Proteção de Dados

28 Janeiro 2026

Da conformidade à confiança: o futuro da proteção de dados na Europa

Celebra-se hoje, 28 de janeiro, o Dia Europeu da Proteção de Dados. Neste dia, refletimos sobre os desafios **para o ano de 2026** e a evolução da Proteção de Dados na Europa.

O panorama europeu da privacidade evoluiu de um modelo centrado no mero cumprimento legal para um modelo assente na confiança, no qual empresas e autoridades partilham um compromisso comum: **proteger os dados pessoais de forma ética, transparente e responsável**.

A evolução da proteção de dados: da conformidade à confiança

Durante anos, o foco das organizações centrou-se, em matéria de proteção de dados pessoais, na conformidade formal com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados ou RGPD).

Contudo, a realidade atual demonstra que **a conformidade, por si só, não é suficiente**. O verdadeiro valor da proteção de dados reside **na construção de relações de confiança pelas empresas** junto de clientes, parceiros e cidadãos em geral, demonstrando que a privacidade não é apenas uma obrigação legal, mas **uma prioridade estratégica de boa governação**.

Neste contexto, **assumem particular relevância três áreas fundamentais, interligadas entre si**, para o futuro da proteção de dados na União Europeia (UE):

1. O Pacote Omnibus Digital, que propõe **simplificações**, mantendo elevados níveis de proteção através de uma abordagem baseada no risco, na proporcionalidade e na eficácia da proteção. Além deste pacote, estão previstas para 2026 novas iniciativas legislativas, como o Regulamento das Redes Digitais (DNA) e o Regulamento da Justiça Digital (DFA), as quais poderão criar **deveres adicionais para as empresas europeias**;
2. A **Inteligência Artificial (IA)**, que amplia a **complexidade do tratamento** de dados pessoais e exige novas salvaguardas;
3. As **transferências de dados para os Estados Unidos (EUA)**, um tema crítico face aos desafios jurídicos persistentes e à necessidade de assegurar que os dados transferidos beneficiam de um **nível de proteção essencialmente equivalente ao exigido na Europa**.

Estes temas são especialmente relevantes porque moldam o futuro da privacidade digital e o modo como **as empresas podem crescer, inovar e gerar confiança num ambiente digital seguro**.

O Omnibus Digital e a reconfiguração do quadro jurídico europeu para o digital e a proteção de dados pessoais

O pacote Omnibus, em particular a mais recente proposta de **Omnibus Digital**, apresentada pela Comissão Europeia no dia 19 de novembro de 2025, representa uma alteração relevante na forma como a União Europeia encara a aplicação das normas de proteção de dados pessoais: **menos centrada numa lógica uniforme e excessivamente formalista e mais orientada para a proporcionalidade, a avaliação do risco e a eficácia material da proteção dos dados pessoais**.

Com esta iniciativa, pretende-se ultrapassar a dispersão normativa existente e aproximar os vários regimes europeus, criando um enquadramento legal mais articulado e funcional que permita às organizações navegar com maior clareza e previsibilidade pelas exigências em matéria de proteção de dados, privacidade, cibersegurança e IA.

A iniciativa traduz-se num conjunto articulado de propostas de alteração a vários instrumentos centrais do direito digital europeu - nomeadamente ao RGPD, ao Regulamento da IA[1], à Diretiva ePrivacy[2], ao Regulamento dos Dados[3] e à Diretiva NIS2[4] - **visando uma maior coerência sistémica e operacional entre regimes que atualmente coexistem de forma algo fragmentada**.

No que respeita ao âmbito da Proteção de Dados, prevê-se, essencialmente:

- A **simplificação da aplicação do RGPD e a extensão à nova categoria empresarial Small Mid-Caps (SMC) de algumas medidas de atenuação** já previstas para as Pequenas e Médias Empresas (PME), incluindo ao nível de certas obrigações administrativas e a **adaptação de determinadas normas**;
- **A revisão das regras respeitantes aos cookies e ao acesso aos dispositivos dos utilizadores**, com o objetivo de **simplificar a experiência digital mediante a eliminação de ações desnecessárias**, sem prejuízo do **reforço de um controlo efetivo e informado por parte dos titulares dos dados**;
- **A criação de um portal centralizado a nível da UE para matérias de cibersegurança e comunicação de violações de dados**, substituindo os atuais múltiplos canais de reporte e promovendo a **simplificação, maior eficiência, uniformidade e previsibilidade na notificação de incidentes e violações e respetiva resposta**;

[1] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento da IA).
[2] Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas).
[3] Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828 (Regulamento dos Dados).
[4] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2).

- **A reorganização e consolidação do regime jurídico dos dados, nomeadamente, do Regulamento dos Dados** – em vigor desde janeiro de 2024 –, integrando disposições atualmente dispersas por outros instrumentos, como o Regulamento da Governação de Dados[5], suprimindo normas consideradas desatualizadas, redundantes ou de reduzida utilidade prática, bem como introduzindo, por exemplo, isenções de aplicação de algumas das suas disposições para as PME e as SMC;
- **A clarificação do enquadramento jurídico aplicável à utilização de dados pessoais no desenvolvimento e na implementação de soluções tecnológicas**, reduzindo encargos desproporcionais para as organizações; e
- **A melhoria do acesso aos dados**, enquanto motor essencial da inovação, clarificando o **enquadramento jurídico da utilização de dados pessoais para o treino de modelos de Inteligência Artificial**, com vista a facilitar o acesso a novos conjuntos de dados de elevada qualidade e a reforçar o potencial global de inovação das empresas em toda a União Europeia.

Estas medidas têm como objetivo não apenas **facilitar a conformidade e reduzir encargos administrativos**, mas também **incentivar o desenvolvimento de soluções tecnológicas**, sem comprometer os elevados padrões europeus de proteção de dados.

Em suma, o Omnibus Digital procura tornar a **proteção de dados mais inteligível, exequível e orientada para a confiança, transformando o cumprimento das normas no âmbito da legislação digital e de proteção de dados pessoais**, de um simples custo burocrático num verdadeiro fator de competitividade e credibilidade no mercado europeu. Resta, contudo, observar quais das propostas serão efetivamente aprovadas e como serão operacionalizadas na prática.

[5] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados).

Importa sublinhar que a simplificação prevista não implica desresponsabilização. O Omnibus Digital visa reduzir a burocracia excessiva, mantendo, contudo, a substância da proteção. Pelo contrário, reforça uma abordagem baseada na avaliação do risco, em linha com a filosofia original do RGPD: as obrigações devem ser proporcionais, mas sempre suficientes para assegurar uma proteção efetiva dos dados pessoais.

As propostas legislativas do Omnibus Digital deverão agora ser aprovadas pelo Conselho e pelo Parlamento Europeu após as negociações em trílogo, antes da sua entrada em vigor.

Além do Omnibus Digital, a Comissão apresentou, na semana passada, a proposta do DNA e, espera-se que apresente no final do ano, a proposta do DFA, as quais introduzem regras sobre interligação de redes, publicidade personalizada e UX (*User Experience*) em plataformas digitais, com o objetivo de reforçar a proteção do consumidor. No mesmo âmbito, têm sido debatidos o controlo de chats privados para combater o abuso sexual de crianças e o sistema de pagamentos "euro digital", entre outras medidas relevantes no âmbito da cibersegurança e da privacidade.

Todo este contexto poderá **impor às empresas europeias deveres e responsabilidades adicionais**, tornando **imperativa a revisão e reestruturação dos seus procedimentos internos**, de forma a garantir **conformidade, eficiência e competitividade** num cenário regulatório e tecnológico em rápida evolução.

Inteligência Artificial e os desafios para este ano

A crescente expansão da inteligência artificial tem suscitado desafios inéditos no domínio da proteção da privacidade. Com efeito, os sistemas de IA assentam, em larga medida, no **tratamento de volumes significativos de dados**, o que pode, nomeadamente, colidir com princípios estruturantes da proteção de dados pessoais, tais como os princípios da minimização dos dados, da limitação das finalidades, da exatidão e da responsabilidade (*accountability*).

A União Europeia procurou responder a esta realidade, em especial, através do Regulamento da IA.

O referido Regulamento entrou em vigor em 1 de agosto de 2024, com algumas disposições aplicáveis já em 2025. Segundo o seu artigo 113.º, tornar-se-á plenamente aplicável a 2 de agosto de 2026, enquanto a aplicação às categorias de sistemas de IA abrangidas pela legislação europeia de harmonização da segurança dos produtos está prevista para 2 de agosto de 2027 (artigo 6.º, n.º 1, e Anexo I do Regulamento da IA).

O Omnibus Digital, já mencionado, integra uma Proposta de Regulamento destinada a alterar o Regulamento da IA e prevê o **adiamento destes prazos de aplicação**. Em concreto, propõe-se uma prorrogação de até 6 meses relativamente às obrigações aplicáveis aos sistemas de IA de risco elevado (artigo 6.º, n.º 2 e Anexo III) e de até 12 meses para os sistemas de IA abrangidos pela legislação de harmonização da UE em matéria de segurança dos produtos (artigo 6.º, n.º 1 e Anexo I), sem que as novas datas possam ultrapassar 2 de dezembro de 2027 e 2 de agosto de 2028, respetivamente.

Relativamente aos prestadores de sistemas de IA generativa colocados no mercado antes de 2 de agosto de 2026, é proposto um prazo adicional de seis meses para o cumprimento das obrigações previstas no artigo 50.º, n.º 2, do Regulamento da IA, designadamente no que respeita à marcação de conteúdos gerados ou manipulados artificialmente e à inclusão de sinais legíveis por máquina.

Estas prorrogações têm como objetivos permitir a **definição e adoção atempadas de normas técnicas pelos organismos europeus competentes** e evitar **distorções de concorrência entre operadores estabelecidos e novos participantes no mercado.** Paralelamente, prevê-se **uma simplificação geral das regras de IA**, destinada a **facilitar a sua aplicação progressiva, reforçar a segurança jurídica e reduzir os encargos de conformidade**, especialmente para **PME e SMC**.

A reforma justifica-se pela necessidade de garantir uma aplicação uniforme do Regulamento da IA, apoiada no desenvolvimento das normas técnicas, na disponibilização de orientações interpretativas e na criação de autoridades nacionais responsáveis pela supervisão do cumprimento.

A Proposta introduz também uma **nova exceção em matéria de proteção de dados pessoais**, permitindo que prestadores e responsáveis por sistemas de IA de risco elevado realizem, de forma

excecional, o tratamento de categorias especiais de dados pessoais (nos termos do RGPD), desde que cumpram salvaguardas rigorosas, incluindo medidas para deteção e mitigação de *bias*.

Apesar da potencial simplificação das normas e a prorrogação parcial da sua aplicação poderem aliviar a carga administrativa das empresas, o interregno até à eventual aprovação cria um vazio normativo que aumenta a exposição a riscos cibernéticos — os quais, no ano de 2025, cresceram exponencialmente não apenas em quantidade, mas também em complexidade, prevendo-se um novo aumento em 2026 — e deixando os titulares de dados pessoais potencialmente desprotegidos. Assim, uma das questões centrais para 2026 continua a ser **conciliar o impulso à inovação em IA com a preservação dos direitos e valores digitais que estruturam a política europeia de dados**.

Por fim, importa referir que, **a nível nacional**, o Governo português apresentou recentemente a **Agenda Nacional de IA**, prevendo medidas como a criação de uma **plataforma de soluções de IA para PME**, destinada a facilitar a implementação desta tecnologia no tecido empresarial, bem como outras iniciativas, nomeadamente no âmbito da **investigação e desenvolvimento em IA**.

Transferências de dados UE-EUA: perspetivas e riscos para 2026

As transferências de dados pessoais da União Europeia para os EUA continuam a ser um tema sensível da proteção de dados pessoais.

A jurisprudência europeia, designadamente o acórdão *Schrems II*, evidenciou que o cumprimento meramente formal de cláusulas contratuais não é suficiente, sendo necessário assegurar que os dados pessoais beneficiam de um nível de proteção essencialmente equivalente ao exigido pelo Direito da União.

Em 2025, o **Tribunal Geral da União Europeia** indeferiu o recurso de anulação da decisão da Comissão Europeia de 2023 relativa à adequação do **Data Privacy Framework (DPF)**, confirmando que, naquele momento, os Estados Unidos asseguravam um nível de proteção de dados pessoais essencialmente

equivalente ao exigido pelo Direito da União. Esta decisão pode ser entendida como uma validação, ainda que provisória, das transferências de dados pessoais entre a União Europeia e os Estados Unidos ao abrigo do artigo 45.º do RGPD.

Atualmente, milhares de empresas norte-americanas encontram-se certificadas ao abrigo do DPF, permitindo que as empresas europeias continuem a basear as suas transferências transatlânticas de dados pessoais para os EUA no DPF, o que contribui para mitigar a incerteza no curto prazo e evitar, para já, disrupções significativas nos fluxos internacionais de dados.

Não obstante, a estabilidade deste enquadramento jurídico não pode ser tida como garantida.

Desde logo, subsiste a possibilidade de uma nova impugnação judicial, potencialmente de maior alcance, suscetível de voltar a colocar em causa a compatibilidade do regime norte-americano com os padrões europeus de proteção de dados.

Acresce que os desenvolvimentos recentes nos EUA levantam riscos e questões adicionais quanto à proteção de dados pessoais, inclusivamente:

- **Retaliações contra a UE**: advertências sobre possíveis sanções se a regulamentação digital europeia for considerada "discriminatória" para empresas americanas, incluindo críticas ao **RGPD**, ao **Regulamento dos Serviços Digitais (DSA)**[6] e ao **Regulamento dos Mercados Digitais (DMA)**[7];
- **Retirada de organismos internacionais**: saída dos EUA de fóruns de cibersegurança, comprometendo a cooperação em matéria de proteção de dados;
- **Risco para fornecedores de *cloud***: determinadas ordens executivas podem colocar em causa o uso de fornecedores norte-americanos de serviços de computação em nuvem

[6] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais).
[7] Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais).

por empresas e organismos da UE devido ao acesso ampliado do governo dos EUA aos dados.

Os desafios centrais permanecem: a necessidade de conciliar interesses políticos divergentes, assegurar a competitividade das empresas europeias, definir prioridades regulatórias e gerir as tensões transatlânticas, atendendo a que a introdução de novas regras da UE pode gerar efeitos inesperados em diversos setores da economia.

Assim, apesar da aparente estabilidade do DPF, **a atual incerteza política e jurídica nos Estados Unidos obriga empresas e autoridades europeias a prepararem-se para eventuais alterações do panorama atual**, impondo-se a manutenção de uma avaliação contínua do risco e de uma atuação responsável, atento o potencial de alteração da legislação e das práticas norte-americanas.

No essencial, as modificações que possam vir a ocorrer neste âmbito, implicam para as empresas europeias:

- **Rever contratos e mecanismos de transferência**;
- **Implementar medidas adicionais de proteção**, como encriptação e anonimização;
- **Garantir documentação e avaliação de riscos** sempre que os dados saiam da UE.

Conclusão: perspetivas para 2026

À medida que avançarmos no ano 2026, a proteção de dados na Europa enfrentará desafios tecnológicos, geopolíticos e regulatórios, evoluindo, ao que tudo indica, para um modelo centrado na confiança, responsabilidade e transparência.

O foco das empresas terá, tendencialmente, de evoluir do mero cumprimento da lei para a construção de relações sólidas com clientes e parceiros, promovendo um ecossistema digital seguro, confiável e favorável à sua atividade empresarial.

O ano de 2026 será, assim, antecipa-se, marcado pela implementação gradual do Omnibus Digital, o qual simplificará e tornará mais exequível a legislação existente, enquanto, por um lado, o DNA, o DFA e outras iniciativas legislativas poderão introduzir novos deveres para as empresas em áreas como a interligação de redes, publicidade, UX, chats privados e pagamentos digitais. Paralelamente, a **IA** continuará a desafiar o enquadramento regulatório e exigir salvaguardas rigorosas, enquanto as **transferências de dados para os EUA** manterão riscos e exigirão avaliação contínua de conformidade.

Neste contexto, as organizações que adotam uma abordagem proativa — assente em avaliação de risco, inovação responsável e proteção efetiva de dados — não se limitam a cumprir a lei. Transformam a privacidade num **fator estratégico de sustentabilidade governativa e competitividade no mercado, fortalecendo a reputação da marca, consolidando a confiança de clientes e parceiros e criando novas oportunidades de inovação segura**.

No Dia Europeu da Proteção de Dados celebramos, mais do que regras e regulamentos, este compromisso coletivo com **um futuro digital seguro, ético e confiável**, onde os dados pessoais são valorizados e protegidos.

Para as empresas, isto significa que colocar a proteção de dados entre as suas prioridades estratégicas não é apenas uma obrigação legal, mas uma vantagem competitiva real no mercado europeu, que reforça a respetiva reputação ao assegurar que os cidadãos sentem que os seus dados pessoais são respeitados.

Este artigo foi preparado pela equipa de Proteção de Dados da GPA (Paula Alegria Martins, Associada Coordenadora |Matilde Pereira de Jesus, Advogada Estagiária).

Contacto:

gpa@gpasa.pt