

Novo Regulamento sobre aplicação da LGPD para agentes de pequeno porte

Em 28 de janeiro de 2022, dia Internacional da proteção de dados pessoais, foi publicada a Resolução CD/ANPD nº 2/2022 da Autoridade Nacional de Proteção de Dados (ANPD). A Resolução aprova o regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte e entrou em vigor na mesma data de sua publicação ("Regulamento").

O Regulamento apresenta um tratamento jurídico sobre a aplicação da LGPD para microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado que atendam aos requisitos de faturamento previstos na legislação vigente, além de pessoas naturais e entes privados sem personalidade jurídica.

Dentre as flexibilizações estabelecidas pelo Regulamento, destacam-se: (i) a possibilidade de os agentes de pequeno porte organizarem-se em entidades de representação ou procuradores para fins de negociação, mediação e conciliação de reclamações de titulares; (ii) a necessidade de elaboração e manutenção de registro das operações de tratamento de forma simplificada, a partir do modelo a ser fornecido pela ANPD; (iii) comunicação de incidentes de segurança à autoridade e aos titulares de maneira simplificada; (iv) desnecessidade de indicação de encarregado; e (v) contagem de prazo em dobro para o cumprimento das obrigações previstas na lei.



As flexibilizações trazidas pelo Regulamento não são obrigatórias, sendo que a opção por seguir as regras gerais da lei por esses agentes será considerada como atendimento às recomendações e boas práticas de prevenção e segurança para fins da aplicação de eventuais sanções administrativas pela ANPD.

Além disso, o tratamento jurídico diferenciado estabelecido no Regulamento não poderá ser aplicado a agentes que realizem tratamento de alto risco para os titulares (como o tratamento de dados em larga escala ou que possa afetar os interesses e liberdades dos titulares, utilização de tecnologias emergentes ou inovadoras, realização de vigilância ou controle de zonas acessíveis ao público, utilização de tratamentos automatizados e tratamento de dados sensíveis ou dados de crianças, adolescentes ou idosos) ou que tenham receita superior ao estabelecido na lei vigente para serem considerados como de pequeno porte (considerando o grupo econômico de fato ou de direito do qual façam parte, se aplicável).

De qualquer maneira, a ANPD poderá determinar ao agente de tratamento de pequeno porte o cumprimento das disposições dispensadas ou flexibilizadas pelo Regulamento, caso as circunstâncias do caso justificarem essa medida.

Primeira minuta das Diretrizes 01/2022 sobre o direito de acesso

Em 28 de janeiro de 2022, o Conselho Europeu de Proteção de Dados (EDPB) publicou a primeira minuta das Diretrizes 01/2022 sobre direitos dos titulares de dados, especialmente o tratamento de dados pessoais, cuja finalidade é orientar os titulares de dados e os agentes de tratamento de dados. O direito de acesso dos titulares está consagrado no artigo 8 da Carta dos Direitos Fundamentais da União Europeia e é melhor detalhado e regulamentado no artigo 15 do Regulamento Geral sobre a Proteção de Dados (GDPR).

Tais diretrizes abrangem uma série de tópicos relacionados ao direito de acesso, incluindo a análise de uma solicitação; definição da identidade do titular solicitante dos dados; avaliação do escopo do direito de acesso; orientação sobre a forma que o controlador de dados pode atender a uma solicitação; prazo para resposta das solicitações; redução adequada da coleta e do armazenamento de dados e limites ao direito de acesso.

Sobre esse último tópico, o EDPB detalha algumas limitações, como a impossibilidade de acesso aos dados pessoais quando esse direito afetar negativamente os direitos e liberdades de terceiros, como, por exemplo, segredos comerciais ou direitos autorais sobre software. Entretanto, a EDPB afirma que essas considerações sobre as limitações não devem ser uma justificativa para a recusa em fornecer todas as informações ao enviado; o controlador deve tentar conciliar os direitos conflitantes (por exemplo, removendo informações de terceiros).

Sendo assim, a minuta das diretrizes fornece esclarecimentos importantes sobre como as autoridades supervisoras da União Europeia interpretam o direito de acesso previsto no GDPR.

Declaração europeia sobre direitos digitais na era digital

O Parlamento Europeu, o Conselho Europeu e a Comissão Europeia publicaram, em 26 de janeiro de 2022, uma Declaração Conjunta sobre os direitos e princípios digitais relacionados à era digital, cujos objetivos são explicar as intenções políticas compartilhadas, reforçar os direitos relevantes no contexto da transformação digital, orientar empresas e outras entidades relevantes para o desenvolvimento e implantação de novas tecnologias e inserir as pessoas como o centro da transformação digital, reforçando a inclusão, a liberdade de escolha, a participação do espaço digital, segurança, proteção, capacitação e sustentabilidade.

Esta Declaração, em seu capítulo V, aborda temas relacionados à proteção de dados, tais como proteção e segurança do ambiente digital, privacidade e controle individual sobre os dados e a segurança no ambiente digital de crianças e adolescentes.

Nesse sentido, a Declaração estabelece que todos devem ter acesso às tecnologias, produtos e serviços digitais que sejam seguros e protegidos. Para tanto, os autores da Declaração se comprometeram a (i) proteger os interesses das todas as crianças e instituições públicas contra os crimes cibernéticos, incluindo violações de dados pessoais e ataques cibernéticos, (ii) proteger a identidade digital contra roubo ou manipulação de identidade, (iii) combater e responsabilizar aqueles que procuram prejudicar a segurança digital e a integridade do ambiente digital dos cidadãos europeus ou que promovem a violência e o ódio através de meios digitais.

Além disso, a Declaração estabelece que todos têm direito de controlar seus dados em relação a como são usados e com quem são compartilhados, bem como o direito à confidencialidade das comunicações e informações disponíveis nos dispositivos eletrônicos de seus usuários, sendo proibidas medidas ilícitas de vigilância.

Por fim, no que se refere às crianças e adolescentes, os autores da Declaração se comprometem a (i) promover um ambiente digital positivo, adequado à idade e seguro para crianças e adolescentes, (ii) proporcionar oportunidades a todas as crianças de adquirir as aptidões e competências necessárias para navegar no ambiente digital de forma ativa com segurança e fazer escolhas conscientes e informadas quando estiverem online e (iii) proteger todas as crianças contra conteúdos nocivos e ilegais, ou conteúdo envolvendo a exploração, manipulação e assédio online, bem como impedir que o espaço digital seja utilizado para cometer ou facilitar crimes.



Regulamentação do Projeto de Lei de Regulamentação de Segurança e Mídia Online (16ª ed./fev.)

Em 12 de janeiro de 2022, foi lançado o Projeto de Lei de Regulamentação de Segurança e Mídia Online (MSMR), que regulamentará emissoras e serviços de streaming online.

O MSMR estabelece, entre outras disposições, um novo órgão para regulamentar emissoras e serviços de streaming online ("Comissão de Mídia"), como o Netflix, para substituir a Autoridade de Broadcasting da Irlanda (BAI) - que atualmente regulamenta as emissoras de rádio e televisão. Sob o projeto de lei, a Comissão de Mídia terá mais poderes para impor seu cumprimento, penalizar plataformas digitais e, se necessário, bloquear serviços online, além de poder instituir e processar crimes sumários.

Além disso, o projeto de lei aborda conteúdos ilegais e também prejudiciais e abrange categorias de "danos online". Essas categorias incluem conteúdos que (i) são considerados ilegais de acordo com leis criminais irlandesas, (ii) tenham o efeito de intimidar, ameaçar, humilhar ou perseguir alguém (cyberbullying), (iii) encorajem ou fomentem distúrbios alimentares, automutilação e suicídio, e (iv) compartilhem conhecimento de métodos de automutilação ou suicídio.

Diante do exposto, fica evidente que a Comissão de Mídia se tornará um importante órgão regulador do setor de tecnologia, tanto na Irlanda quanto na União Europeia.



Acordo internacional de transferência de dados, adendo e disposições transitórias são apresentados perante o Parlamento do Reino Unido

Conforme declaração do Information Commissioner's Office (ICO) do Reino Unido, o Departamento de Cultura, Meios de Comunicação Social e Desporto (DCMS) apresentou ao Parlamento no dia 2 de fevereiro de 2022 o Acordo Internacional de Transferência de dados (IDTA), o Adendo de transferência internacional de dados às cláusulas contratuais padrão da Comissão Europeia e um documento que estabelece disposições transitórias quanto ao uso das atuais cláusulas padrão de proteção de dados para transferências internacionais.

Vale destacar que o IDTA e o Adendo são redigidos com o objetivo de ajudar as organizações a garantir que protejam corretamente os dados pessoais ao transferi-los para países de fora do Reino Unido. Nesse sentido, a aplicação de altos padrões de proteção de dados aos fluxos de dados globais é essencial para manter a confiança das pessoas nesse ecossistema.

Além disso, o IDTA e o Adendo também ajudarão a apoiar a economia digital do Reino Unido, permitindo o fluxo global de dados pessoais das pessoas, a fim de fornecer bens e serviços. O IDTA, o Adendo e as disposições transitórias foram apresentados ao Parlamento e entrarão em vigor em 21 de março de 2022.

Avanço nas leis dos Estados Unidos da América relacionadas a proteção de dados genéticos

Os Estados Unidos estão fortalecendo leis de privacidade envolvendo a proteção de dados genéticos, uma vez que é cada dia mais comum o uso de dados genéticos para realização de testes de DNA, os quais podem ser comprados online diretamente de empresas de 23andMe e Ancestry, bem como o uso de dados genéticos para realização de investigação de crimes violentos por parte das autoridades americanas.

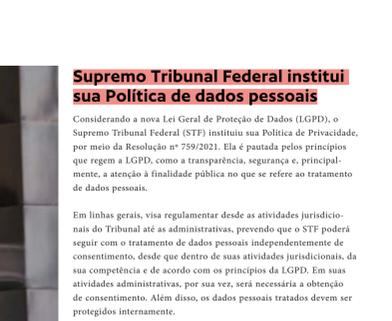
Neste sentido, o estado da Califórnia sancionou a Lei de Privacidade de Informações Genéticas (SB 41), a qual entrou em vigor em janeiro de 2022 e impõe restrições aos dados genéticos coletados por empresas de testes de DNA diretamente pelos consumidores. O SB 41, em suma: (i) exige que os titulares de dados deem consentimento expresso antes que seus dados possam ser usados para pesquisas científicas ou compartilhados com terceiros; (ii) após o devido consentimento, as empresas devem fornecer a opção para os titulares deixarem de participar de tais pesquisas a qualquer tempo; (iii) as empresas devem fornecer aos titulares, de forma clara, a opção de encerrar suas contas e eliminar seus dados de DNA do banco de dados da empresa; (iv) as empresas devem proceder à destruição da amostra biológica dentro de 30 dias após a devolução da solicitação.

Diante desse cenário, os estados de Utah e Arizona promulgaram leis semelhantes à da Califórnia, as quais abordam disposições relacionadas ao consentimento, segurança de dados, direitos dos titulares em relação aos seus dados genéticos, entre outros.

Além disso, os estados de Maryland e Montana foram os primeiros estados a aprovar leis de privacidade de dados genéticos em que as autoridades utilizam o perfil de DNA de um suspeito ou vítima anônima para construir a árvore genealógica desse indivíduo.

A lei de Montana estabelece que as autoridades obtenham um mandato de busca para visualizar dados genéticos em um banco de dados de DNA. Enquanto a lei de Maryland estabelece que, em suma, (i) os dados genéticos só podem ser utilizados para investigar assassinatos, estupros ou outros crimes que representem uma ameaça à segurança pública; (ii) para ter acesso ao banco de dados genéticos é necessária a autorização de um juiz, por escrito, bem como é imprescindível que tenham se esgotado todas as outras vias de investigação; e (iii) genealogistas deverão obter uma licença especial para trabalhar com estes dados.

Diante do exposto, ainda não está claro como será realizado o monitoramento de eventuais violações a essas leis, bem como a maneira que as empresas de testes de DNA serão responsabilizadas.



Supremo Tribunal Federal institui sua Política de dados pessoais

Considerando a nova Lei Geral de Proteção de Dados (LGPD), o Supremo Tribunal Federal (STF) instituiu sua Política de Privacidade, por meio da Resolução nº 759/2021. Ela é pautada pelos princípios que regem a LGPD, como a transparência, segurança e, principalmente, a atenção à finalidade pública no que se refere ao tratamento de dados pessoais.

Em linhas gerais, visa regulamentar desde as atividades jurisdicionais do Tribunal até as administrativas, prevendo que o STF poderá seguir com o tratamento de dados pessoais independentemente de consentimento, desde que dentro de suas atividades jurisdicionais, de sua competência e de acordo com os princípios da LGPD. Em suas atividades administrativas, por sua vez, será necessária a obtenção de consentimento. Além disso, os dados pessoais tratados devem ser protegidos internamente.

Outro ponto estabelecido se refere às informações sobre crianças e adolescentes. O tratamento destes dados deverá ser informado de forma clara e acessível a este público e a seus responsáveis legais.



Presidente do TSE afirma que não haverá imposição de sigilo a dados de doações eleitorais e eleitores que prestem serviços para campanhas políticas.

A discussão se dá em um processo no qual o TSE analisa a aplicação da LGPD (Lei Geral de Proteção de Dados) no contexto eleitoral, diante do receio de entidades de que uma determinada leitura da LGPD leve a Corte a privilegiar a proteção dos dados pessoais em detrimento da transparência, subvertendo o princípio da Lei de Acesso à Informação (LAI), segundo o qual a publicidade deve ser a regra; e a sigilo, a exceção. Na avaliação dessas organizações, isso seria um retrocesso.

O próprio ministro ressaltou, porém, que a prioridade é a transparência: "Os atuais mecanismos que estão hoje à disposição da sociedade na Justiça Eleitoral, especialmente no Tribunal Superior Eleitoral, se forem alterados, talvez sejam alterados após um longo debate com a sociedade e especialistas interessados, onde se evidencie em relação a esses dados questões como necessidade, utilidade e adequação", afirmou Fachin.

Em entrevista concedida à Folha de S.Paulo, ele ainda confirmou que priorizará a segurança no TSE e que, a despeito de os sistemas do órgão poderem ser atacados, as urnas eletrônicas são seguras e não se conectam à internet.

Empresa é condenada judicialmente a interromper o envio de mensagens publicitárias e excluir todos os dados pessoais armazenados do consumidor autor da ação

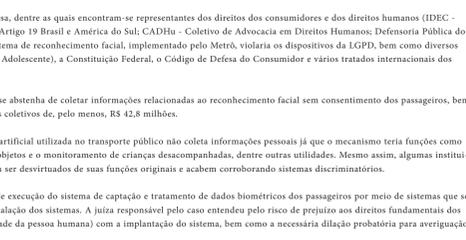
O envio semanal de propagandas de telemarketing a telefone pessoal enseja a propugnação de ação por parte do consumidor contra empresa de comércio e serviços de distribuição no foro de Ribeirão Preto. De acordo com o Autor, a empresa Ré estaria armazenando indevidamente seus dados pessoais, recusando-se a fornecê-los ou excluí-los de seu banco de dados, além de efetuar tratamento abusivo no que diz respeito à utilização para fins publicitários.

Em resposta, a empresa requerida forneceu os dados do encarregado da proteção de dados, sustentando a ausência de armazenamento ou tratamento de dados pessoais do titular, bem como que o telefone do Autor pertencia anteriormente à empresa que era sua cliente. Além disso, afirmou que a LGPD não se aplicaria às pessoas jurídicas, bem como que o nome do Autor teria sido obtido por meio de algoritmo do aplicativo de atendimento ao consumidor.

Diante destas circunstâncias, o magistrado considerou que, uma vez que a empresa Ré estava ciente da alteração da titularidade da linha, teria ela incorrido em violação aos direitos do CDC e da LGPD ao negar os pedidos de fornecimento de dados do consumidor. Ademais, reiterou que a falta de indicação do encarregado de dados no site da empresa impossibilita o recebimento de reclamações e tomada de providências por parte do titular dos dados, bem como viola o artigo 11, parágrafo 1º, da LGPD.

Assim, houve condenação ao fornecimento e exclusão de todos os dados pessoais armazenados e tratados relacionados ao consumidor, bem como à cessação do envio de mensagens publicitárias a ele, sob pena de multa diária de R\$ 500,00 (quinhentos reais). Não obstante as alegações contestadas, o pedido de indenização por danos morais não foi acolhido em razão de se ter entendido não ser o dano presunível no caso concreto.

O magistrado fundamentou a improcedência do pedido indenizatório no sentido de que, embora tenha ocorrido o tratamento não autorizado de dados, "não se tratam de dados sensíveis, não reflexos houve repasse indevido a terceiros, depreciação do titular, uso econômico indevido, limitação a direitos da personalidade (honra, integridade psicológica, etc.) ou reflexos materiais sobre outros direitos, havendo mera utilização para campanha de marketing, passível de simples cancelamento com decreto judicial" (processo nº 1007913-21.2021.8.26.0506).



Presidente do TSE afirma que não haverá imposição de sigilo a dados de doações eleitorais e eleitores que prestem serviços para campanhas políticas.

A discussão se dá em um processo no qual o TSE analisa a aplicação da LGPD (Lei Geral de Proteção de Dados) no contexto eleitoral, diante do receio de entidades de que uma determinada leitura da LGPD leve a Corte a privilegiar a proteção dos dados pessoais em detrimento da transparência, subvertendo o princípio da Lei de Acesso à Informação (LAI), segundo o qual a publicidade deve ser a regra; e a sigilo, a exceção. Na avaliação dessas organizações, isso seria um retrocesso.

O próprio ministro ressaltou, porém, que a prioridade é a transparência: "Os atuais mecanismos que estão hoje à disposição da sociedade na Justiça Eleitoral, especialmente no Tribunal Superior Eleitoral, se forem alterados, talvez sejam alterados após um longo debate com a sociedade e especialistas interessados, onde se evidencie em relação a esses dados questões como necessidade, utilidade e adequação", afirmou Fachin.

Em entrevista concedida à Folha de S.Paulo, ele ainda confirmou que priorizará a segurança no TSE e que, a despeito de os sistemas do órgão poderem ser atacados, as urnas eletrônicas são seguras e não se conectam à internet.

Juiz da Justiça do Trabalho do MS decide que uso do bafômetro em empregados viola LGPD

Um trabalhador do Mato Grosso do Sul foi demitido por justa causa após seu empregador realizar teste de bafômetro e constatar que seu teste indicava 0,078 mg de álcool por litro de ar. Ao entrar na Justiça do Trabalho, o funcionário alegou que a empresa estava infringindo a LGPD, já que o cidadão passou a ter o direito de decidir quais tipos de dados pessoais fornece e de que modo esses dados serão coletados e armazenados.

Tendo isso em vista, o juiz da 1ª Vara de Trabalho de Dourados (MS) avaliou que a empresa descumpria a LGPD ao não comunicar a finalidade e a necessidade da realização do teste, sendo esse um dado sensível, já que é relacionado à saúde do cidadão.

A empregadora ainda tentou utilizar o art. 482, "f", da CLT, que fala justamente sobre a possibilidade de demissão por justa causa em caso de embriaguez habitual ou em serviço. Porém, o juiz entendeu que a realização de exames toxicológicos apenas não dependeria de consentimento do empregado se ele fosse motorista, para fins de cumprimento do art. 168, § 6º, da CLT.

Verifica-se, assim, a importância que deve ser dada à LGPD perante a Justiça do Trabalho, que somente em 2021 contou com pelo menos 2.048 novos processos que citavam a lei nas petições iniciais.



MPF instaura investigação sobre os Acordos de Cooperação que autorizam o acesso dos bancos a dados pessoais biométricos e biográficos dos cidadãos

Após representação apresentada pelo deputado federal Carlos Veras, o Ministério Público Federal (MPF) decidiu instaurar uma investigação sobre os Acordos de Cooperação (MPE nº 16/2021 e nº 27/2021, celebrados pelo Ministério da Economia com a Federação Brasileira de Bancos (FEBRABAN) e a Associação Brasileira de Bancos (ABBC), respectivamente. Referidos acordos autorizam que bancos tenham acesso a dados pessoais biométricos e biográficos dos cidadãos armazenados na base de dados da Identificação Civil Nacional (Lei nº 14.444/2017) e da plataforma Gov.br, para fins de "Identidade Digital" e de período de um ano.

O MPF notificou a Secretaria Especial de Desburocratização, Gestão e Governo Digital, vinculada ao Ministério da Economia, para que prestasse esclarecimentos sobre: (i) em que consistem os dados fornecidos às instituições celebrantes dos acordos; (ii) se houve estudo dos riscos envolvidos no compartilhamento de tais dados e quais medidas de segurança foram tomadas para a proteção das informações compartilhadas no âmbito dos acordos, de modo a evitar vazamentos indevidos de dados, especialmente para terceiros não envolvidos nos acordos; (iii) como se dará o consentimento dos titulares dos dados ao seu compartilhamento com instituições financeiras; (iv) a finalidade e utilidade do compartilhamento de tais dados; e (v) como se dará o livre acesso, a transparência, a responsabilização e a prestação de contas dos dados compartilhados e (vi) se houve pronunciamento dos órgãos de controle sobre o mérito dos acordos.

Além disso, a Autoridade Nacional de Proteção de Dados foi acionada para prestar informações esclarecendo se emite parecer sobre os termos dos acordos de cooperação e se os documentos estariam em conformidade com a Lei Geral de Proteção de Dados (LGPD).



PROCON/MS autua empresas por estarem em desacordo com a LGPD

Empresas dos setores de e-commerce foram autuadas pelo PROCON/MS, por supostamente infringirem a Lei Geral de Proteção de Dados. Segundo os fiscais do PROCON, os sites e aplicativos delas possuem termos de uso abusivos, bem como políticas de privacidade e cookies em descumprimento com a Lei mencionada anteriormente.

Questões como a violação ao artigo 6º da LGPD por coleta de dados de registro eletrônico de dispositivos e de interação do usuário ou mesmo a coleta de dados biométricos da empresa também seriam excessivas perante as análises dos fiscais, tendo também sido constatado que não haveria exatidão e transparência quanto à exposição de dados criptografados de cookies expostos a consumidores.

Os fiscais do PROCON teriam verificado, em uma das empresas, que os seus termos de privacidade seriam pouco transparentes, confusos e possuiriam a capacidade de compartilhar dados dos consumidores que excederiam as exigências do artigo 11 da LGPD. Já outra possuiria irregularidades em seu site quanto à identificação das empresas que receberiam os dados dos consumidores.

Por fim, os fiscais do PROCON também autuaram uma empresa por supostamente incluir automaticamente os seus consumidores em programas de fidelidade de outros fornecedores, em desacordo com a legislação consumerista e, ainda, por não especificar quais são os fornecedores que receberão esses dados compartilhados.

Empresas de telecomunicações multadas pela Autoridade Grega

Dois das maiores empresas de telecomunicações da Grécia, integrantes do mesmo grupo econômico, foram sancionadas em 6 milhões e 3,2 milhões de euros por irregularidade no tratamento de dados pessoais.

A investigação se iniciou com a notificação de um incidente de segurança - vazamento de dados de chamada de assinantes - por uma das empresas. Após exame do incidente, foram reveladas diversas infrações ao Regulamento Geral sobre Proteção de Dados da Europa (GDPR), incluindo aos princípios da legalidade e transparência, devido ao fornecimento incorreto de informações aos assinantes.

Além disso, também foram constatadas irregularidades em: (i) relatórios de impacto à proteção de dados; (ii) anonimização de dados; (iii) medidas de segurança adotadas; e (iv) enquadramento das duas empresas como agentes de tratamento - controlador e operador.

Cabe destacar que, embora integrantes do mesmo grupo econômico, empresas devem garantir sua conformidade com as leis de proteção de dados separadamente. A obscuridade em termos de conformidade e o falho posicionamento com relação ao tratamento de dados desempenhado podem ser consideradas circunstâncias agravantes no cálculo de multas.

Autoridade húngara aplica multa a importador de carros por práticas ilegais de tratamento de dados

Este caso teve início depois que o Requerente teve seu carro inspecionado/revisado pelo Requerido, o qual possui uma oficina automotiva especializada, fornecendo-lhe seu endereço de e-mail. Posteriormente, o Requerente recebeu um e-mail não solicitado requisitando que fosse preenchido um questionário de satisfação em relação ao serviço prestado anteriormente e, logo após, outro e-mail solicitando que ele completasse o questionário novamente devido à ausência de resposta.

Os e-mails continham informações particulares do Requerente, mas os e-mails não foram enviados pelo Requerido, mas sim por um remetente terceiro, qual seja, um importador de automóveis. Nesse sentido, não houve o consentimento do Requerente para que fosse tratada a transferência de dados pessoais para terceiros, ao passo que ele nem mesmo foi informado sobre tal compartilhamento.

Dessa forma, após a realização de uma investigação por parte do Órgão de Fiscalização, não foi possível demonstrar como os dados tratados estão relacionados com os propósitos declarados de medição de satisfação e gerenciamento de reclamações. À vista disso, o tratamento de tais dados pessoais foi considerado ilegal segundo o disposto pelo GDPR, de modo que se ordenou a aplicação da prática de tratamento de dados utilizada, bem como uma multa foi aplicada ao Requerido.



No Brasil, a Lei Geral de Proteção de Dados (LGPD), assim como o GDPR, estabelece que os titulares dos dados possuem o direito a oposição ao tratamento de dados pessoais coletados sem a base legal do consentimento (art. 18, inciso VIII e § 2º, da LGPD). No que diz respeito ao consentimento, a LGPD deixa claro que, para ser válido, o consentimento deve ser livre, informado, inequívoco e específico, sob pena de nulidade.



Este material não pode ser reproduzido integralmente ou parcialmente sem consentimento e autorização prévios de TozziniFreire Advogados.

Este boletim é um informativo da área de Cybersecurity & Data Privacy de TozziniFreire Advogados.

SÓCIAS RESPONSÁVEIS PELO BOLETIM:

- ✉ Marcela Waksman Ejnisman
- ✉ Patrícia Helena Marta Martins
- ✉ Carla do Couto Hellu Battilana
- ✉ Bruna Borghi Tomé

Mais informações em: tozzinifreire.com.br/

Foto: Paulo Roberto/Contrasto, Tozzini Freire Advogados