

Edição 21 | 2022

cybernews.

**Tozzini
Freire.**
ADVOGADOS



**Tozzini
Freire.**

.ADVOGADOS

sumário

REALIDADE BRASILEIRA

Aprovada no Senado Medida Provisória que transforma a ANPD em autarquia de natureza especial..... 4

ANPD lança guia orientativo “Cookies e Proteção de Dados Pessoais” 4

Cartórios têm até março de 2023 para adequação às novas regras de proteção de dados.....5

Conselho Federal de Medicina (CFM) publica cartilha de orientação a médicos sobre a aplicação da LGPD 6

CNseg cria novo serviço para reporte de incidentes cibernéticos 6

ANPD publica Nota Técnica que analisa Acordo de Cooperação entre SERPRO e empresa 6

ORIENTAÇÕES GERAIS

AEPD e EDPS publicam artigo conjunto sobre equívocos relacionados a Machine Learning7

ICO/UK publica orientações sobre tecnologias de melhoria da privacidade.....7

ICO/UK publica Guia de compartilhamento de dados pessoais para estudantes universitários.....7

AVANÇOS NORMATIVOS

As autoridades de proteção de dados e privacidade do G7 discutem a proteção de dados e o fluxo de dados através das fronteiras 8

Escritório Federal de Segurança da Informação da Alemanha publica relatório sobre tecnologia na indústria automotiva 8

PODER JUDICIÁRIO

CNJ adere à LGPD na digitalização de processos 9

STF decide que os princípios e garantias que resguardam os dados pessoais devem ser observados pelos órgãos públicos quando do compartilhamento de dados 9

Criado grupo de inteligência pelo TSE para combate à violência política10

TJMG entende que não são sensíveis os dados fornecidos rotineiramente10

TJMG nega acesso irrestrito aos cadastros públicos nos sistemas conveniados ao Tribunal 11

TJSP reconhece a legalidade da divulgação de dados pessoais não sensíveis quando relacionados à atividade de proteção ao crédito 11

MINISTÉRIO PÚBLICO

MPF instaura inquérito por compartilhamento de dados de cidadãos pelo Ministério da Economia 12

DECISÕES INTERNACIONAIS

Autoridade de Proteção de Dados de Berlim impõe multa de 525 mil euros por violação relacionada ao Encarregado.....13

EDPS se manifesta sobre a violação contida no Novo Regulamento da Europol 13

///// Realidade Brasileira

Aprovada no Senado Medida Provisória que transforma a ANPD em autarquia de natureza especial

O Senado Federal aprovou, em 18 de outubro de 2022, a Medida Provisória nº 1.124/2022, que transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial.

A modificação da natureza jurídica já estava prevista na LGPD, que estipulava que ela poderia ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

Com a aprovação do Senado, o documento segue agora para publicação no Diário Oficial.

ANPD lança guia orientativo “Cookies e Proteção de Dados Pessoais”

No dia 18 de outubro de 2022, a ANPD publicou o guia orientativo “Cookies e Proteção de Dados Pessoais”.

Apesar de não ser um documento vinculante, o guia foi elaborado para orientar os agentes de tratamento sobre as boas práticas envolvendo o tema, além de traçar um panorama geral sobre o assunto.

Em suma, a ANPD:

- Reconhece a existência de outras hipóteses legais, além do consentimento e do legítimo interesse, para a coleta de dados pessoais por meio de cookies (p. 17);
- Desaconselha a utilização de banners de cookies com opções pré-selecionadas (“on by default”), sendo necessária conduta ativa da pessoa titular nesse sentido – exceção feita aos cookies necessários (p. 19); e
- Aconselha o uso de consentimento para os cookies não necessários (i.e., cookies cuja desabilitação não impede o funcionamento do site ou aplicação ou a utilização dos serviços pelo usuário) (p. 20).



Segundo a visão da ANPD, o legítimo interesse pode ser a hipótese legal mais adequada para a coleta de dados por meio de cookies necessários, uma vez que esses cookies são usados como forma de apoio e promoção das atividades do controlador e de prestação dos serviços que beneficiem a pessoa titular, bem como para cookies analíticos, em determinados contextos (p. 24).

A ANPD também reforça a questão da transparência ao titular, que pode ser efetivada por meio da elaboração e publicação de uma Política de Cookies (a qual pode ser uma seção do próprio Aviso de Privacidade) ou da disponibilização de informação diluída no banner de cookies (p. 28 e 29).

O guia ficará aberto a comentários e contribuições contínuas da sociedade. O objetivo é que o material se mantenha sempre atualizado, quando novas regulamentações e entendimentos forem estabelecidos. As sugestões poderão ser enviadas para a Ouvidoria da ANPD, por meio da [Plataforma Fala.BR](#).

A versão completa do guia pode ser consultada [aqui](#).

Cartórios têm até março de 2023 para adequação às novas regras de proteção de dados

A Corregedoria Nacional de Justiça, órgão do Conselho Nacional de Justiça (CNJ), publicou, no final do mês de agosto, o Provimento nº 134/2022, que regulamentou o processo de adequação das serventias extrajudiciais à Lei Geral de Proteção de Dados (LGPD). A expectativa do CNJ com a publicação do Provimento é a adoção de procedimentos mais transparentes no âmbito das atividades de tratamento de dados pessoais.

Entre as disposições do Provimento nº 134 há o mapeamento das atividades de tratamento – que identificará as operações de tratamento que serão realizadas, os dados pessoais tratados, sua finalidade e o prazo esperado de tratamento – e a realização de manutenções ano a ano no inventário de informações. Destaca-se que, além dos tópicos acima, o Provimento incentiva a elaboração de procedimentos eficazes para atendimento aos direitos dos titulares.

Nesse sentido, vale observar que o Provimento está diretamente relacionado à natureza e ao volume dos dados pessoais tratados pelas serventias extrajudiciais, ligados a questões como filiação, parentalidade, óbito, nascimento e diversas relações jurídicas patrimoniais, em escala consideravelmente alta.

Ademais, há, ainda, a previsão de que haja o arquivamento desse inventário de dados nos cartórios, disponibilizados em caso de solicitação do CNJ, por meio da Corregedoria, da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) ou de demais órgãos de controle.





Conselho Federal de Medicina (CFM) publica cartilha de orientação a médicos sobre a aplicação da LGPD

Com o objetivo de promover maior segurança no tratamento de dados pessoais na área de saúde, o Conselho Federal de Medicina (CFM) editou uma cartilha de orientação sobre proteção de dados pessoais aos médicos. As instituições de saúde devem visar a completa conformidade com a LGPD, uma vez que lidam com dados de saúde, ou seja, dados pessoais sensíveis e, portanto, devem ser precedidos de cautelas maiores em seu tratamento.

A cartilha traz os principais conceitos da LGPD e instruções sobre as condutas necessárias que devem ser tomadas pelos médicos para assegurar o efetivo sigilo dos dados pessoais, além de detalhar os papéis dos agentes de tratamento, com foco total na área de saúde.

Especial atenção deve ser dada ao tratamento de dados pessoais relativos à saúde, que deve se dar por meio do consentimento do titular dos dados, mas a cartilha destaca algumas hipóteses excepcionais que podem ocorrer sem a coleta do consentimento, como a manutenção do prontuário do paciente, para atender a normas que preveem a guarda do documento para fins de utilidade pública.

CNseg cria novo serviço para reporte de incidentes cibernéticos

Em setembro, a Confederação Nacional das Seguradoras (CNseg) adotou o chamado Compartilhamento de Incidentes Cibernéticos (CIC), o qual consiste em um sistema para centralizar os reportes de incidentes cibernéticos a todas as supervisionadas.

Este novo serviço possibilita às empresas seguradoras uma redução de custos operacionais para cumprir as imposições da Circular SUSEP nº 638/2021 – de alinhamento do mercado securitário às disposições da LGPD – porque seus incidentes de segurança poderão ser informados a diversas supervisionadas simultaneamente e haverá maior celeridade na realização de iniciativas para proteger os danos causados pelos incidentes.

No mais, as empresas que se associarem ao CIC terão acesso exclusivo a soluções que possibilitam aumentar a receita, otimizar e aperfeiçoar os processos de precificação, cotação, subscrição e regulação de sinistros, reduzir custos, mitigar riscos, prevenir e combater fraudes e manter-se em conformidade legal, resultando em melhoria contínua na prestação de serviços ao cliente.

ANPD publica Nota Técnica que analisa Acordo de Cooperação entre SERPRO e empresa

No dia 21 de setembro de 2022, a ANPD publicou a Nota Técnica nº 75/2022/CGF/ANPD, que analisa o possível compartilhamento de dados pessoais no âmbito do Acordo de Cooperação Técnica entre o Serviço Federal de Processamento de Dados (SERPRO) e a empresa DrumWave. Vale destacar que a DrumWave é uma empresa que exerce atividade análoga a um cartório de dados digitais, monetizando o valor dos dados de empresas e pessoas.

Nesse sentido, tendo em vista que, atualmente, não há compartilhamento de dados pessoais no contexto do referido Acordo, concluiu-se ser desnecessária a atuação da ANPD nesse momento. No entanto, caso o SERPRO, em ocasião futura, opte pelo compartilhamento de dados pessoais no âmbito do Acordo, deverá comunicar à Autoridade imediatamente.

AEPD e EDPS publicam artigo conjunto sobre equívocos relacionados a Machine Learning

A Autoridade Espanhola de Proteção de Dados (AEPD) e a Autoridade Europeia de Proteção de Dados (EDPS) publicaram conjuntamente, no dia 20 de setembro, um artigo de comentários a diversos equívocos populares relacionados a Machine Learning (ML). A publicação, disponível no website da EDPS, tem como objetivo desfazer concepções errôneas sobre os sistemas que utilizam ML e, ao mesmo tempo, ressaltar a importância da utilização de tais sistemas em conformidade com os princípios de proteção de dados.

Entre os mitos abordados, estão dizeres como “os sistemas com Machine Learning estão menos sujeitos a preconceitos humanos”; “o Machine Learning consegue prever com precisão o futuro”; e até “decisões automáticas tomadas por algoritmos com Machine Learning não podem ser explicadas”.

Em diversos mitos, a causa normalmente se relaciona com a crença errônea de que o ML estaria livre de interferência humana, o que está distante de ser realidade. A enorme maioria dos sistemas ML, atualmente, depende de humanos para a seleção inicial e habitual, catalogação, delineamento e treinamento dos dados; em todas as fases citadas, o sistema ML estaria sujeito a vieses humanos.

Nesse sentido, a preocupação crescente com o tratamento automatizado de dados, bem como com as decisões potencialmente preconceituosas tomadas por sistemas ML, é justificável; por isso a atenção das legislações de proteção de dados ao tema.

ICO/UK publica orientações sobre tecnologias de melhoria da privacidade

Em setembro de 2022, o Information Commissioner's Office (ICO) – a autoridade independente do Reino Unido responsável pela manutenção do interesse público nas questões envolvendo dados pessoais – publicou orientações sobre tecnologias de aprimoramento de privacidade (PETs) (acesse [aqui](#)).

As PETs permitem que as organizações tratem dados pessoais de forma responsável, segura, legal e colaborativa, por meio de, por exemplo, redução do grau de identidade dos indivíduos de quem os dados são processados, minimização da quantidade de dados tratados, anonimização dos dados e divisão ou controle de acesso aos dados pessoais.

Ainda que as PETs já sejam utilizadas por organizações financeiras em investigações relativas à lavagem de dinheiro e pelo setor de saúde no oferecimento de melhores serviços de saúde ao público, o uso de PETs ainda está em estágio inicial. Por esse motivo, as orientações incentivam o uso de PETs, demonstram os diferentes tipos existentes e explicam os benefícios de seu uso para a conformidade. Faltou o terceiro texto desta seção “Orientações Gerais”:

ICO/UK publica Guia de compartilhamento de dados pessoais para estudantes universitários

Em 14 de setembro de 2021, o ICO publicou um Guia Orientativo, com o intuito de orientar universidades e estudantes acerca dos cuidados necessários e boas práticas a serem seguidas no compartilhamento de dados pessoais.

Dentre as práticas indicadas, está a elaboração de uma Avaliação de Impacto de Proteção de Dados, com o objetivo de identificar antecipadamente possíveis falhas na segurança do compartilhamento de dados e auxiliar no planejamento de procedimentos de emergência a serem seguidos em caso de incidentes. Além disso, outra indicação foi implementar a execução de Acordos de Compartilhamento de Dados entre os envolvidos (universidade e estudantes), para que as informações sejam compartilhadas de maneira segura e legítima.

Por fim, outra prática recomendada é o treinamento dos funcionários da universidade acerca de suas responsabilidades, dos direitos dos titulares e dos princípios que devem ser seguidos no tratamento e compartilhamento de dados pessoais.

As autoridades de proteção de dados e privacidade do G7 discutem a proteção de dados e o fluxo de dados através das fronteiras

As autoridades de proteção de dados dos países componentes do G7 reuniram-se em Bonn, na Alemanha, no início de setembro, para elaborar estratégias conjuntas ligadas ao conceito “Livre Fluxo de Dados com Confiança”. A reunião é a segunda do tipo, demonstrando interesse intenso das economias globais na adoção de melhores práticas globais para proteção de dados.

Em termos gerais, o norte da reunião é a construção de confiança dos consumidores, assegurando padrões globais de proteção de dados para o fluxo internacional de dados.

Entre as discussões que receberam contribuições das autoridades, está a criação e manutenção de “espaços de dados internacionais”, vistos como uma abordagem emergente para o compartilhamento nacional ou internacional de dados, de maneira confiável e voluntária, dentro de organizações e setores, para apoiar a inovação no meio acadêmico, na indústria e na administração pública.



Escritório Federal de Segurança da Informação da Alemanha publica relatório sobre tecnologia na indústria automotiva

Em 19 de setembro de 2022, o Escritório Federal de Segurança da Informação da Alemanha (BSI) publicou a segunda edição do Relatório de Situação do Setor Automotivo 2021/2022, o qual analisa a segurança cibernética no setor automotivo, tanto no que diz respeito à indústria quanto aos próprios veículos.

Nessa perspectiva, tendo em vista a rápida progressão tecnológica no setor automotivo, bem como o avanço das possíveis ameaças dos mais diversos tipos de ataques cibernéticos, o documento realiza um panorama geral do cenário contemporâneo da digitalização do setor automotivo na Alemanha, de modo que objetiva aumentar a segurança cibernética no país. Dessa maneira, o Relatório fornece dicas de cuidados e recomendações que a indústria deve ter em mente no desenvolvimento dos produtos, assim como perpassa pelo gerenciamento de vulnerabilidades e outros pontos voltados para a segurança de automação e inteligência artificial.

Nos termos de uma declaração oficial do presidente do BSI, o Relatório “evidencia mais uma vez que a segurança cibernética deve ser considerada em todos os elos da cadeia de suprimentos – desde o início até o produto acabado”. Portanto, é de suma importância que as novas tecnologias necessárias para que a devida segurança seja garantida não sejam manipuláveis e que eventuais ataques cibernéticos não tenham qualquer impacto na segurança da condução dos veículos automotores.



CNJ adere à LGPD na digitalização de processos

O Conselho Nacional de Justiça (CNJ) aprovou, em outubro, a Resolução nº 469/2022, com o objetivo de estabelecer novas normas e diretrizes para a digitalização de documentos judiciais e administrativos e para a gestão de documentos em processos já digitalizados, à exceção do Supremo Tribunal Federal (STF).

Incorporando a LGPD, a Resolução tem, entre seus propósitos, garantir e preservar a integridade, autenticidade, confidencialidade e preservação dos documentos judiciais e administrativos.

O texto da Resolução detalha as políticas de gestão documental, procurando que os Órgãos Públicos se adequem à LGPD e consigam preservar e garantir a qualidade dos arquivos judiciais e administrativos. Dessa forma, os órgãos judiciários deverão promover a distinção dos documentos que devem ser descartados daqueles que devem ser preservados, acessados e difundidos, fazendo parte do patrimônio do Poder Judiciário brasileiro.

A presidente da Comissão Permanente de Gestão Documental e Memória do Poder Judiciário do CNJ, Salise Monteiro Sancho-tene, trouxe importantes dados em relação à digitalização de processos judiciais no Brasil. Destacando o grande crescimento de percentual de processos novos exclusivamente eletrônicos, que chegaram em 96,6% em 2020, enfatizou também que há ainda uma quantidade considerável de processos que tramitam em meio físico e estão para ser digitalizados.

STF decide que os princípios e garantias que resguardam os dados pessoais devem ser observados pelos órgãos públicos quando do compartilhamento de dados

Em 15 de setembro, encerrou-se o julgamento referente à utilização dos parâmetros estabelecidos pela Lei Geral de Proteção de Dados Pessoais nas normas do Decreto nº 10.046/2019, que trata do compartilhamento de dados pessoais entre órgãos federais e institui o Cadastro Base do Cidadão, bem como o Comitê Central de Governança de Dados.

O Supremo Tribunal Federal (STF) decidiu, por maioria de votos, que o Decreto que criou o Cadastro Base do Cidadão – que reúne informações sobre os cidadãos existentes em diferentes órgãos da administração pública – deve ser interpretado conforme a Constituição, seguindo-se uma série de princípios que foram fixados pelo relator Gilmar Mendes.

Dentre os princípios, tem-se que o compartilhamento de dados deve se limitar ao atendimento da finalidade informada e que devem ser cumpridas as garantias e os procedimentos estabelecidos na Lei Geral de Proteção de Dados no que se refere ao setor público.

Criado grupo de inteligência pelo TSE para combate à violência política

Após reunião do atual presidente do TSE, ministro Alexandre de Moraes, com os comandantes-gerais das polícias militares, em 24 de julho deste ano, para discutir a segurança das eleições, foi definida a implantação de um núcleo de inteligência para combater a violência nas eleições.

O núcleo foi criado no início de setembro, por meio da publicação da Portaria TSE nº 833, com o objetivo de coletar e processar dados de segurança pública durante o período eleitoral, para combater a violência política.

O grupo será formado pelo ministro Alexandre de Moraes e por demais membros do TSE, como o juiz auxiliar Marco Antonio Martin Vargas, que ficará responsável pela Secretaria-Executiva. Já da parte do CNCG (Conselho Nacional de Comandantes-Gerais das Polícias Militares), integrarão o grupo alguns tenentes-coronéis. Os membros atuarão em conjunto durante todo o período eleitoral para evitar e identificar casos de violência política.

A Portaria TSE nº 833 não estabelece expressamente como será a forma de atuação, mas apenas dispõe que esta será definida pelo presidente do Tribunal, ministro Alexandre de Moraes, na primeira reunião de seus integrantes.



TJMG entende que não são sensíveis os dados fornecidos rotineiramente

A 18ª Câmara Cível do TJMG negou provimento à apelação interposta por consumidora que pleiteava a reforma de sentença para que o réu Banco FICSA fosse condenado ao pagamento de danos morais por supostas violações à LGPD.

A Apelante havia ajuizado a ação em face do banco para, além da mencionada indenização, obter pagamento em dobro do valor cobrado referente a empréstimo consignado não contratado, tendo sido a sentença procedente apenas quanto à restituição em dobro do valor.

Embora fosse incontroversa a contratação de empréstimo consignado sem anuência da Apelante, o Tribunal entendeu que a consumidora não comprovou os requisitos ensejadores de ressarcimento quanto aos danos morais. Como principal fundamento, o Tribunal destacou que a LGPD estabelece que apenas a utilização de dados caracterizados como “sensíveis” pode ensejar o direito à indenização. No entanto, segundo o Tribunal, os dados pessoais não se configuram como “sensíveis” quando são passíveis de acesso por terceiros, e fornecidos rotineiramente em estabelecimentos comerciais ou em aplicativos móveis.

Além disso, o Tribunal também entendeu que não restou comprovado o nexo causal entre o suposto vazamento de dados e a contratação de empréstimo.

Em que pese o entendimento do Tribunal, destacamos que ele se mostra contrário à devida interpretação da lei, uma vez que não há disposição na LGPD que limite a responsabilidade civil por violação da lei de proteção de dados pessoais apenas quando envolver os dados ditos sensíveis.

TJMG nega acesso irrestrito aos cadastros públicos nos sistemas conveniados ao Tribunal

Na ação originária, a parte autora tem buscado perante o Juízo a adoção de diligências para a obtenção de dados pessoais dos requeridos, com a finalidade de localizar quais seriam os herdeiros dos proprietários (já falecidos) dos imóveis objeto da ação de usucapião.

Para além dos pedidos comumente deferidos (como diligências frente ao “SISBajud, Renajud, Infojud”), a parte autora requereu também o acesso a informações contidas em cadastros públicos nos sistemas conveniados ao Tribunal com a finalidade de identificar e localizar os herdeiros para figurarem no polo passivo, mas a 21ª Câmara Cível Especializada entendeu pela necessidade de prévia individualização mínima das pessoas em quem se pretende fazer recair a pesquisa.

Segundo o Tribunal, a pretensão de acesso irrestrito às bases de dados pessoais ofende a LGPD, além do postulado constitucional de proteção à privacidade, tendo em vista que ausente a demonstração da finalidade legítima e proporcional de tal tratamento. No entendimento exposto no acórdão “*O dado pessoal poderá estar publicamente acessível, mas nem por isso poderá ser genericamente capturado para qualquer outro objetivo ou finalidade, por parte de terceiros*”.

Assim, o Tribunal assentou ser ônus da parte interessada a indicação específica das pessoas cujos dados pessoais se busca nos sistemas conveniados ao Poder Judiciário, a fim de que sejam analisados o propósito e o contexto do pedido de obtenção dos dados pessoais.

TJSP reconhece a legalidade da divulgação de dados pessoais não sensíveis quando relacionados à atividade de proteção ao crédito

O Tribunal de Justiça do Estado de São Paulo firmou entendimento de que dados cadastrais que não forem sensíveis não necessitam de autorização de seu titular ou tampouco de comunicação prévia para a sua divulgação por parte de empresa com atuação no âmbito das relações de proteção ao crédito.

Na ação de origem, o Autor buscava a condenação da empresa Serasa S/A na abstenção de divulgação de seus dados (como “*renda mensal, endereço e telefones pessoais*”) e no pagamento de indenização em razão da suposta ausência de autorização para a comercialização de seus dados pessoais. Afirma o Autor que seria inaceitável que a empresa tornasse disponível em banco de dados informações em relação às quais não teria ocorrido comunicação prévia.

Ao manter a sentença de improcedência da ação, o Tribunal considerou que não houve, por parte do Autor da ação, demonstração de que teria ocorrido suposta divulgação indevida de seus dados e, ainda, que as informações divulgadas e discutidas nos autos se mostram necessárias para subsidiar a análise de crédito.

O referido entendimento confirma a posição da 2ª Câmara de Direito Privado – já exposta em outras oportunidades – quanto à legalidade da divulgação de dados no contexto de subsidiar análise de crédito por empresas atuantes no setor





MPF instaura inquérito por compartilhamento de dados de cidadãos pelo Ministério da Economia

O Ministério Público Federal instaurou inquérito civil para apurar o acordo de cooperação firmado entre o Ministério da Economia, a Federação dos Bancos Brasileiros e a Associação Brasileira de Bancos, que autorizaram mais de 100 instituições financeiras a acessar dados biométricos e dados pessoais de cidadãos armazenados no banco de dados nacional de cidadania (chamado “*Identificação Civil Nacional*”) e na plataforma Gov.br por um período de um ano, para fins de identidade digital.

O Ministério da Economia informou à imprensa que, até o momento, os atos foram apreciados pela ANPD e pelo TCU, que se manifestaram pela legalidade destes e arquivamento dos processos.

Autoridade de Proteção de Dados de Berlim impõe multa de 525 mil euros por violação relacionada ao Encarregado

A Autoridade de Proteção de Dados e Liberdade de Informação de Berlim condenou, em 22 de setembro, um varejista situado na cidade de Berlim, Alemanha, pelo não cumprimento dos requisitos relacionados ao Encarregado presentes no Regulamento Geral Europeu sobre a Proteção de Dados (GDPR).

A decisão da autoridade de Berlim ocorreu, no entanto, após um primeiro aviso ao varejista, realizado em 2021. Além da primeira orientação, o órgão de proteção de dados berlinense conduziu uma investigação que levou ao seu convencimento sobre a potencial infração ao artigo 38 (6) do GDPR. O referido artigo trata sobre as tarefas e deveres a que o DPO poderá ser submetido pelo controlador ou operador, exigindo que essas tarefas não resultem em um conflito de interesses.

A multa, contudo, pelo relatório da autoridade de proteção de dados de Berlim, ainda não é judicialmente vinculativa, de maneira que o Encarregado ainda poderá pleitear a sua anulação.



EDPS se manifesta sobre a violação contida no Novo Regulamento da Europol

Em 16 de setembro de 2022, a EDPS – a autoridade de controle da proteção de dados das instituições, órgãos, escritórios e agências da UE – requereu a anulação, pelo Tribunal de Justiça da União Europeia (TJUE), de duas disposições do novo Regulamento da Agência da União Europeia para a Cooperação Policial (Europol), que está em vigor desde 28 de junho de 2022, porque elas impactam as atividades de tratamento de dados pessoais realizadas no passado pela Europol.

Estes dois dispositivos (artigos 74a e 74b do Regulamento) legalizam retroativamente a prática da Europol de processar grandes volumes de dados pessoais que foram transmitidos à Europol para verificar se o indivíduo tem alguma ligação estabelecida com atividade criminosa. Caso essa relação não fosse constatada, esses dados deveriam ser apagados o mais tardar até 04 de janeiro de 2023, conforme instruído pela EDPS. As novas disposições do regulamento da Europol permitem que a Europol continue a tratar os dados que ainda não foram apagados, apesar da ordem da EDPS.

Por esse motivo, estas disposições ameaçam tanto a segurança jurídica dos dados pessoais das pessoas quanto a independência da EDPS.



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
- ✉ Luiza Sato
- ✉ Sofia Kilmar

Mais informações em:
tozzinifreire.com.br/

**Tozzini
Freire.**
ADVOGADOS

**Tozzini
Freire.**
ADVOGADOS

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