pessoa em causa devem ser prontamente comunicadas pelo responsável pelo tratamento à pessoa em causa.

Multas:
Os titulares dos dados podem fazer valer os seus direitos ARCO, quando não obtiverem resposta do responsável pelo tratamento de dados, através do INAI e, em última instância, do sistema judicial. Se for alegada qualquer violação da lei ou dos seus regulamentos, o INAI pode efetuar uma inspeção no local nas instalações do responsável pelo tratamento de dados para verificar o cumprimento da lei. As violações da Lei podem resultar em sanções pecuniárias ou prisão, incluindo as seguintes: (i) O INAI pode impor sanções monetárias no intervalo de 100 a 320.000 vezes o salário mínimo da Cidade do México (atualmente, MX $88.36, atualizado todos os anos) - as sanções podem ser aumentadas até ao dobro dos montantes acima referidos no caso de violações que envolvam dados pessoais sensíveis; (ii) pode ser imposta uma pena de prisão de três meses a três anos a qualquer pessoa autorizada a tratar dados pessoais que, com fins lucrativos, provoque uma violação da segurança que afete as bases de dados sob a sua custódia - as penas serão duplicadas se estiverem envolvidos dados pessoais sensíveis; e (iii) pena de prisão de seis meses a cinco anos para quem, com o objetivo de obter lucro ilícito, tratar dados pessoais de forma enganosa, aproveitando-se de um erro do titular dos dados ou de uma pessoa autorizada a tratar esses dados. As sanções serão agravadas para o dobro se estiverem em causa dados pessoais sensíveis. As sanções impostas pelo INAI não prejudicam qualquer outra responsabilidade civil ou penal.

Atualizações legislativas:
Não há atualizações legislativas relevantes.



VEIRANO ADVOGADOS

A Experiência Veirano conta com uma abordagem holística, multidisciplinar e orientada para negócios. A fim de suprir todas as necessidades relacionadas à LGPD, nosso time de Proteção de Dados & Privacidade desenvolveu diversos formatos de projetos, que compreendem diferentes escopos de trabalho para atender demandas específicas de cada um dos nossos clientes:

1. Adequação completa

Com a atuação de uma equipe multidisciplinar, este projeto é destinado aos clientes que possuem como objetivo identificar e avaliar todas as atividades de Tratamento realizadas pela sua empresa e, a partir disso, identificar as vulnerabilidades e estruturar um plano de ação para criação de um programa de privacidade, proteção de dados embasado em pilares jurídico, processuais, de segurança da informação e governança corporativa.

2. *DPO as a service*

Neste modelo, assumimos a função de Encarregado (DPO) em nome do cliente. Para isso, alocamos um profissional para executar as atividades de gestão e monitoramento do programa de proteção de dados e privacidade do cliente.

3. Assessoria em M&A

Criado para assessorar clientes nos processos de auditoria legal de operações de fusão e aquisição, com o propósito de identificar questões de natureza jurídica relevantes (*red-flags*) e mitigar riscos relacionados à proteção e segurança de dados pessoais da empresa-alvo.

4. LGPD Pocket

Uma assessoria "pocket" para a adequação das atividades e/ou dos produtos desenvolvidos pela empresa, independentemente de seu porte ou linha de negócios, com um número reduzido de entregáveis.

5. LGPD on Demand

O LGPD on Demand é direcionado às organizações que desejam contar com uma assessoria multidisciplinar jurídica, de segurança da informação e governança corporativa, com atuação pontual e específica, relacionada a proteção de dados pessoais.

6. LGPD Legal Helpdesk

O Helpdesk foi criado para assessorar clientes em consultas e demandas sobre proteção de dados dentro de um pacote mensal de horas, seja antes, durante ou após o processo de adequação inicial.

7. Task Force para avaliação e comunicação de incidentes de segurança (VA Cybersecurity)

Assessoria jurídica específica e multidisciplinar para aspectos relacionados à suspeita ou ocorrência de um Incidente de Segurança, de acordo com as instruções mais atualizadas da ANPD e demais leis e regulamentos aplicáveis ao tema.

8. Representação em ações administrativas e judiciais envolvendo proteção de dados

Representação de clientes em ações ou potenciais ações administrativas e/ou judiciais em matéria de proteção de dados.

9. Análise de decisões administrativas e judiciais sobre proteção de dados

Monitoramento periódico de decisões proferidas em processos judiciais e administrativos, a fim de apresentar o entendimento das autoridades e os impactos para a empresa ou setor econômico ao cliente de forma resumida.

10. Elaboração e atualização de relatório de impacto à proteção de dados

A ANPD poderá solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais (“RIPD” ou, em inglês, “DPIA”). Nossa equipe possui expertise no tema, e pode auxiliar com a elaboração e atualização do RIPD.

11. Desenvolvimento de workshops

Elaboração e aplicação de treinamentos sobre os principais conceitos de privacidade e proteção de dados para capacitação de seus colaboradores.

12. Playbook para negociação de contratos comerciais

Elaboração de *playbooks* para negociação e contratos comerciais, para facilitar e agilizar processos internos de equipes comerciais, técnicas e jurídicas.

13. Handbook para resposta aos titulares

Elaboração de materiais para auxiliar as empresas no atendimento tempestivo das solicitações dos titulares, bem como no procedimento a ser seguido pela empresa na resposta ao titular, conforme o modelo de negócio da companhia.

14. Transferência internacional de dados

Ajudamos clientes a entender o contexto da transferência internacional, adequá-la ao fundamento legal aplicável, avaliar requisitos de localização de dados, aditar contratos, elaborar e revisar acordos intragrupo e, de forma geral, responder consultas relacionadas à harmonização da legislação estrangeira com a brasileira.

15. Auditoria de privacidade e proteção de dados

Realizamos auditorias para avaliação do nível de maturidade da companhia, apresentando recomendações para mitigação de risco.

16. Elaboração e revisão de documentos pertinentes ao setor financeiro

Nosso time tem expertise em elaborar políticas de segurança em conformidade com as regulamentações específicas de segurança da informação do Banco Central, além de responder consultas sobre o tema.

Estamos à disposição caso tenha dúvidas ou precise de informações adicionais



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br



DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br



CECILIA COUTINHO
+55 11 2313-4855
cecilia.silva@veirano.com.br

Disclaimer: Este material foi atualizado pela última vez em 18 de agosto de 2023 e publicado em 18 de julho de 2023. Para informações mais atualizadas, entre em contato conosco.