

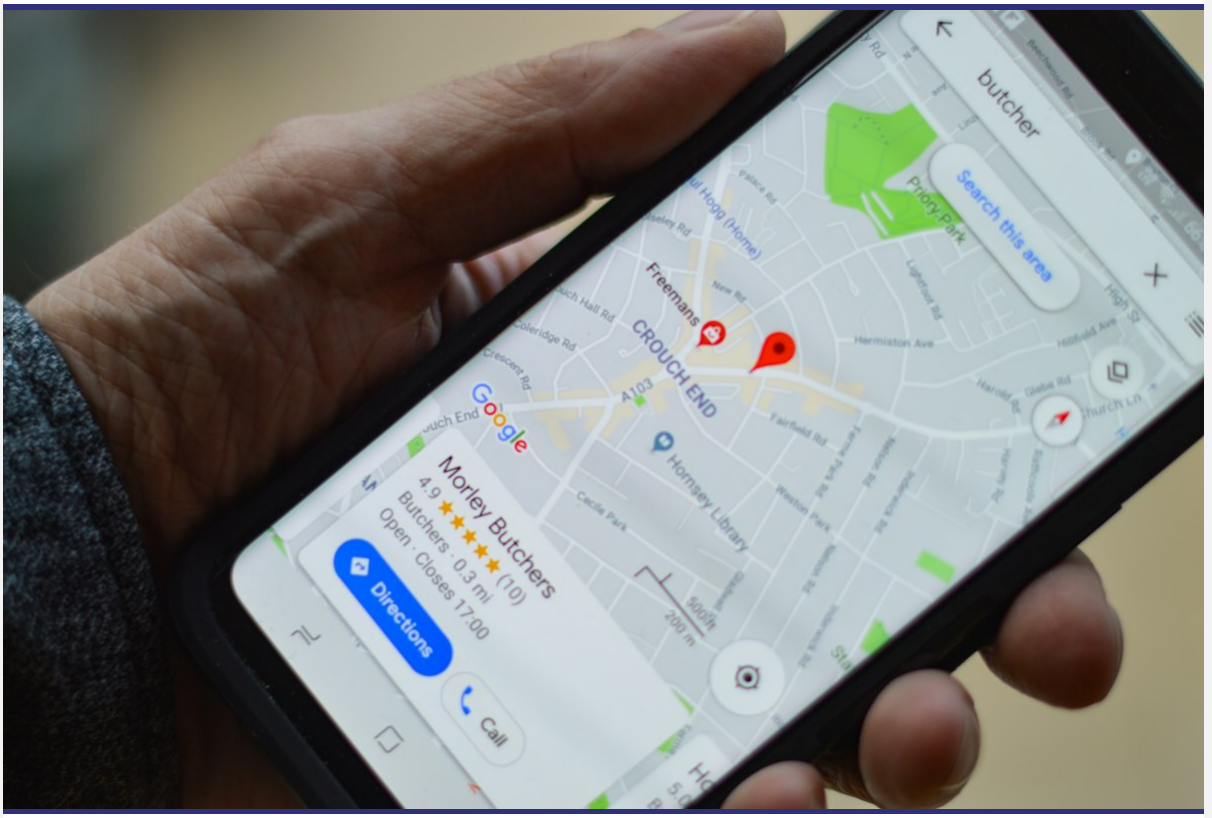
Bom dia,

Bem-vindo(a) à newsletter #137 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.

Google multada em 403 milhões de euros por tratamento de dados de localização



A autoridade irlandesa concluiu que a empresa violou o RGPD entre 2018 e 2020 na forma como recolheu, utilizou e conservou dados de localização. É a quarta maior coima de sempre aplicada pela DPC.

A Comissão de Proteção de Dados da Irlanda (DPC) anunciou, a 21 de setembro, uma coima de 403 milhões de euros à Google por violações do Regulamento Geral sobre a Proteção de Dados (RGPD) no tratamento de dados de localização. A decisão encerra um inquérito aberto em fevereiro de 2020, na sequência de queixas de várias organizações europeias de defesa do consumidor, e incide sobre o período entre maio de 2018 e fevereiro de 2020.

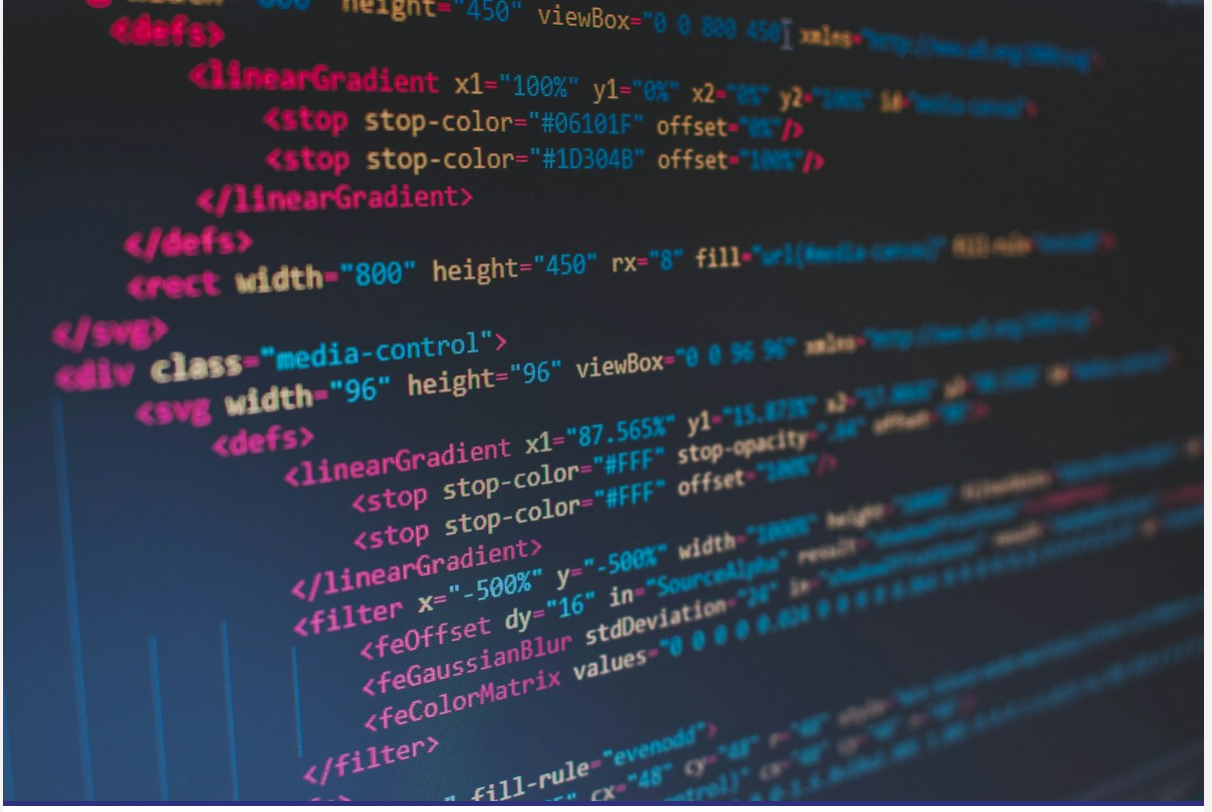
Em causa estão três funcionalidades: Atividade na Web e em Apps, Histórico de Localização e Precisão da Localização. A DPC concluiu que a empresa não respeitou os princípios da licitude e da lealdade e que conservou dados de localização durante mais tempo do que o necessário. Segundo a autoridade, os utilizadores podiam não saber que a sua localização era usada para direcionar publicidade ou inferir os seus interesses. Além da coima, a Google tem seis meses para pôr os tratamentos em conformidade. O texto integral da decisão ainda não foi publicado.

Porque importa

Os dados de localização não integram, por si só, as categorias especiais do artigo 9.º do RGPD, mas podem revelar rotinas e permitir inferências sobre aspetos íntimos da vida privada, como a frequência de locais de culto ou de unidades de saúde. A sua recolha exige um fundamento de licitude adequado a cada finalidade, informação clara e prazos de conservação justificados. As organizações que recolhem localização através de aplicações ou serviços digitais devem verificar se as finalidades estão bem definidas, se o consentimento, quando é esse o fundamento, é livre, específico e informado, se a desativação de uma definição interrompe efetivamente a recolha e se os prazos respeitam o princípio da limitação da conservação (artigo 5.º, n.º 1, alínea e), do RGPD). O acesso à informação no equipamento do utilizador está ainda sujeito às regras da Lei n.º 41/2004 (ePrivacy).

Saiba mais

Ataque a prestador informático expõe dados ligados às secretas portuguesas



Foi comprometido o servidor de testes da empresa que desenvolveu os sites públicos do SIRP, do SIS e do SIED. O caso expõe os riscos da cadeia de fornecimento e do uso de dados reais em ambientes de desenvolvimento.

Um acervo de cerca de 120 GB, alegadamente relacionado com o Sistema de Informações da República Portuguesa (SIRP), foi posto à venda num fórum de cibercrime no início de outubro. Em esclarecimento à Lusa, a 8 de outubro, o SIRP confirmou que foram obtidos dados não classificados através de um ataque ao servidor de desenvolvimento de um prestador contratado em 2025 para desenhar os sites públicos do SIRP, do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED).
O SIRP garante que não houve intrusão nas suas infraestruturas nem nos centros de dados do SIS e do SIED, e que os servidores dos sites públicos estão totalmente separados dos sistemas operacionais. No seu caso, estarão em causa elementos de um conjunto limitado de candidaturas, que o prestador terá transferido para uma instância sob a sua responsabilidade. O acervo poderá incluir também informação de dezenas de entidades públicas e privadas que recorreram ao mesmo prestador. Segundo o SIRP, foram adotadas medidas de mitigação e os factos foram participados à Procuradoria-Geral da República.

Porque importa

O elo mais fraco está muitas vezes fora da organização. Dados pessoais reais, como candidaturas, não deveriam estar em ambientes de teste. Quando isso for indispensável, devem ser anonimizados ou pseudonimizados, em linha com os princípios da minimização e da proteção de dados desde a conceção (artigos 5.º e 25.º do RGPD). O artigo 28.º exige que só se recorra a subcontratantes com garantias suficientes, com contrato adequado, direito de auditoria e devolução ou eliminação dos dados no fim do serviço.
Em caso de violação de dados, o subcontratante deve informar o responsável pelo tratamento sem demora injustificada. Cabe a cada responsável avaliar a notificação à CNPD no prazo de 72 horas e, se houver risco elevado, a

comunicação aos titulares (artigos 33.º e 34.º). As entidades abrangidas pelo regime jurídico da cibersegurança que transpõe a Diretiva NIS2 devem avaliar também os seus deveres de notificação de incidentes.

Saiba mais

Dez anos depois, o RGPD entra na fase da responsabilidade



Um artigo de opinião publicado no TEK Notícias defende que a maturidade em proteção de dados se mede nas decisões do dia a dia, e não apenas na documentação.

Aprovado em abril de 2016 e aplicável desde 25 de maio de 2018, o RGPD completa este ano uma década desde a sua adoção. Num artigo de opinião publicado no TEK Notícias, Elsa Veloso, CEO da DPO Consulting, faz o balanço deste percurso.

O regulamento não criou o direito à proteção de dados, já consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e no artigo 35.º da Constituição. Deu-lhe, no entanto, instrumentos de aplicação efetiva: regras harmonizadas, direitos reforçados para os titulares e coimas com efeito dissuasor. Com isso, os dados pessoais passaram a estar no centro da relação entre empresas, cidadãos e Estado.

O artigo sustenta que a conformidade não se esgota em políticas, procedimentos e registos. O princípio da responsabilidade (artigo 5.º, n.º 2, e artigo 24.º do RGPD) obriga as organizações a demonstrar que cumprem. Esse cumprimento vê-se nas decisões concretas: a escolha de fornecedores, a conceção de produtos, a gestão de incidentes e a adoção de ferramentas de inteligência artificial.

Para a próxima década, o desafio apontado é integrar a proteção de dados na estratégia e nos processos das organizações, tratando a privacidade como fator de confiança, de gestão do risco e de sustentabilidade da inovação. A tarefa torna-se mais exigente com a aplicação do AI Act e do novo quadro de cibersegurança.

Saiba mais

ChatGPT passa a ter marca de água invisível na União Europeia



A OpenAI vai marcar os textos gerados pelo ChatGPT e pelo Codex para cumprir as regras de transparência do AI Act. A própria empresa admite que a tecnologia tem limites.

A OpenAI anunciou, a 5 de outubro, que vai incorporar uma marca de água invisível nos textos gerados pelo ChatGPT e pelo Codex na União Europeia. A medida será aplicada de forma gradual, nas semanas seguintes, a utilizadores elegíveis de todos os planos. Fora da UE, a marcação não será ativada por predefinição, mas os clientes da API em todo o mundo podem ativá-la opcionalmente em modelos selecionados.
A iniciativa responde ao artigo 50.º, n.º 2, do Regulamento Europeu da Inteligência Artificial (AI Act), aplicável desde 2 de agosto de 2026. Esta norma obriga os fornecedores de sistemas de IA que geram conteúdo sintético a marcar os resultados num formato legível por máquina e detetável como artificial. A OpenAI, a Anthropic, a Google, a Meta e a Microsoft estão entre as empresas que aderiram ao código de práticas europeu sobre conteúdos gerados por IA.

Como funciona e quais os limites

A tecnologia, designada textGrain, não acrescenta nenhum símbolo visível. Em vez disso, introduz um padrão estatístico na escolha das palavras, que pode ser reconhecido por uma ferramenta de deteção. A OpenAI reconhece que textos curtos, editados ou traduzidos são mais difíceis de detetar e que a ausência de marca de água não prova autoria humana. A marca também não identifica o utilizador nem a conversa. O acesso ao detetor está sujeito a candidatura.

O que muda para as organizações

A obrigação de marcação recai sobre os fornecedores dos sistemas, não sobre quem os utiliza. Os responsáveis pela implantação têm, porém, deveres próprios. Ao abrigo do artigo 50.º, n.º 4, devem divulgar os conteúdos manipulados do tipo *deepfake* e os textos gerados por IA publicados para informar o público sobre matérias de interesse público, salvo quando houver revisão humana e alguém assumir a responsabilidade editorial. Aplica-se ainda, desde fevereiro de 2025, o dever de assegurar literacia em IA (artigo 4.º). As organizações que desenvolvem soluções próprias sobre modelos de terceiros e as colocam no mercado em seu nome devem confirmar se não passam, elas próprias, a ser consideradas fornecedoras.

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