

Bom dia,

Bem-vindo(a) à newsletter #135 da DPO Consulting, o nosso meio informativo sobre o mundo da Privacidade, Proteção de Dados, *Compliance* e Inteligência Artificial.

Contacte-nos e leve a sua conformidade a outro nível.

Proteja os Dados. Reforce a Confiança. Simplifique a Conformidade.

CNPD lança canal prioritário para reforçar proteção de crianças e jovens



Participações sobre acesso indevido a dados de menores, conteúdos sensíveis e publicidade direcionada passam a assumir caráter urgente

A Comissão Nacional de Proteção de Dados (CNPD) disponibilizou, desde 15 de setembro, um novo Canal Prioritário destinado a reforçar a proteção dos dados pessoais de crianças e jovens no ambiente digital. O canal permite apresentar participações ou queixas com caráter urgente sempre que estejam em causa situações de acesso indevido a dados de menores, recolha ou divulgação não consentida de imagem ou som com conteúdo sensível ou de violência, ou

publicidade direcionada a menores.

O Canal Prioritário pode ser utilizado diretamente por crianças e jovens, mas também por qualquer cidadão que detete a partilha ilícita deste tipo de conteúdos. A iniciativa integra a Ação Estratégica n.º 3 do Plano Plurianual de Atividades da CNPD para 2024-2026 e procura reforçar a capacidade de resposta da autoridade perante situações que possam afetar particularmente os direitos e a privacidade dos menores.

A criação deste mecanismo surge num contexto de crescente exposição de crianças e jovens no ambiente digital e deverá continuar a ser acompanhada por novas ações da CNPD no próximo ciclo estratégico. Para as organizações que tratam dados de menores, o lançamento do Canal constitui também um alerta para a necessidade de reforçar medidas de proteção, avaliar os riscos associados aos tratamentos e assegurar especial atenção à divulgação de imagens, utilização de dados para publicidade e segurança dos dados pessoais de crianças e jovens.

Saiba mais

Informação clínica pertence ao utente: ERS reforça direito de acesso aos dados de saúde



Clínicas não podem recusar, dificultar ou condicionar o acesso dos utentes à sua informação clínica

A Entidade Reguladora da Saúde (ERS) veio reforçar que a informação de saúde é propriedade do próprio utente e que os prestadores de cuidados de saúde são apenas os seus depositários. O alerta surge na sequência de situações em que

clínicas terão recusado ou condicionado o acesso dos utentes aos seus processos clínicos. A ERS recorda que o direito de acesso abrange a consulta, a obtenção de cópia e a possibilidade de solicitar a retificação de informação inexata ou incompleta.

A posição da ERS encontra fundamento na Lei de Bases da Saúde e na Lei n.º 12/2005, que estabelecem que a informação de saúde pertence à pessoa a quem respeita. Os prestadores devem assegurar que a informação é devidamente armazenada e protegida, garantindo o acesso aos próprios utentes ou a quem estes autorizem. O acesso só pode ser recusado em circunstâncias excecionais, nomeadamente quando seja demonstrado que a consulta da informação pode prejudicar gravemente a saúde do utente.

Para as organizações de saúde, o alerta é particularmente relevante: ser depositário da informação clínica implica um dever de conservação, segurança e disponibilização, mas não confere propriedade sobre os dados.

O acesso à informação de saúde deve ser assegurado sem condicionamentos indevidos, incluindo a exigência de pagamento prévio de valores em dívida. Em matéria de proteção de dados, a ERS recorda ainda que, perante uma violação de dados pessoais, o utente pode apresentar uma reclamação junto da CNPD.

Saiba mais

Revolut alvo de ciberataque: hackers exigem resgate de três milhões de dólares



Ataque expõe dados de clientes e coloca novamente em evidência os riscos associados à segurança das instituições financeiras digitais

A Revolut foi alvo de um ciberataque que terá permitido aos atacantes aceder a informação de clientes, tendo posteriormente exigido um resgate de três milhões de dólares. O incidente coloca em evidência a exposição crescente das

instituições financeiras digitais a ataques direcionados e a importância de mecanismos robustos de prevenção, deteção e resposta a incidentes de segurança.

O caso é particularmente relevante do ponto de vista da proteção de dados, uma vez que um ciberataque desta natureza pode envolver o acesso não autorizado a dados pessoais de clientes. Para as organizações, um incidente de segurança implica não apenas avaliar a extensão do acesso e os dados afetados, mas também determinar se existe uma violação de dados pessoais suscetível de desencadear as obrigações previstas no RGPD, incluindo a eventual notificação à autoridade de controlo no prazo de 72 horas.

O incidente reforça ainda a importância de uma abordagem integrada entre **cibersegurança e proteção de dados**, desde a implementação de medidas técnicas e organizativas adequadas até à existência de procedimentos de resposta a incidentes, avaliação de riscos e comunicação. Num contexto de ataques cada vez mais direcionados, a capacidade de limitar rapidamente o acesso indevido e demonstrar uma resposta adequada é determinante para reduzir o impacto sobre os titulares dos dados e sobre a própria organização.

Saiba mais

Conselho da Europa lança metodologia para detetar discriminação causada por IA



Nova ferramenta permite avaliar, de forma estruturada, se sistemas algorítmicos contribuíram para resultados discriminatórios

O Conselho da Europa publicou uma nova metodologia europeia para apoiar organismos de igualdade e outras entidades na identificação de situações em que sistemas de Inteligência Artificial (IA) possam ter contribuído para práticas discriminatórias. A ferramenta apresenta uma abordagem passo a passo que permite identificar o sistema algorítmico envolvido, recolher a informação

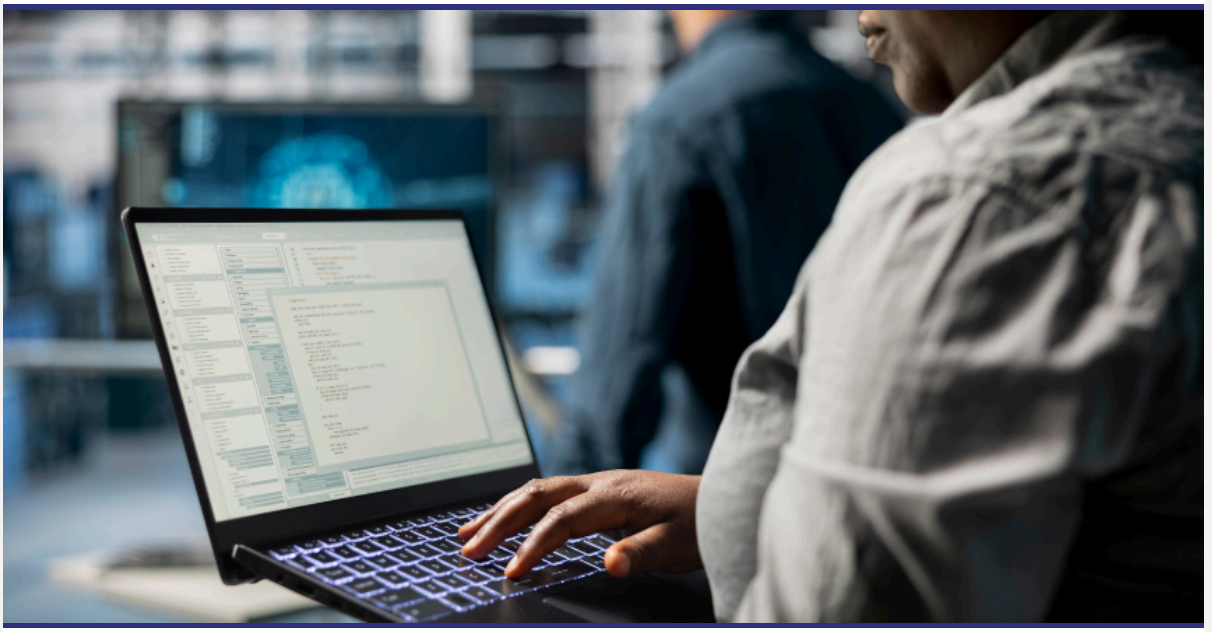
necessária e avaliar o caso do ponto de vista jurídico e técnico.

A metodologia resulta de um projeto de dois anos, cofinanciado pela União Europeia e desenvolvido pelo Conselho da Europa em cooperação com a Comissão Europeia. O projeto envolveu organismos de igualdade da Bélgica, Finlândia e Portugal, incluindo a Comissão para a Cidadania e a Igualdade de Género (CIG), e procurou desenvolver ferramentas para responder aos desafios colocados pela utilização de IA nas administrações públicas.

A publicação permite ainda identificar possíveis medidas de reparação quando seja confirmada uma situação de discriminação. Para as organizações, representa mais um passo na concretização dos princípios de igualdade, não discriminação e proteção dos direitos fundamentais no desenvolvimento e utilização de sistemas de IA, reforçando a necessidade de avaliar os impactos dos sistemas algorítmicos ao longo do seu ciclo de vida. A metodologia está já disponível, incluindo em português.

Saiba mais

Elsa Veloso alerta: PME portuguesas continuam expostas aos riscos de cibersegurança



CEO da DPO Consulting analisa os desafios das pequenas e médias empresas num contexto de crescente ameaça cibernética

A Elsa Veloso, CEO da DPO Consulting, foi destaque na *PME Magazine* numa análise dedicada ao panorama da cibersegurança em Portugal. Apesar da evolução positiva do país nesta área, a realidade das pequenas e médias empresas continua marcada por uma exposição significativa a ciberataques, num contexto de crescente sofisticação das ameaças e de maior dependência de sistemas e serviços digitais.

A análise evidencia os desafios que as PME enfrentam na prevenção e resposta a incidentes, nomeadamente ao nível dos recursos, do investimento e da capacidade de implementar medidas de proteção adequadas. Neste contexto, a cibersegurança deve ser encarada não apenas como uma questão tecnológica, mas como uma componente essencial da gestão do risco e da proteção da informação.

Para Elsa Veloso, o reforço da resiliência das organizações exige uma abordagem preventiva e estruturada, que articule cibersegurança, proteção de dados e conformidade regulatória. A intervenção da CEO da DPO Consulting reforça, assim, a importância de preparar as organizações para um cenário em que a capacidade de prevenir, detetar e responder a incidentes é cada vez mais determinante.

Saiba mais

AI no recrutamento: Bruxelas procura contributos das empresas sobre sistemas de alto risco



Comissão Europeia prepara orientações para clarificar quando as ferramentas de IA utilizadas no emprego devem ser classificadas como sistemas de risco elevado

A Comissão Europeia está a recolher contributos de empresas e outras partes interessadas para definir com maior clareza quando um sistema de Inteligência Artificial deve ser classificado como de risco elevado ao abrigo do AI Act. Entre os casos abrangidos estão os sistemas utilizados no recrutamento e seleção de trabalhadores, área em que a utilização de IA pode ter um impacto significativo

nos direitos fundamentais.

As orientações procuram ajudar fornecedores, responsáveis pela implantação e autoridades de fiscalização a determinar se um sistema se enquadra nas categorias de alto risco previstas no Regulamento, através de critérios e exemplos práticos. No domínio do emprego, estão abrangidas utilizações de IA que podem, por exemplo, influenciar processos de recrutamento, seleção ou avaliação de trabalhadores. A Comissão pretende garantir uma aplicação mais uniforme das regras em toda a União Europeia.

Para as organizações, a discussão é particularmente relevante porque a classificação como sistema de alto risco implica um conjunto reforçado de requisitos de conformidade. Na sequência do acordo político sobre o AI Omnibus, as regras aplicáveis aos sistemas de IA de alto risco utilizados no emprego deverão aplicar-se a partir de 2 de dezembro de 2027, permitindo às organizações preparar os seus processos, avaliar os sistemas utilizados e clarificar responsabilidades antes da aplicação das novas exigências.

Saiba mais

Partilhe, querendo, a newsletter da DPO Consulting.

Ficamos ao dispor para qualquer esclarecimento que haja por conveniente e voltamos ao contacto na próxima newsletter, com mais novidades e informações de relevo.

Até breve.
Elsa Veloso
CEO da DPO Consulting

DPO Consulting
Avenida da República, nº 18 3º - 1050-191 Lisboa
Rua Eugénio de Castro, 370 – H185 4100-225 Porto

Contacte-nos
A DPO Consulting tratará os seus dados pessoais, nos termos da sua Política de Privacidade cuja leitura recomendamos.

Pretendo deixar de receber as newsletters DPO Consulting.
unsubscribe