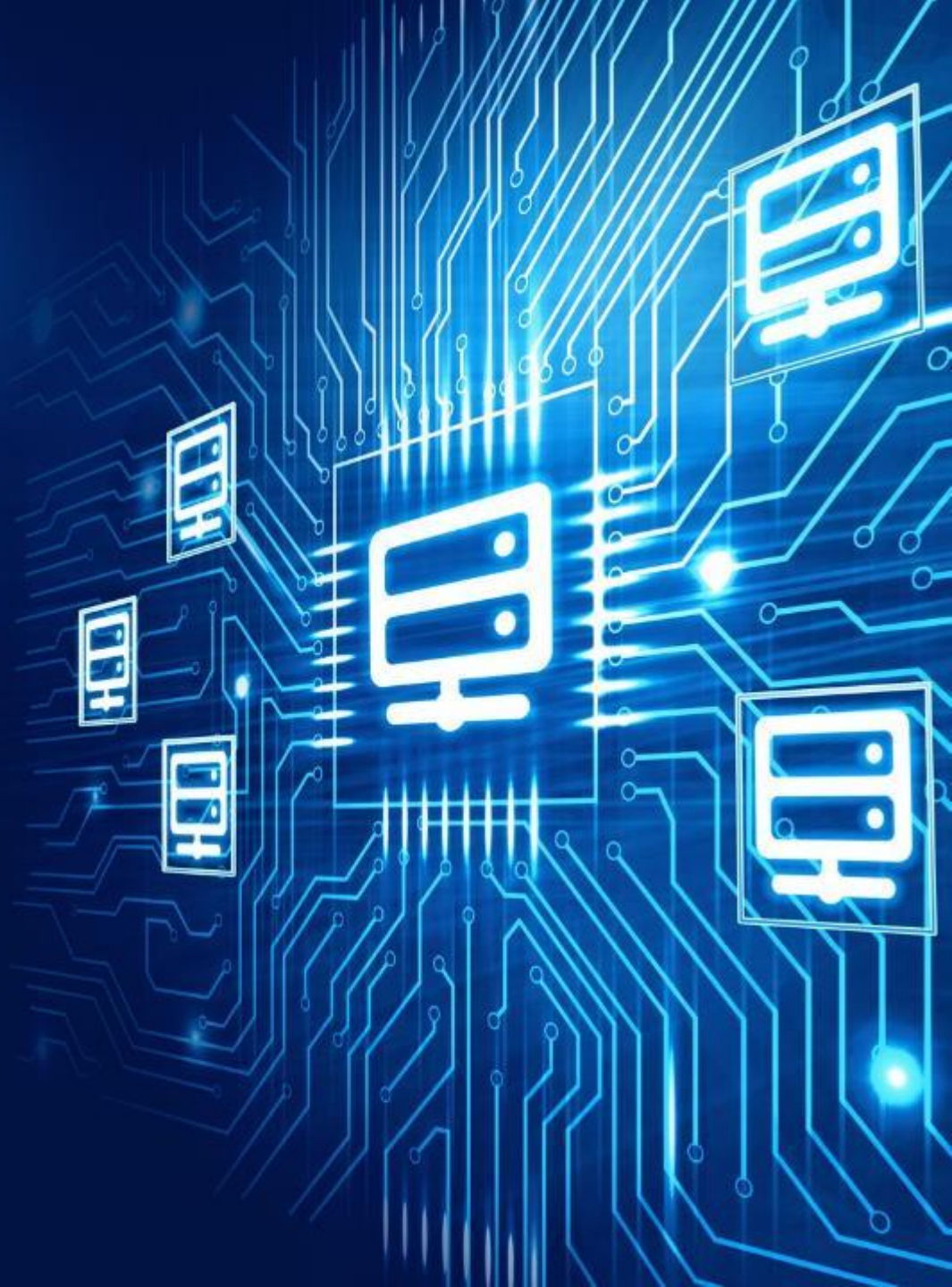
PI, DADOS E TECNOLOGIA

Panorama Jurídico em revista:
Retrospetiva 2024 e Perspetivas para 2025

Portugal



CUATRECASAS

Janeiro de 2025

Índice

Editorial

1. Inteligência Artificial

2. Propriedade Intelectual

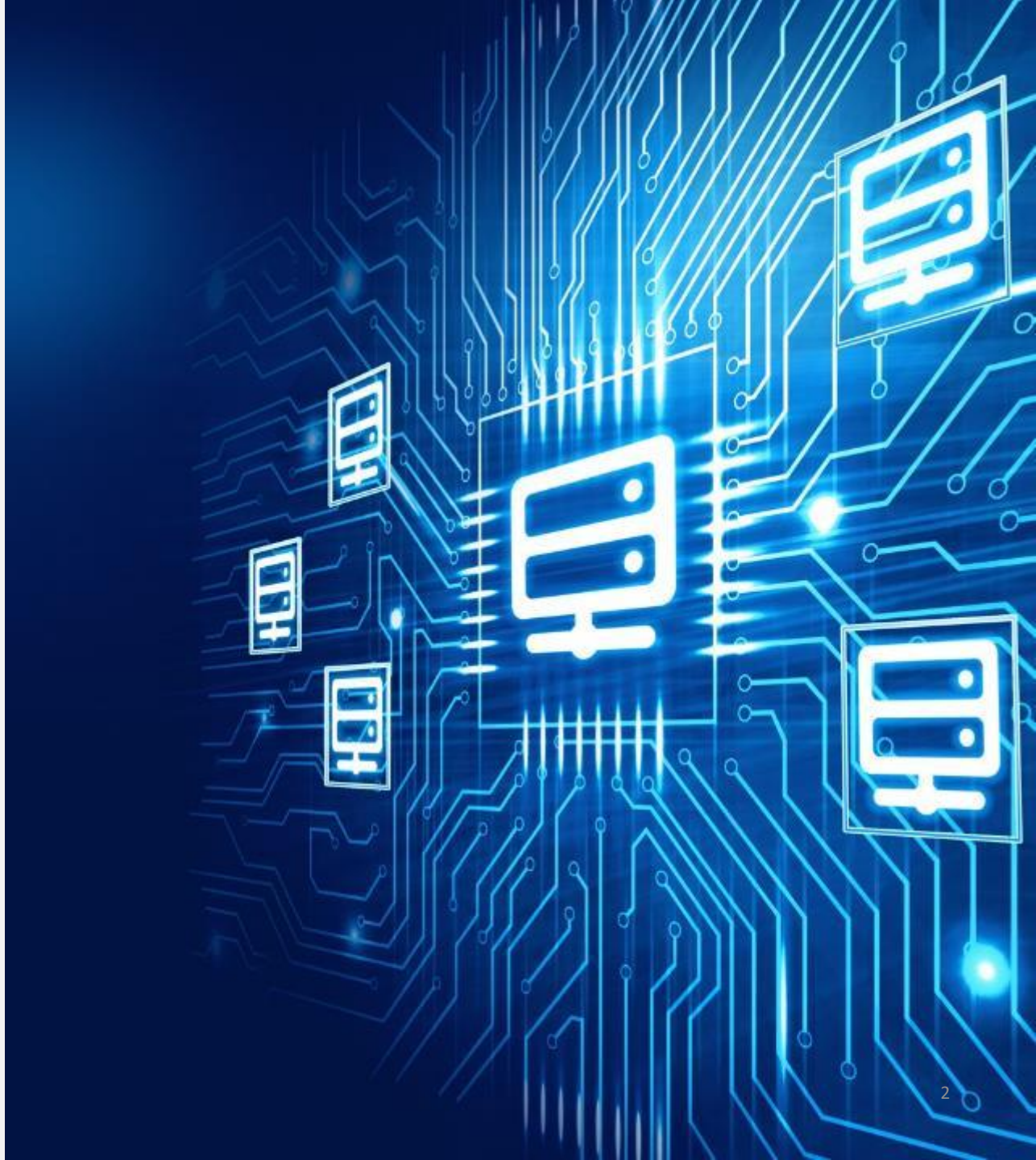
3. Privacidade e Proteção de Dados

4. Telecomunicações e Tecnologia

5. Cibersegurança

6. Publicidade e Consumo

Conclusão



Editorial

O ano de 2024 foi um marco de transformação e adaptação nas grandes áreas de negócios, especialmente nas que envolvem tecnologias emergentes e regulamentações complexas, estando **a Inteligência Artificial**, a **Cibersegurança**, a **Privacidade e Proteção de Dados**, a **Propriedade Intelectual**, a **Publicidade** e o **Consumo** e as **Telecomunicações** no centro de importantes mudanças legislativas e operacionais.

A União Europeia, com o objetivo de garantir um **desenvolvimento seguro, ético e sustentável**, está a implementar novos quadros legais e diretrizes que visam equilibrar inovação tecnológica com a proteção dos direitos fundamentais dos cidadãos.

Nesta publicação destacamos de forma não exaustiva as principais tendências e alterações regulatórias que marcaram 2024 e antecipamos já algumas novidades que 2025 trará e que prometem moldar o futuro das referidas áreas, com foco na importância da adaptação das empresas às novas exigências jurídicas e tecnológicas que se avizinham.

Legal Framework

	Inteligência Artificial	Propriedade Intelectual	Privacidade e Proteção de Dados	Telecomunicações e Tecnologia	Cibersegurança	Publicidade e Consumo
LEGISLAÇÃO EM VIGOR DESDE 2024	Regulamento da Inteligência Artificial (AI Act)	Novo Pacote Legislativo Europeu para Desenhos ou Modelos	Lei do Acesso aos Metadados	Regulamento relativo à Liberdade dos Meios de Comunicação Social	Regulamentos Delegados Suplementares ao Regulamento DORA Regras de aplicação da Diretiva NIS2 Regulamento da Ciber-Resiliência	Regulamento de Serviços Digitais Diretiva sobre responsabilidade por produtos defeituosos Regulamento para a Conceção de Produtos Sustentáveis Diretiva da Transição Ecológica dos Produtos Diretiva para a Promoção de Reparação de Bens
LEGISLAÇÃO EM RADAR	Diretiva da Responsabilidade IA		Regulamento relativo ao Espaço Europeu de Dados de Saúde, Regras Processuais relativas ao RGPD		Transposição da Diretiva NIS2 Regulamento sobre Cibersolidariedade	Transposição da Diretiva para a Promoção de Reparação de Bens, Transposição da Diretiva da Capacitação dos Consumidores para a Transição Ecológica dos Produtos

Inteligência Artificial

Com a entrada em vigor do **Regulamento da IA** ("AI Act") e a criação do ***European Artificial Intelligence Office***, a Europa reforçou a sua posição como líder global na regulação de sistemas de IA. Além disso, o **Tratado sobre Inteligência Artificial** e as **Recomendações específicas da Autoridade Europeia para a Proteção de Dados** ("AEPD") e da OCDE para a proteção de dados em sistemas de IA tornaram-se guias fundamentais para empresas do setor público e privado.

À medida que nos projetamos para 2025, as previsões apontam para um ano de transição regulamentar e crescente adoção da IA em setores estratégicos. A **aplicabilidade parcial do Regulamento da IA** marcará os primeiros passos na implementação prática das novas normas e, paralelamente, aguardamos também por desenvolvimentos no que respeita à Diretiva de Responsabilidade da IA (proposta publicada em setembro de 2022).

Inteligência Artificial | Legislação

Regulamento da Inteligência Artificial (AI Act)

O pioneiro Regulamento da IA da UE é crucial para as empresas, uma vez que estabelece um quadro comum baseado no risco e impõe um conjunto abrangente de obrigações a todos os intervenientes na cadeia de valor da IA, desde os prestadores aos responsáveis pela implantação.

Introduz também sanções substanciais em caso de incumprimento conforme destacamos infra. Consequentemente, as organizações devem identificar e mitigar os riscos associados aos seus modelos de IA através de medidas específicas.

Ver o nosso Guia: *Regulamento da IA: Guia Prático*

2 de agosto 2024	2 de fevereiro 2025	2 de agosto 2025	2 de agosto 2026	2 de agosto 2027
Entrada em vigor	Aplicação das disposições gerais do Regulamento da IA, requisitos de literacia e práticas de IA proibidas (Capítulos I e II)	Fornecimento de sistemas de IA de Finalidade Geral e sensibilização sobre os novos organismos reguladores e de supervisão relevantes (Capítulo III, secção 4, Capítulo V, VII e XII e o artigo 78.º , com exceção do artigo 101.º)	Aplicação geral do Regulamento da IA, com as exeções para classificação e obrigações correspondentes de Sistemas de IA de Risco Elevado	Aplicação geral do Regulamento da IA, sem exceções

Em caso de violação

- € 35 milhões ou 7% do volume de negócios anual (o que for superior) para práticas de IA proibidas.
- € 15 milhões ou 3% para a violação de outras obrigações
- € 7,5 milhões ou 1% por prestar informações incorretas
- Para as pequenas e médias empresas (“PME”), incluindo *startups*, as coimas não poderão exceder os montantes e percentagens acima referidos, consoante o montante mais baixo.

ACTION POINTS

- Avaliar o impacto da aplicação do Regulamento da IA;
- Mapear os sistemas de IA utilizados/produzidos;
- Classificar os sistemas de IA e avaliar os riscos inerentes aos mesmos;
- Definir um plano de ação com eventuais medidas de mitigação a serem aplicadas;
- Criar um sistema de gestão interno para a governação da utilização de IA numa organização;
- Sensibilizar e dar formação aos utilizadores dos sistemas de IA (fomentar a literacia no domínio da IA).

Inteligência Artificial | Orientações

Orientações AEPD - Sistemas de IA Generativa

Fornecem diretrizes para as instituições, órgãos, organismos e agências da União Europeia ("IUE") garantirem a conformidade com as obrigações de proteção de dados ao utilizarem sistemas de IA generativa

Destacam a importância de princípios como os da **minimização de dados**, **exatidão e transparência**, e a necessidade de Avaliações de Impacto Sobre os Dados Pessoais ("AIPD") para sistemas de IA com riscos elevados

Enfatizam a responsabilidade das IUE em desenvolver e utilizar a IA de maneira **ética e legal**, evitando enviesamentos e garantindo a segurança dos dados. Os sistemas de IA generativa apresentam desafios na proteção de dados pessoais e na transparência para os indivíduos. As IUE devem adotar uma **política de governança de dados robusta** e envolver os Encarregados da Proteção de Dados ("EPD") em todas as fases do ciclo de vida dos sistemas de IA para assegurar a conformidade regulatória.

Ver o nosso Post: *Orientações da AEPD sobre utilização de IA generativa*

ACTION POINTS

- Garantir o envolvimento do Encarregado de Proteção de Dados na utilização de sistemas de IA que tratam dados pessoais;
- Assegurar a conformidade no desenvolvimento e na implementação de um sistema de IA generativa com as obrigações em matéria de proteção de dados;
- Identificar e compreender o ciclo de vida e funcionamento dos sistemas de IA, em particular, garantir a identificação da origem/fonte dos dados pessoais, a base de licitude para esse tratamento;
- Compreender os resultados gerados pelos sistemas de IA (como funcionam os mecanismos de input e output) e analisar os processos de decisão implementados no sistema;
- Aplicar os princípios de proteção de dados;
- Garantir o cumprimento dos procedimentos em matéria de proteção de dados, em particular: (i) realizar uma avaliação de impacto sobre a proteção de dados, sempre que aplicável, (ii) atualizar o registo de atividades de tratamento, (iii) assegurar a revisão e conclusão de acordos de tratamento de dados.

Inteligência Artificial | Orientações

CEPD: Parecer 28/2024 sobre certos aspetos da proteção de dados relacionados ao tratamento de dados pessoais no contexto de modelos de IA

A autoridade de controlo irlandesa solicitou ao Comité Europeu para a Proteção de Dados ("CEPD") uma opinião sobre **a aplicação do RGPD no desenvolvimento de modelos de IA**, abordando anonimização, interesse legítimo e tratamento ilegal de dados pessoais.

O CEPD destacou:

- necessidade de avaliações caso a caso para anonimização
- a realização de um teste de três etapas para justificar o interesse legítimo e a consideração das expectativas dos titulares dos dados
- em relação ao tratamento ilegal, foram apresentados três cenários, cada um exigindo avaliação específica de conformidade com o RGPD
- a opinião do CEPD enfatiza a importância de medidas mitigadoras e a conformidade com a proteção de dados.

ACTION POINTS

- Documentar detalhadamente o processo de anonimização e manter registos que comprovem a anonimidade dos dados utilizados em sistemas de IA;
- Realizar Testes de Ponderação dos Interesses Legítimos ("TPIL") e AIPDs para analisar o impacto do tratamento nos titulares
dos dados;
- Considerar as expectativas razoáveis dos titulares dos dados ao desenvolver e implementar modelos de IA;
- Estabelecer procedimentos para lidar com cenários de tratamento ilegal de dados pessoais, incluindo retenção de dados nos sistemas de IA, tratamento por outro responsável e anonimização antes de novo tratamento.

Inteligência Artificial | Orientações

Recomendação OCDE - Inteligência Artificial

A OCDE atualizou a sua Recomendação sobre Inteligência Artificial para orientar os países membros na criação de políticas que promovam o desenvolvimento responsável da IA:

- importância da transparência, explicabilidade, proteção dos direitos humanos, e promoção de uma IA inclusiva e sustentável.
- abordagem centrada no ser humano, garantindo robustez e segurança dos sistemas de IA, e uma governança de dados de alta qualidade.
- responsabilidade dos prestadores e responsáveis pela implantação de sistemas de IA
- cooperação internacional para enfrentar desafios globais através da partilha de boas práticas e colaboração em pesquisa e desenvolvimento.

Ver o nosso Post: *A OCDE atualiza os seus princípios sobre IA*

ACTION POINTS

- Desenvolver e implementar sistemas de IA que sejam transparentes e explicáveis;
- Realizar avaliações de impacto ético e de direitos fundamentais para identificar e mitigar possíveis riscos dos sistemas de IA;
- Adotar práticas que promovam a inclusão e a sustentabilidade na utilização da IA;
- Garantir que os sistemas de IA são robustos e seguros contra ataques e falhas de segurança;
- Criar mecanismos claros de responsabilidade para os *developers* e operadores de sistemas de IA;
- Utilizar dados de alta qualidade e protegê-los contra utilizações indevidas;
- Promover a cooperação internacional através da partilha de boas práticas e da colaboração em pesquisas e desenvolvimento

Inteligência Artificial | Previsão **2025**

01

Aplicabilidade parcial do Regulamento da IA

O ano de 2025 marca o início da aplicabilidade do Regulamento da IA.

A partir do dia 2 de fevereiro, as empresas deverão garantir o seguinte:

- **Formação e literacia em IA**: As pessoas envolvidas na operação e utilização de sistemas de IA devem dispor de um nível suficiente de literacia no domínio da IA.
- **Práticas de IA proibidas**: Descontinuação da utilização de sistemas de IA em particular, práticas de IA proibidas.
- Sistema de inventário.

Já em agosto, o foco recairá sobre os **modelos de IA de finalidade geral.** Para este efeito, a partir do dia 2 desse mês, os prestadores de modelos desse tipo, deverão assegurar:

- ***Compliance***: Cumprimento de diversas obrigações relativas à documentação técnica, transparência e disponibilização de informações, que deverão estar registadas em políticas internas e em outros documentos acessíveis ao público.
- **Modelos de IA de finalidade geral com risco sistémico:** os prestadores destes modelos de IA deverão notificar a Comissão e cumprir com obrigações adicionais, incluindo a avaliação técnica, a documentação de testagens do modelo, a comunicações de incidentes às entidades competentes e a garantia de níveis de cibersegurança apropriados.

Até essa data, cada Estado-Membro deverá também ter designado ou criado **organismos reguladores e de supervisão competentes.**

02

Diretiva da Responsabilidade da IA

Em 2022, a Comissão Europeia apresentou a proposta da **Diretiva sobre a Responsabilidade da IA**, destinada a adaptar o direito privado às exigências da transição para a economia digital e a facilitar a apresentação de reclamações por danos causados por sistemas de IA e pela utilização de IA.

Esta proposta de Diretiva ainda necessita de ser analisada pelo Parlamento Europeu e pelo Conselho da União Europeia. Após as negociações e a sua adoção, os Estados-Membros da UE serão obrigados a transpor os termos da Diretiva sobre a Responsabilidade da IA para as respetivas legislações nacionais, num prazo que deverá rondar os dois anos.

Prevê-se que, em 2025, exista uma maior pressão política e legislativa para a aprovação desta Diretiva, considerando a sua complementaridade com o Regulamento sobre a IA.

Propriedade Intelectual

O ano de 2024 foi marcado por novidades legislativas no campo da propriedade intelectual na União Europeia. Destaca-se, em primeiro lugar, a implementação do pacote legislativo, composto pelo **Regulamento (UE) 2024/2822** e pela **Diretiva (UE) 2024/2823**, que visa **modernizar e simplificar o sistema de proteção de desenhos industriais**.

Além disso, a Recomendação (UE) 2024/915 da Comissão Europeia, de 19 de março de 2024, estabeleceu **medidas para combater a contrafação** e melhorar o respeito pelos direitos de propriedade intelectual na União Europeia.

Já no que toca a decisões judiciais no campo da propriedade intelectual, destacam-se os acórdãos proferidos pelo Tribunal de Justiça da União Europeia que **clarificaram o âmbito de aplicação e de proteção do direito de autor e de direitos sobre marcas e patentes**, abordando questões como o uso referencial de marcas, o ónus da prova para determinados casos, a proteção de obras de arte aplicadas e a modificação de programas de computador, entre outras.

Propriedade Intelectual | Legislação

Novo Pacote Legislativo Europeu para Desenhos ou Modelos

O pacote legislativo composto pelo Regulamento (UE) 2024/2822 e pela Diretiva (UE) 2024/2823 visa modernizar e simplificar o **sistema de proteção de desenhos industriais na União Europeia**, harmonizando regras de registo e introduzindo procedimentos mais ágeis e menos burocráticos. A reforma facilita o processo de **registo**, **reduz custos**, combate a **pirataria** e **falsificação**, e fortalece os **direitos dos titulares**. Além disso, amplia a **proteção de desenhos não registados** e adapta a legislação às novas tecnologias, como a digitalização e a impressão 3D, garantindo uma proteção eficaz no ambiente digital.

Ver o nosso Post: *Publicada a reforma da legislação europeia em matéria de desenhos*

Regulamento (UE) 2024/2822

13 de novembro 2024	1 de maio 2025	1 de julho 2026
Entrada em vigor	Aplicação do Regulamento, com algumas exceções no que toca às alterações propostas ao Regulamento 6/2002, de 12 de dezembro (artigo 1.º, pontos 21, 22, 24, 26 a 30, 32, alínea b), 34, al. b), 37, 40, 42, 45, 46, 49, 52, 54, 56, 58, 61, 63, 65, 66, 70, 72, 74, 76, 78, 80, al. b), 81, 85, 88 na medida em que visa o artigo 72.º, n.º 3, al. a), e), f) e m), e os pontos 90, 98, alínea b), 111, 113 e 123)	Aplicação geral do Regulamento

Diretiva (UE) 2024/2823

13 de novembro 2024	9 de dezembro 2027
Entrada em vigor e data de aplicação da Diretiva, com algumas exceções no que toca ao direito substantivo em matéria de desenhos ou modelos (artigos 4.º, 5.º, 7.º, 8.º, 9.º, 20.º e 22.º)	Aplicação geral da Diretiva

ACTION POINTS

- As empresas devem garantir que os seus processos de registo de desenhos ou modelos estão em conformidade com os **novos requisitos estabelecidos pelo Regulamento (UE) 2024/2822 e pela Diretiva 2024/2823**;
- As empresas devem adotar medidas proativas para proteger os seus desenhos ou modelos contra a contrafação. Isso inclui **monitorizar a entrada de produtos no mercado da União Europeia** e utilizar os **procedimentos aduaneiros** definidos no Regulamento (UE) 608/2013 para impedir a entrada de produtos que violem os seus direitos de desenho ou modelo;
- Para cumprir a **"cláusula de reparação"** e evitar problemas legais, as empresas que fabricam ou vendem componentes de produtos complexos devem informar claramente os consumidores sobre a origem comercial e a identidade do fabricante dos produtos utilizados para reparação.

Propriedade Intelectual | Orientações

Recomendação da Comissão - Combate à contrafação e melhoria do respeito pelos direitos de PI

A Recomendação (UE) 2024/915 da Comissão Europeia, de 19 de março de 2024, estabelece medidas para combater a contrafação e melhorar o respeito pelos direitos de propriedade intelectual na União Europeia

- destaca a necessidade de uma política robusta contra essas atividades ilícitas
- promove a cooperação entre titulares de direitos, prestadores de serviços intermediários e autoridades competentes, e incentiva o uso de novas tecnologias e boas práticas.
- promove a modernização de instrumentos voluntários, a designação de pontos de contacto únicos, e a utilização de ferramentas como o Portal para Aplicação de DPI (IPEP) e o sistema de alerta rápido *Safety Gate*
- estabelece medidas específicas para evitar o uso abusivo de serviços de transporte, logística, pagamento e redes sociais
- promove a resolução alternativa de litígios
- promove a adaptação às novas tecnologias, como a inteligência artificial.
- encoraja a sensibilização e formação em matéria de propriedade intelectual, especialmente para PME, através de iniciativas como o Fundo PME e instrumentos de prevenção do furto informático, sublinhando a importância de uma abordagem coordenada e colaborativa para proteger a inovação e os investimentos na UE.

ACTION POINTS

- Estabelecer parcerias e colaborar estreitamente com titulares de direitos, prestadores de serviços intermediários e autoridades competentes para combater a contrafação e a pirataria, nomeadamente através da utilização de instrumentos voluntários, como memorandos de entendimento;
- Designar **pontos de contacto únicos dentro da empresa** para lidar com questões de respeito dos direitos de propriedade intelectual;
- Adotar e **implementar novas tecnologias**, como a inteligência artificial e sistemas avançados de rastreio, para **identificar e combater mercadorias de contrafação**;
- Utilizar ferramentas como o **Portal para Aplicação de DPI** (IPEP) e o **sistema de alerta rápido *Safety Gate*** para facilitar a cooperação e a partilha de informações sobre atividades ilícitas.

Propriedade Intelectual | Jurisprudência

Violação de Direitos de Marca

O Acórdão do Tribunal de Justiça da União Europeia de 11 de janeiro de 2024, no processo C-361/22, interpretou o artigo 6.º, n.º 1, alínea c), da Diretiva 2008/95/CE, que permite o **uso de marcas por terceiros** para indicar o destino de produtos ou serviços, desde que em conformidade com práticas honestas.

O litígio no processo principal opôs a Inditex e a Buongiorno Myalert sobre a utilização da marca "ZARA" numa campanha promocional, tendo o Tribunal concluído que tal **uso é permitido apenas quando necessário para indicar o destino de um produto ou serviço oferecido pelo terceiro**.

Esgotamento dos direitos conferidos por uma marca da UE

O Acórdão C-367/21 do Tribunal de Justiça da União Europeia, de 18 de janeiro de 2024, aborda o esgotamento dos direitos de marca no caso entre Hewlett Packard e Senetic. O tribunal decidiu que o **ónus da prova do esgotamento dos direitos de marca não pode recair exclusivamente sobre a demandada**, especialmente quando os produtos não têm identificação clara do mercado de destino e são distribuídos por redes seletivas.

Em tais casos, o titular da marca deve provar que os produtos foram inicialmente colocados no mercado fora do EEE, para evitar a compartimentação dos mercados nacionais e garantir a livre circulação de mercadorias, equilibrando a proteção dos direitos de propriedade intelectual com as liberdades do mercado interno.

Violação de Direitos de Autor

O Processo C-159/23 tem por objeto um pedido de decisão prejudicial em que se colocou ao TJUE a questão de saber se a modificação do conteúdo das variáveis armazenadas na memória interna de um computador por outro programa, sem alterar o código-fonte ou o código-objeto do programa protegido, constitui uma violação dos direitos de autor conforme a Diretiva 2009/24/CE. O Tribunal de Justiça da União Europeia concluiu que **a proteção conferida pela diretiva se aplica apenas à expressão literal do programa de computador, como o código-fonte e o código-objeto, e não às ideias, princípios ou funcionalidades subjacentes**. Assim, a modificação do conteúdo das variáveis por outro programa, que não permite a reprodução ou realização posterior do programa protegido, não está coberta pela proteção da diretiva.

Propriedade Intelectual | Jurisprudência

Violação de Direitos de Autor

No Processo C-227/23 o TJUE foi chamado a interpretar a **aplicabilidade dos direitos de autor sobre obras de arte aplicadas especificamente no contexto da Convenção de Berna e da Diretiva 2001/29/CE**. O Tribunal concluiu que os Estados-Membros não podem aplicar o critério de reciprocidade material da Convenção de Berna a obras de países terceiros, devendo a harmonização dos direitos de autor ser determinada pelo legislador da União Europeia.

Esta decisão assegura uma proteção uniforme e elevada para todas as obras no mercado interno da UE, independentemente do país de origem ou da nacionalidade do autor.

Prazo para reivindicar o direito de prioridade no registo de desenhos e patentes

O Acórdão C-382/21 do Tribunal de Justiça da União Europeia, de 27 de fevereiro de 2024, abordou a **aplicação do prazo de prioridade de seis meses do artigo 41.º do Regulamento (CE) n.º 6/2002 a pedidos internacionais de patente**.

No litígio no processo principal envolvendo a The KaiKai Company Jaeger Wichmann GbR, que reivindicou prioridade com base num pedido internacional de patente sob o Tratado de Cooperação em Matéria de Patentes (TCP), o **Tribunal Geral considerou que havia uma lacuna legislativa e aplicou o prazo de doze meses da Convenção de Paris**.

No entanto, o Tribunal de Justiça discordou, afirmando que o artigo 41.º é claro e exaustivo, limitando o direito de prioridade a seis meses para pedidos de registo de desenhos ou modelos, e concluiu que a decisão do Tribunal Geral excedeu os limites de uma interpretação conforme.

Propriedade Intelectual | Previsão **2025**

01

Tribunal Unificado de Patentes

O referendo esperado na Irlanda sobre a ratificação do Acordo relativo ao Tribunal Unificado de Patentes poderá realizar-se, o que colocaria as empresas irlandesas sob a jurisdição do TUP.

Esta mudança permitiria a execução centralizada de patentes europeias, simplificando os litígios para os titulares de patentes.

No entanto, esta alteração também poderá levantar questões sobre mudanças jurisdicionais e implicações práticas para as empresas que operam na Irlanda.

02

Proteção de Propriedade Intelectual Relacionada com IA

Com o contínuo avanço das ferramentas de inteligência artificial, os debates jurídicos em torno da proteção de obras geradas por IA e da patenteabilidade de invenções impulsionadas por estas tecnologias deverão intensificar-se. Questões fundamentais, como a possibilidade de proteger criações geradas por IA ao abrigo da legislação de propriedade intelectual, e se o uso de propriedade intelectual de terceiros para treinar modelos de IA constitui infração, estarão no centro das discussões. Paralelamente, temas como o papel dos inventores humanos, os critérios de novidade e passo inventivo, e a potencial consideração da IA como inventora por mérito próprio poderão levar a alterações legislativas ou ao desenvolvimento de nova jurisprudência.

Tanto na União Europeia como a nível global, é esperado que estas mudanças tragam maior clareza e definição ao enquadramento legal destas questões em 2025 , principalmente a nível jurisprudencial e com a aplicabilidade de algumas das disposições do Regulamento de IA a partir de fevereiro deste ano.

As empresas que inovam no campo da IA deverão monitorizar cuidadosamente estes desenvolvimentos, garantindo que as suas criações e invenções estão devidamente protegidas e em conformidade com as normas emergentes.

Ver Secção Inteligência Artificial.

Privacidade e Proteção de Dados

No ano de 2024, verificou-se uma consolidação dos conceitos e métodos de recolha e tratamento de dados pessoais. Destacam-se, em particular, as orientações do Comité Europeu para a Proteção de Dados (CEPD) sobre a utilização de **tecnologias de reconhecimento facial**, da Autoridade de Controlo Espanhola (AEPD) quanto aos riscos do **Wi-Fi Tracking**, bem como as decisões proferidas pelo Tribunal de Justiça da União Europeia (TJUE) relativas aos **princípios consagrados no RGPD** e ao **cálculo de coimas** aplicáveis.

Pela Europa fora, durante o ano de 2024, foram **aplicadas coimas de valores extraordinários**, destacando-se a coima aplicada pela Autoridade de Controlo Irlandesa (DPC) ao LinkedIn no valor de €310 milhões.

Saliente-se ainda que a Comissão Nacional de Proteção de Dados (CNPD) investigou e subsequentemente suspendeu o **tratamento de dados biométricos** prosseguido pela Worldcoin Foundation, cujo projeto visava a criação de uma prova de identidade digital (WorldID).
O ano de 2025 não será certamente diferente no que diz respeito à dinâmica existente em matéria de proteção de dados, especificamente no que se refere às decisões de autoridades judiciais administrativas competentes, à organização das estruturas empresarias e à atenção dispensada pelos titulares dos dados a estas questões.

Privacidade e Proteção de Dados | Orientações

Consentimento Válido no Contexto de Modelos de Consentimento ou Pagamento implementados por Grandes Plataformas em Linha

As Autoridades de Controlo dos Países Baixos, Noruega e Alemanha solicitaram ao Comité Europeu para a Proteção de Dados (CEPD) um parecer sobre as condições em que as **grandes plataformas online** podem aplicar, de forma válida e livre, modelos de "**consentimento ou pagamento**" para **publicidade comportamental**. O CEPD sublinha que:

- o consentimento deve cumprir os princípios do RGPD, incluindo os da necessidade, proporcionalidade e lealdade. As plataformas devem garantir a disponibilização de alternativas gratuitas ou que impliquem um tratamento de dados pessoais mais reduzido.
- o consentimento deve ser dado livremente, sem que a taxa cobrada comprometa a liberdade de escolha dos titulares de dados, especialmente quando o serviço for essencial para a vida social ou profissional.
- deve ser evitada a condicionalidade do consentimento, devendo ser oferecidas alternativas equivalentes que não exijam o tratamento de dados pessoais.
- o consentimento deve ser específico, informado e explícito, permitindo granularidade nas finalidades apresentadas. Os responsáveis devem evitar modelos enganosos, avaliar a periodicidade de renovação do consentimento, facilitar a sua retirada e assegurar que os titulares dos dados compreendem plenamente as suas escolhas e respetivas consequências.

ACTION POINTS

- Fornecer informações claras e compreensíveis relativamente às opções à disposição dos titulares dos dados num modelo de "Consentimento ou Pagamento", para que estes possam realizar uma escolha verdadeiramente livre;
- Garantir que o consentimento recolhido é livre, específico, informado e explícito;
- Garantir que a taxa exigida no modelo de pagamento não é alta ao ponto de condicionar a escolha do titular dos dados.

Privacidade e Proteção de Dados | Orientações

Orientações sobre os Riscos de Wi-Fi Tracking

As orientações elaboradas pela AEPD, APDCAT, AVPD e CTDPA sobre os riscos associados ao Wi-Fi Tracking destacam a crescente preocupação com a privacidade e a proteção de dados pessoais, enfatizando a necessidade de transparência e consentimento informado dos titulares dos dados cujos dados são recolhidos.

- as empresas devem informar claramente os titulares de dados sobre a recolha e oferecer-lhes a opção de consentir ou recusar, além de implementarem medidas de segurança robustas para proteger os dados.
- as autoridades reguladoras são incentivadas a reforçar a fiscalização e garantir a conformidade com o RGPD. Simultaneamente, as empresas devem realizar Avaliações de Impacto sobre a Proteção de Dados (AIPD) e adotar uma abordagem de *Privacy By Design*.

ACTION POINTS

- Informar claramente os titulares de dados sobre a recolha de dados através de Wi-Fi Tracking;
- Recolher o consentimento livre, específico, informado e explícito dos titulares dos dados antes de recolher os seus dados;
- Implementar e rever medidas de segurança avançadas para proteger os dados recolhidos contra acessos não autorizados e incidentes de segurança;
- Realizar Avaliações de Impacto sobre a Proteção de Dados (AIPD) para identificar e mitigar riscos associados ao Wi-Fi Tracking;
- Oferecer aos titulares dos dados a opção clara e fácil de recusar a recolha dos seus dados através de Wi-Fi Tracking.

Privacidade e Proteção de Dados | Orientações

Orientações 2/2023 sobre o âmbito de aplicação técnica do artigo 5.º, n.º 3 da Diretiva relativa à Privacidade e às Comunicações Eletrónicas

As Diretrizes do CEPD de 2024 clarificam a aplicação do Artigo 5.º, n.º 3 da Diretiva (UE) 2002/58/EC (**Diretiva E-Privacy**) a diversas soluções técnicas, abordando ambiguidades relacionadas com novas ferramentas de rastreamento.

Visa **proteger a esfera privada dos utilizadores**, abrangendo não apenas dados pessoais, mas também qualquer informação armazenada no equipamento terminal. A proteção aplica-se a operações que envolvem armazenamento ou acesso a informações no equipamento terminal de um assinante ou utilizador, independentemente da origem ou natureza da informação.

O Artigo 5.º, n.º 3 da Diretiva E-Privacy não se restringe ao uso de cookies, mas também a tecnologias semelhantes.

As diretrizes identificam e analisam os principais elementos associados ao artigo sob análise : **"informação"**, **"equipamento terminal de um assinante ou utilizador"**, **"rede de comunicações eletrónicas"**, **"acesso"** e "**informação armazenada/armazenamento".**

ACTION POINTS

- Garantir que qualquer utilização de tecnologias de rastreamento, como cookies, fingerprinting de dispositivos, e pixels, seja precedido pela obtenção de consentimento explícito e informado dos titulares dos dados;
- Adotar medidas para proteger a privacidade dos titulares dos dados, garantindo que qualquer acesso ou armazenamento de informações no equipamento terminal seja devidamente regulado e consentido.

Privacidade e Proteção de Dados | Jurisprudência

Interpretação do conceito de "Dados Pessoais"

O Processo C-604/22 analisou a definição de "dados pessoais" e a responsabilidade das organizações setoriais no tratamento de dados relacionados com o consentimento na publicidade digital.

O TJUE concluiu que a Transparency and Consent String (TC String), utilizada pela IAB Europe no Transparency & Consent Framework (TCF), **constitui um dado pessoal, visto que é suscetível de identificar pessoas singulares**.

A IAB Europe foi considerada "Responsável Conjunta pelo Tratamento" dos dados pessoais, uma vez que influencia as finalidades e meios de tratamento, mesmo sem ter acesso direto aos dados em causa.

No entanto, o TJUE esclareceu que a sua responsabilidade não se estende automaticamente a tratamentos subsequentes realizados por terceiros, como fornecedores de sites, salvo se a IAB influenciar diretamente esses tratamentos.

Acesso a dados pessoais no contexto de uma investigação penal sem autorização judicial

O Processo C-548/21 do TJUE abordou a **legalidade da apreensão e acesso a dados de telemóveis por autoridades policiais sem autorização judicial**, no contexto de investigações criminais.

O TJUE concluiu que tal acesso constitui uma grave ingerência nos direitos à privacidade e proteção de dados pessoais, **devendo ser limitado a investigações de infrações penais graves e sujeito a fiscalização prévia** por um juiz ou entidade independente, exceto em casos de urgência justificada.

A legislação nacional em causa que permite o acesso sem autorização judicial é incompatível com a Diretiva (UE) 2016/680 e a Carta dos Direitos Fundamentais. Em particular, as autoridades deverão informar os titulares dos dados sobre a tentativa de acesso, salvo se essa informação comprometer a investigação.

De igual forma, a regulamentação deverá definir claramente as infrações que justificam tal acesso, respeitando o princípio da proporcionalidade.

Privacidade e Proteção de Dados | Decisões das Autoridades de Controlo

Princípios Gerais de Proteção de Dados

A Amazon France Logistique, responsável pelos armazéns da Amazon em França, foi investigada pela Autoridade de Controlo Francesa (CNIL) após denúncias sobre o **uso de scanners para monitorizar a atividade dos trabalhadores em tempo real.**

A CNIL identificou várias irregularidades, incluindo a violação do princípio da minimização dos dados, uso excessivo e ilegal de indicadores de produtividade, falta de informação adequada aos trabalhadores temporários e visitantes sobre a recolha de dados e videovigilância, e falhas na segurança do acesso ao software de videovigilância.

A decisão destacou a necessidade de respeitar o princípio da minimização dos dados, garantir transparência e segurança no tratamento de dados pessoais, e evitar o controlo excessivo dos trabalhadores.

Dados Biométricos

A CNPD iniciou uma investigação sobre a conformidade do tratamento de dados biométricos pela Worldcoin Foundation, que recolhia imagens da íris, olhos e rosto de indivíduos em troca da criptomoeda Worldcoin (WLD) para criar uma **prova de identidade digital** (World ID). A CNPD determinou que a Worldcoin Foundation recolheu dados biométricos de menores sem uma verificação prévia de idade, impossibilitou o exercício do direito ao apagamento e à revogação do consentimento, tendo ainda fornecido informações insuficientes aos titulares dos dados, violando as regras e princípios consagrados no RGPD.

A 25 de março de 2024, a **CNPD impôs uma limitação de 90 dias à recolha e tratamento de dados biométricos** pela Worldcoin Foundation em Portugal. Posteriormente, a 9 de julho de 2024, a CNPD reconheceu a **BayLDA como a Responsável pelo Tratamento principal** para este tratamento de dados transfronteiriço, declarando-se como Autoridade de Controlo Interessada.

ACTION POINTS

- Garantir que as práticas de monitorização dos trabalhadores sejam proporcionais e justificadas, evitando o controlo excessivo e respeitando os direitos de privacidade dos trabalhadores;
- Informar claramente todos os trabalhadores, temporários e permanentes, bem como visitantes, sobre a recolha de dados e sobre a utilização de sistemas de videovigilância;
- Recolher apenas os dados estritamente necessários para a gestão das operações e evitar a recolha excessiva de informações sobre os trabalhadores.

Privacidade e Proteção de Dados | Decisões das Autoridades de Controlo

Princípios Gerais de Proteção de Dados

A Autoridade de Controlo dos Países Baixos (AP) iniciou uma investigação à Uber após mais de 170 queixas sobre a **informação transmitida aos titulares dos dados e transferências de dados pessoais para fora do Espaço Económico Europeu (EEE)**.

Durante esta investigação, determinou-se que a Uber recolhia e armazenava informação sensível sobre os condutores europeus em servidores nos EUA sem ter adotado métodos de transferência adequados, incluindo dados de conta, licenças de táxi, localização, fotografias, detalhes de pagamento, documentos de identidade, e, em alguns casos, dados criminais e médicos.

Nestes termos, a AP aplicou uma **coima de €290 milhões** à Uber, a terceira desde 2018 por **violações de dados pessoais e incumprimento dos deveres de informação**.

ACTION POINTS

- Garantir que todas as transferências de dados pessoais para fora do Espaço Económico Europeu (EEE) são realizadas utilizando mecanismos de transferência adequados, nos termos do RGPD;
- Fornecer informações claras e completas aos titulares dos dados sobre a forma como os seus dados pessoais são recolhidos, usados, armazenados e transferidos, cumprindo todas as obrigações de informação estabelecidas pelo RGPD.

Privacidade e Proteção de Dados | Conteúdos Legais

Quadro de Privacidade UE-US FAQ

O Comité Europeu para a Proteção de Dados (CEPD) publicou um FAQ sobre o **Quadro de Privacidade entre a União Europeia e os Estados Unidos**, que visa facilitar a transferência de dados pessoais entre as duas regiões, garantindo um nível adequado de proteção de dados.

Este Quadro de Privacidade foi desenvolvido em resposta às preocupações levantadas pelo Tribunal de Justiça da União Europeia (TJUE), que determinou a invalidação do anterior EU-US Privacy Shield.

As orientações do CEPD destacam a necessidade de **transparência**, medidas de **segurança** adequadas, respeito pelos **direitos dos titulares dos dados**, e mecanismos eficazes de **recurso e supervisão**.

Além disso, o CEPD forneceu **recomendações para as empresas**, como a realização de Avaliações de Impacto sobre a Proteção de Dados (AIPD) e a criação de políticas claras de privacidade, com o objetivo de promover uma transferência de dados segura e eficiente, protegendo os direitos fundamentais dos titulares dos dados.

ACTION POINTS

- As empresas devem implementar procedimentos de transferências internacionais de dados que sejam claros e que cumpram com os requisitos de transferências internacionais da UE;
- Celebrar Acordos de Subcontratação sobre o Tratamento de Dados Pessoais com terceiros para garantir que as transferências de dados por estes efetuadas cumprem com os requisitos estabelecidos no RGPD.

Privacidade e Proteção de Dados | Conteúdos Legais

Regulamento de Dados FAQ

A Comissão Europeia publicou FAQs sobre o Regulamento de Dados, uma proposta legislativa que visa regular o acesso e a utilização de dados na União Europeia, promovendo a inovação e a competitividade.

O Regulamento de Dados estabelece um quadro jurídico para a partilha de dados entre empresas, consumidores e autoridades públicas, assegurando a proteção dos direitos dos titulares dos dados e a segurança dos mesmos.

As FAQs destacam:

- quem pode aceder aos dados e em que condições
- as obrigações das partes envolvidas
- a interoperabilidade dos sistemas de dados
- a responsabilidade na gestão dos dados e as medidas de segurança necessárias.

Além disso, propõe mecanismos para resolver disputas relacionadas com o acesso e utilização de dados, como mediação e arbitragem, visando criar um mercado único de dados na UE.

Ver o nosso Legal Flash: *Regulamento Dados ("Data Act"): finalmente aprovado pelo Parlamento Europeu*

Privacidade e Proteção de Dados | Previsão **2025**

01

Aplicabilidade do Regulamento de Dados

O Regulamento de Dados tornar-se-á aplicável ao longo de 2025. Este diploma tem como objetivo garantir que os dados gerados por dispositivos conectados e serviços digitais sejam acessíveis e utilizáveis por diferentes partes, promovendo a inovação e a competitividade no mercado europeu.

02

Regulamento relativo ao Espaço Europeu de Dados de Saúde

Espera-se que avancem as discussões sobre a proposta de Regulamento relativo ao Espaço Europeu de Dados de Saúde, cujo propósito é criar um espaço comum europeu onde as pessoas singulares possam controlar os seus dados de saúde eletrónicos (COM 2022/197).

03

Regras processuais relativas ao RGPD

Espera-se que ocorram avanços na proposta de Regulamento que visa estabelecer normas processuais relativas ao tratamento de reclamações e à realização de investigações no âmbito do RGPD (COM/2023/348).

04

Cláusulas contratuais-tipo para a transferência de dados

Prevê-se que a Comissão Europeia publique Cláusulas Contratuais-Tipo destinadas a situações em que um importador de dados sujeito ao RGPD esteja localizado num país terceiro.

Telecomunicações e Tecnologia

O ano de 2024 foi marcado pela inovação tecnológica, razão pela qual destacamos nesta área a **Estratégia Digital Nacional** orientada para as Pessoas, Empresas, Estado e Infraestruturas e que pretende posicionar Portugal como líder na transição digital até 2030.

Na área das Telecomunicações temos a destacar no ano de 2024 a decisão do Tribunal Constitucional que declarou a inconstitucionalidade com força obrigatória geral das normas constantes da Portaria n.º 1473-B/2008, aprovada pela ANACOM, que cobravam **taxas aos fornecedores de redes e serviços de comunicações eletrónicas enquadrados no "Escalão 2"**. Em particular, o Tribunal determinou que as normas em causa violavam o princípio da reserva de função legislativa.

Telecomunicações e Tecnologia | Legislação

Regulamento relativo à Liberdade dos Meios de Comunicação Social

O Regulamento (UE) 2024/1083 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, estabelece um **quadro comum para os serviços de comunicação social no mercado interno da União Europeia**, visando proteger a liberdade e o pluralismo dos meios de comunicação social.

Este regulamento harmoniza as regras nacionais para garantir condições equitativas para os prestadores de serviços de comunicação social, incluindo os **setores audiovisual**, **rádio** e **imprensa**.

A digitalização e a internacionalização dos meios de comunicação social aumentaram a importância de uma abordagem coordenada para enfrentar desafios como a desinformação, a manipulação da informação e a interferência de países terceiros.

1 de maio 2024	8 de novembro 2024	8 de fevereiro 2025	8 de maio 2025	8 de agosto 2025	8 de maio 2027
Entrada em vigor	Aplicação da norma relativa aos direitos dos destinatários de serviços de comunicação social	Aplicação das normas relativas aos direitos e deveres dos prestadores de serviços, do capítulo referente à cooperação entre autoridades	Aplicação da secção referente à cooperação e convergência em matéria de regulamentação	Aplicação da totalidade do Regulamento em apreço, salvo as exceções elencadas	Aplicação da norma referente ao direito de personalizar a oferta de meios de comunicação social

ACTION POINTS

- Adotar medidas que garantam que as decisões editoriais possam ser tomadas livremente dentro da linha editorial da empresa;
- Dialogar de forma estruturada com fornecedores de plataformas em linha de grande dimensão para resolver questões de moderação de conteúdos e promover o acesso a uma oferta diversificada de meios de comunicação social;
- Fornecer informações exatas e detalhadas sobre as metodologias utilizadas para medir audiências, garantindo que estas sejam transparentes, imparciais e verificáveis e submetê-las a auditorias independentes anuais para assegurar a sua fiabilidade e comparabilidade.

Telecomunicações e Tecnologia | Conteúdos Legais

Estratégia Digital Nacional

A Estratégia Digital Nacional de Portugal visa posicionar o país como líder na **transição digital até 2030**, promovendo a

- **Inclusão digital**
- **Sustentabilidade**
- **Competitividade económica**.

Estruturada em quatro dimensões principais - **Pessoas**, **Empresas**, **Estado** e **Infraestruturas** - a estratégia inclui objetivos como:

- aumentar a literacia digital
- garantir a segurança no uso da tecnologia
- promover a igualdade de género nas áreas STEM
- modernizar e digitalizar os processos administrativos
- expandir a cobertura de internet de alta velocidade
- fortalecer a cibersegurança e desenvolver uma infraestrutura de *cloud* soberana.

A criação de uma Agência Nacional para o Digital e a implementação de uma Agenda Nacional de Inteligência Artificial são ações-chave para garantir uma governança digital robusta e a adoção ética e segura de novas tecnologias.

Plano de Ação para a Comunicação Social

O Setor da Comunicação Social enfrenta desafios significativos que afetam a sustentabilidade das empresas e a estabilidade dos trabalhadores, colocando em risco o pluralismo e a liberdade de expressão.

O Governo compromete-se a desenvolver um plano abrangente para enfrentar problemas estruturais e conjunturais decorrentes de mudanças tecnológicas e de hábitos de consumo, assegurando a sustentabilidade e independência da Comunicação Social em Portugal.

A Resolução do Conselho de Ministros n.º 105/2024 criou a Estrutura de Missão #PortugalMediaLab para coordenar e monitorizar a execução das políticas públicas, promovendo transparência, pluralismo, diversidade e inclusão nos media, e fortalecendo a confiança pública no processo de formulação e execução das políticas.

Telecomunicações e Tecnologia | Previsão **2025**

01

Estratégia Digital Nacional 2030

A Estratégia Digital Nacional de Portugal irá posicionar o país como líder na transição digital até 2030, promovendo a inclusão digital, a sustentabilidade e a competitividade económica.

Antecipa-se que haja desenvolvimentos no que respeita às alterações e melhorias elencadas, primordialmente quanto ao reforço das competências digitais da população e dos recursos para responder a incidentes de cibersegurança que ocorram na Administração Pública.

Cibersegurança

Foram aprovados três Regulamentos Delegados Suplementares ao Regulamento DORA, que introduziram várias normas técnicas relacionadas com a classificação de incidentes e a gestão de riscos associados às tecnologias de informação e comunicação (TIC).

Adicionalmente, a Comissão Europeia aprovou o Regulamento da Ciber-Resiliência, que visa estabelecer normas harmonizadas de cibersegurança para produtos digitais na União Europeia. Paralelamente, foram definidas diversas regras para a aplicação da Diretiva NIS2.

Cibersegurança | Legislação

Regulamento Delegado (UE) 2024/1772

O Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, complementa o Regulamento (UE) 2022/2554 (Regulamento DORA), estabelecendo normas técnicas para a classificação de incidentes relacionados com as TIC e ciberameaças no setor financeiro. Visa harmonizar e simplificar os requisitos de notificação de incidentes para diferentes tipos de entidades financeiras.

Entrada em vigor — 2 de abril 2024 — Aplicação dos Regulamentos

Regulamento Delegado (UE) 2024/1773

O Regulamento Delegado (UE) 2024/1773 da Comissão, de 13 de março de 2024, complementa o Regulamento (UE) 2022/2554 (Regulamento DORA), estabelecendo normas técnicas para a utilização de serviços de TIC prestados por terceiros em funções críticas no setor financeiro.

ACTION POINTS

- Rever e atualizar as atuais políticas e procedimentos de deteção e resposta a ciberameaças e a incidentes de segurança da informação;
- Rever a matriz de risco atual da entidade e atualizá-la consoante o panorama de ameaças de acordo com o setor de atividade, dimensão e exposição ao risco;
- Atualizar os procedimentos de classificação e notificação de incidentes de segurança.

- Desenvolver procedimentos claros de análise prévia à contratação de serviços de TIC de terceiros ou rever e atualizar os procedimentos existentes;
- Desenvolver formulários de análise em matéria de segurança e capacidade técnica e humana para a prestação de serviços de TIC, com foco no risco associado ao serviço e na capacidade de manutenção e continuidade das operações em caso de incidente de segurança;
- Incluir áreas de Compras, Jurídico, IT, DPO e Compliance na análise prévia do prestador, bem como de Recursos Humanos aquando do início de prestação de serviços à entidade abrangida pelo Regulamento DORA;
- Desenvolvimento/atualização de um registo de prestadores de TIC da entidade e respetiva criticidade para a manutenção do negócio.

Cibersegurança | Legislação

Regulamento Delegado (UE) 2024/1774

O Regulamento Delegado (UE) 2024/1774 da Comissão, de 13 de março de 2024, complementa o Regulamento (UE) 2022/2554 e estabelece normas técnicas para a gestão do risco associado às tecnologias da informação e comunicação (TIC) no setor financeiro, visando assegurar a resiliência operacional digital das entidades financeiras.

Entrada em vigor: 2 de abril 2024 ▶ Aplicação do Regulamento

ACTION POINTS

- Revisão dos princípios, políticas e procedimentos relacionados com o risco da entidade financeira, de acordo com o panorama atual de ameaças, vulnerabilidades atuais e emergentes e nível de exposição da entidade a potenciais ciberataques;
- Revisão da classificação de risco dos serviços, produtos ou ativos de TIC na entidade, e identificação de interdependências entre os mesmos para a prestação do serviço.

Cibersegurança | Legislação

Regras de aplicação da Diretiva NIS2

O Regulamento de Implementação da Comissão de 17 de outubro de 2024 estabelece regras de aplicação da Diretiva (UE) 2022/2555 (Diretiva NIS2) relativamente aos requisitos técnicos e metodológicos de medidas de gestão de risco de cibersegurança previstos no artigo 21.º, n.º 2 da Diretiva NIS2 e à especificação adicional dos casos em que um incidente de cibersegurança é considerado como significativo nos termos do artigo 23.º, n.º 3
da Diretiva NIS2, relativamente a prestadores de serviços DNS, registos de nomes TLD, serviços de computação em nuvem, prestadores de serviços de centros de dados, fornecedores de redes de distribuição e conteúdos, fornecedores de serviços geridos, prestadores de serviços de segurança geridos, fornecedores de mercados em linha, motores de pesquisa em linha e de plataformas de serviços de redes sociais e prestadores de serviços de confiança.

Entrada em vigor: 2 de novembro 2024 ▶ Aplicação do Regulamento

ACTION POINTS

- Rever e atualizar, com base neste Regulamento, o plano de segurança da entidade, como foco nas medidas eficazes de identificação, prevenção e mitigação de riscos de segurança da informação;
- Implementar/rever o procedimento de resposta a incidentes, em particular analisar e definir os critérios para a classificação de um incidente de cibersegurança como "significativo", com base nas especificações do artigo 23.º, n.º 3 da Diretiva NIS2;
- Implementar sistemas de monitorização contínua para avaliar a eficácia das medidas de cibersegurança aplicadas, com um plano regular de auditorias e atualizações.

Cibersegurança | Legislação

Regulamento da Ciber-Resiliência

O Regulamento (UE) 2024/2847 estabelece normas unificadas de cibersegurança para produtos digitais na União Europeia, aplicando-se a todos os produtos de hardware e software com elementos digitais.

Este regulamento exige que fabricantes, importadores e distribuidores adotem medidas de segurança desde a conceção dos produtos, promovam avaliações rigorosas para identificar e mitigar riscos, mantenham registos detalhados e garantam a marcação CE.

Além disso, os fabricantes devem comunicar vulnerabilidades e incidentes de cibersegurança às autoridades competentes, como a ENISA e a rede de CSIRT, dentro de prazos específicos, e fornecer atualizações de segurança contínuas.

Ver o nosso Legal Flash: *Regulamento da Ciber-Resiliência*

2 de agosto 2024	2 de fevereiro 2025	2 de agosto 2025	2 de agosto 2026
Entrada em vigor	Aplicação de disposições sobre notificações e conformidade	Aplicação de obrigações de informação pelos fabricantes	Aplicação plena do Regulamento

ACTION POINTS

- Rever os sistemas de gestão de segurança da informação e atualizá-los em conformidade com os padrões de referência atuais para a segurança de produtos;
- Para fabricantes: Garantir a conformidade com as medidas técnicas de segurança e de gestão de risco dos produtos digitais;
- Para importadores e distribuidores: Desenvolver ou adaptar um processo de análise dos produtos em conformidade com as normas e medidas de segurança exigidas pelo Regulamento;
- Estabelecer protocolos e processos de notificação e partilha de informações sobre ameaças, riscos e vulnerabilidades associadas aos produtos digitais;
- Rever/desenvolver políticas e procedimentos de atualização e monitorização contínuas dos produtos digitais e assegurar a capacidade de deteção, resposta e erradicação de riscos quando estes surjam nos produtos;
- Estabelecer procedimentos de resposta a incidentes à autoridade de supervisão competente, com critérios, classificação e conteúdos de notificação definidos.

Cibersegurança | Legislação

Regulamento da Ciber-Resiliência | Incumprimento

Incumprimento dos **requisitos essenciais de cibersegurança** estabelecidos no anexo I e dos artigos 13.º e 14.º:

- coimas até € 15 milhões ou, se for uma empresa, até 2,5% do seu volume de negócios anual total a nível mundial no exercício anterior.

Incumprimento de obrigações impostas aos **fabricantes**, **importadores** e **distribuidores**, de disposições relativas à declaração de conformidade e aposição da marcação CE, à documentação técnica, à avaliação de conformidade e ao acesso a dados e documentação:

- coimas até € 10 milhões ou, se for uma empresa, até 2% do seu volume de negócios anual total a nível mundial no exercício anterior.

Prestação de **informações incorretas ou enganadoras** aos organismos notificados e às autoridades de fiscalização do mercado:

- coimas até € 5 milhões ou, se for uma empresa, até 1% do seu volume de negócios total a nível mundial no exercício anterior.

Cibersegurança | Declaração Conjunta UE-EUA

Declaração Conjunta UE-EUA sobre o Plano de Ação para Produtos Ciber-Seguros

O Plano de Ação UE-EUA em Cibersegurança e **IoT** para o Consumo visa fortalecer a cooperação transatlântica em cibersegurança, especialmente no contexto da Internet das Coisas (IoT) e dos produtos de consumo.

Este plano reconhece a crescente interconexão dos dispositivos IoT e a necessidade de garantir que esses dispositivos sejam seguros e resilientes contra ciberataques. A colaboração entre a União Europeia e os Estados Unidos é vista como essencial para estabelecer normas e práticas comuns que possam ser adotadas globalmente, promovendo um ambiente digital mais seguro para consumidores e empresas.

ACTION POINTS

- Desenvolver e implementar normas de segurança específicas para dispositivos IoT, em colaboração com fabricantes e reguladores, que incluam requisitos como autenticação, criptografia e atualizações automáticas, garantindo a segurança dos dispositivos durante todo o seu ciclo de vida;
- Desenvolver guias práticos para fabricantes, fornecedores e consumidores;
- Estabelecer mecanismos de cooperação transatlântica para a partilha de informações em tempo real sobre ameaças, vulnerabilidades e ciberataques, permitindo uma resposta rápida e coordenada a incidentes de segurança;
- Investir em pesquisa e desenvolvimento entre a UE e os EUA para fomentar tecnologias avançadas de cibersegurança aplicáveis a dispositivos IoT e infraestruturas digitais, fortalecendo a competitividade tecnológica.

Cibersegurança | Previsão **2025**

01

Resiliência operacional digital do setor financeiro (DORA)

As entidades abrangidas devem estar em pleno cumprimento com este Regulamento a partir de 17 de janeiro de 2025.

As empresas deverão ter, entre outras medidas, sistemas e processos rigorosos para identificar, proteger, detetar, responder e recuperar de incidentes cibernéticos, e garantir a continuidade dos serviços críticos, mesmo em situações de disrupção significativa, mantendo uma comunicação transparente com os clientes e partes interessadas sobre a sua resiliência operacional.

Espera-se que o Regulamento DORA promova um ambiente financeiro mais seguro e resiliente, reduzindo os riscos associados a falhas tecnológicas e ciberataques, tanto das entidades financeiras como dos seus prestadores de TIC.

02

Regulamento sobre Cibersolidariedade

Prevê-se a promoção da colaboração entre empresas e as autoridades nacionais, através da partilha de informações e recursos para melhorar a resposta a incidentes. A criação de uma infraestrutura pan-europeia de Centros de Operações de Segurança (*SOCs*) e a implementação de um Mecanismo de Emergência de Cibersegurança serão relevantes para garantir uma resposta coordenada e eficaz às ameaças, assegurando a continuidade dos serviços críticos e a proteção de dados sensíveis.

03

Transposição da Diretiva NIS2

A transposição da NIS2 exigirá que as entidades abrangidas implementem medidas rigorosas de segurança das redes e da informação, incluindo a gestão eficaz do risco, adaptada ao setor de atividade e nível de exposição.

O CNCS disponibilizará, ao longo de 2025, ferramentas de suporte à análise de risco e de outras medidas de segurança obrigatórias. Espera-se também que o Quadro Nacional de Referência para a Cibersegurança seja atualizado, permitindo um maior suporte na implementação das medidas de segurança exigidas pela NIS2. A colaboração com autoridades nacionais e a comunicação transparente sobre incidentes de segurança serão cruciais para a conformidade com a NIS2.

Publicidade e Consumo

O ano de 2024 será lembrado como um marco significativo no campo da publicidade e consumo, especialmente no que diz respeito ao seu desenvolvimento e regulamentação à luz do **mercado único digital**. Num contexto de avanços tecnológicos e mudanças nos hábitos de consumo, a União Europeia tomou a dianteira na criação de um **quadro legal e ético para o uso responsável** dessas práticas, sublinhando o seu compromisso com a inovação segura e sustentável, assim como a publicidade responsável.

Com a implementação da **nova Diretiva relativa à responsabilidade por produtos defeituosos**, juntamente com o Regulamento dos Serviços Digitais (***Digital Services Act***), a União Europeia consolida a sua posição como líder global na regulação de práticas de consumo, acompanhando a inovação nas várias fases da sua evolução. Adicionalmente, transitamos para um quadro legislativo ecologicamente consciente, em linha com a estratégia ambiental adotada pela União Europeia nos últimos anos, com a **revisão do regime das reparações** e com a criação de **novos deveres de informação e práticas comerciais desleais** que visam trazer mais transparência às alegações publicitárias, facilitando a decisão de compra informada por parte do consumidor.

À medida que avançamos para 2025, as previsões indicam um ano de transição regulatória e crescente adoção **de práticas comerciais inovadoras** em setores estratégicos. É essencial que as transposições para a legislação portuguesa sejam rigorosas e equilibradas, com regras claras e objetivas que permitam uma aplicação eficaz das referidas normas. A nova legislação deve procurar **equilibrar a segurança dos produtos**, a **sustentabilidade** e a **capacidade de adaptação das empresas**, tendo em conta os direitos dos consumidores e os progressos tecnológicos, de forma a criar um mercado justo e dinâmico.

Consumo | Legislação

Regulamento para a Conceção de Produtos Sustentáveis

O Regulamento de Conceção Ecológica para Produtos Sustentáveis integra um conjunto de medidas essenciais para alcançar os objetivos estabelecidos pelo Plano de Ação para a Economia Circular de 2020. De modo geral, o Regulamento visa aumentar substancialmente a circularidade, a eficiência energética e diversos outros aspetos da sustentabilidade ambiental dos produtos comercializados no mercado europeu.

Ver o nosso Legal Flash: *Publicação do Regulamento europeu de conceção ecológica*

Entrada em vigor — 18 de julho 2024 ▶ — Aplicação do Regulamento

Diretiva da Transição Ecológica dos Produtos

Esta Diretiva vem alterar algumas das principais Diretivas do Direito do Consumo, criando novas práticas comerciais desleais e novos requisitos de informação que ambicionam aumentar a transparência nas comunicações ao consumidor. As medidas impostas pela presente Diretiva impõem restrições à publicidade dos produtos e serviços, à rotulagem e às alegações de responsabilidade quando o consumidor decide incorporar peças ou acessórios de terceiros.

Ver o nosso Post: *Alterações às diretivas do consumo para prevenção do ecobranqueamento*

Entrada em vigor — 26 de março 2024 ▶ 9 de dezembro 2026 — Limite para transposição

ACTION POINTS

- Adotar práticas de design que aumentem a durabilidade, reparabilidade e reciclabilidade dos produtos;
- Desenvolver sistemas para rastrear a origem dos materiais e componentes utilizados e fornecer informações claras e acessíveis sobre a sustentabilidade dos produtos aos consumidores;
- Investir em tecnologias que reduzam o consumo de energia durante a produção e implementar medidas para diminuir as emissões de carbono ao longo do ciclo de vida do produto.

- Alterar os termos e condições para cumprir os novos requisitos de informação;
- Rever as comunicações publicitárias para evitar práticas comerciais desleais;
- Rever as alegações inseridas na rotulagem dos produtos.

Consumo | Legislação

Diretiva para a Promoção de Reparação de Bens

A Diretiva (UE) 2024/1799 que vem alterar as obrigações de reparação dos fabricantes e vendedores, em caso de defeito em bens vendidos a consumidores.

Ver o nosso Post: *UE impõe novas obrigações de reparação a fabricantes e vendedores*

Entrada em vigor: 30 de julho 2024 ▶ 31 de julho 2026 — Limite para transposição

Diretiva sobre responsabilidade por produtos defeituosos - Adaptação aos Avanços Tecnológicos

A Diretiva (UE) 2024/2853 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, substitui a Diretiva 85/374/CEE, atualizando o regime de responsabilidade por produtos defeituosos para incluir avanços tecnológicos como a inteligência artificial, novos modelos de negócio da economia circular e cadeias de abastecimento globais. A diretiva amplia o conceito de "produto" para incluir software e produtos digitais, reforça a responsabilidade dos fabricantes e operadores económicos, como importadores e distribuidores, e estabelece um regime de responsabilidade objetiva. Além disso, enfatiza a transparência e rastreabilidade na cadeia de fornecimento, exigindo registos detalhados para facilitar a identificação e retirada de produtos defeituosos, promovendo práticas comerciais mais responsáveis e seguras.

Ver o nosso Post: *Nova Diretiva relativa à responsabilidade por produtos defeituosos*

Entrada em vigor: 8 de dezembro 2024 ▶ 9 de dezembro 2026 — Limite para transposição

ACTION POINTS

- Alterar os termos e condições para garantir o cumprimento das novas regras;
- Rever os procedimentos de resposta a reclamações / exercício de direitos dos consumidores;
- Preparação do formulário europeu de informações sobre as reparações

- As empresas devem implementar procedimentos de monitorização e atualização contínua do software para identificar e corrigir vulnerabilidades nos seus produtos;
- As empresas devem documentar e manter registos detalhados que documentem a conformidade dos produtos com os requisitos de segurança nacionais e da UE;
- As empresas devem desenvolver planos de resposta a incidentes que detalhem os procedimentos a serem seguidos em caso de falhas de segurança ou defeitos nos produtos.

Consumo | Legislação

Regulamento relativo à Segurança Geral dos Produtos

O Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho relativo à segurança geral dos produtos estabelece regras essenciais em matéria de segurança dos produtos de consumo disponibilizados no mercado e que visa responder aos avanços tecnológicos recentes, à crescente globalização dos mercados e cadeias de fornecimento, e ao aumento das vendas à distância e online.

Entrada em vigor		Data de aplicação
30 de maio 2023	▶	13 de dezembro 2024

ACTION POINTS

- Garantir que os produtos disponibilizados estão em conformidade com o requisito geral de segurança;
- Utilizar as plataformas *Safety Gate* e *Safety Business Getaway* para disponibilizar informações relacionadas com a segurança dos produtos;
- Cumprir e garantir que os operadores económicos com quem contratam cumprem as obrigações de informação aos consumidores.

Consumo | Previsão **2025**

01

Transposição da Diretiva da Capacitação dos Consumidores para a Transição Ecológica dos Produtos

A transposição da Diretiva da **Capacitação dos Consumidores para a Transição Ecológica dos Produtos** para o ordenamento jurídico português, em princípio, prevista para 2025, trará mudanças significativas nas práticas comerciais e na proteção dos consumidores.

As empresas terão que ajustar suas **estratégias de marketing e publicidade** para evitar alegações enganosas sobre características ambientais e sociais dos produtos, sendo proibidas alegações não comprovadas.

Será necessário fornecer provas concretas para qualquer alegação ambiental e informações claras sobre **durabilidade**, **reparabilidade** e **atualizações** dos produtos que colocam no mercado, assim como maior transparência sobre garantias e serviços pós-venda (incluindo comunicação de opções de entrega ambientalmente respeitadoras)

Essas mudanças exigirão adaptações internas e investimentos em certificações, assim como para a sensibilização e formação dos colaboradores envolvidos nestes processos.

02

Transposição da Diretiva para a Promoção de Reparação de Bens

A transposição da Diretiva para a **Promoção de Reparação de Bens** para o ordenamento jurídico português, expectante para 2025, trará mudanças significativas nas obrigações de reparação dos fabricantes e vendedores.

A Diretiva exige aos vendedores o **dever de informar** os consumidores do seu direito de escolher entre a **reparação e a substituição**, e da extensão do período de responsabilidade por mais 12 meses, se o consumidor optar pela reparação.

Os fabricantes deverão reparar determinados bens e divulgar preços indicativos de reparação nos seus websites, além de fornecer peças sobresselentes e ferramentas a preços acessíveis.

É criada a figura legal do reparador para facilitar o acesso a serviços de reparação qualificados e eficientes, de forma a promover a sustentabilidade e a responsabilidade circular pelos produtos colocados no mercado.

Conclusões

Inteligência Artificial

A entrada em vigor do Regulamento da IA e a criação do European Artificial Intelligence Office reforçaram a posição da Europa como líder global na regulação de sistemas de IA. As empresas devem estar atentas às novas obrigações e sanções substanciais em caso de incumprimento, além de garantir a conformidade com as recomendações da AEPD e da OECD.

Propriedade Intelectual

A modernização do sistema de proteção de desenhos industriais e as medidas para combater a contrafação destacam-se como avanços importantes.

As empresas devem adaptar-se às novas regras de registo e adotar tecnologias avançadas para proteger os seus direitos de PI.

Privacidade e Proteção de Dados

A consolidação dos conceitos e métodos de recolha e tratamento de dados pessoais, juntamente com as orientações do CEPD e as decisões judiciais, sublinham a importância crescente da conformidade com o RGPD. As empresas devem garantir a transparência e a segurança no tratamento de dados pessoais, especialmente em transferências internacionais.

Telecomunicações e Tecnologia

A Estratégia Digital Nacional de Portugal e a decisão do Tribunal Constitucional sobre as taxas da ANACOM são marcos importantes.

As empresas devem estar preparadas para as mudanças regulatórias e aproveitar as oportunidades de inovação tecnológica.

Cibersegurança

O Regulamento DORA e o Regulamento da Ciber-Resiliência estabelecem normas harmonizadas de cibersegurança para produtos digitais.

As empresas devem rever e atualizar as suas políticas de segurança e procedimentos de resposta a incidentes para garantir a resiliência operacional.

Publicidade e Consumo

A Diretiva relativa à Responsabilidade por Produtos Defeituosos e o Regulamento dos Serviços Digitais reforça a posição da UE na regulação de práticas de consumo.

As empresas devem adotar práticas comerciais transparentes e sustentáveis, garantindo a segurança dos produtos e a proteção dos consumidores.

As previsões para o ano de 2025 apontam para uma transição regulatória e crescente adoção de práticas inovadoras em setores estratégicos.

É essencial que as empresas se adaptem às novas exigências jurídicas e tecnológicas, garantindo a conformidade e a competitividade no mercado europeu.

O que oferecemos

Prestamos assessoria em todas as áreas do Direito empresarial e ajudamos os nossos clientes nos assuntos mais exigentes, em qualquer território, fornecendo a experiência e o conhecimento de equipas especializadas.

29
Especialidades jurídicas

+2000
Profissionais

26
Escritórios em 12 países

29
Nacionalidades & 16 línguas

+300
Professores & 9 catedráticos

26%
Mulheres em cargos de direção

FT INNOVATIVE LAWYERS EUROPE 2024 WINNER

Sociedade mais inovadora da Europa em "Talent management", 2024

Sociedade mais inovadora da Europa continental, 2023

Máxima presença na Península Ibérica
2 escritórios em Portugal e 13 em Espanha

THE LAWYER

Highly commended na Península Ibérica, 2024

Sociedade do ano na Europa e na península ibérica, 2022

RepScore 2024

2.º posição no índice de reputação OnStrategy, 2023-24

Enfoque na América Latina
Escritórios no Chile, Colômbia, México e Perú
Mais de 20 anos de experiência no mercado da América Latina

Escritórios em Bruxelas, Casablanca, Londres, Luanda*, Nova Iorque, Pequim e Xangai
4 desks internacionais
Rede europeia com sociedades líderes na Alemanha, França e Itália

*em colaboração com sociedades de advogados locais.

- Visão sectorial adaptada a cada tipo de negócio.
- Máxima especialização combinada com tecnologia de ponta.
- Relações de longa duração com os nossos clientes, que vão além do âmbito jurídico.

CUATRECASAS ESG

Cumprimos critérios ambientais, sociais e de bom governo (ESG) na prestação dos nossos serviços e na nossa gestão interna.

Aqui detalhamos os principais parâmetros com que medimos o nosso desempenho em termos de ESG.

Consulte também a nossa última Memória Empresarial.

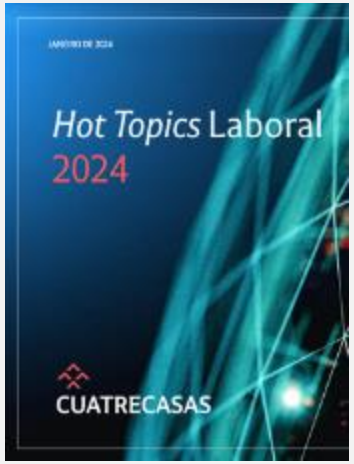
GOLD 2023 ecovadis

Guias práticos

Este ano, as nossas equipas publicaram diversos guias práticos sobre desenvolvimentos jurídicos e tendências de mercado. Pode aceder a todos os guias através dos seguintes ícones:

Regulamento (UE) IA

Hot Topics Laboral 2024



Guia Simplex Urbanístico

Plano de ação para inspeções da AdC

Proposta de Lei OE 2025

Key Contacts

Joana Mota Agostinho
Sócia | Proteção de Dados | Tecnologias e Meios Digitais (TMT)

Ver CV
joana.agostinho@cuatrecasas.com

Sónia Queiroz Vaz
Sócia | Propriedade Intelectual, Industrial e Segredos | Proteção de Dados

Ver CV
sonia.queiroz.vaz@cuatrecasas.com

A informação contida nesta apresentação foi obtida de fontes gerais, é meramente expositiva, e tem de ser interpretada juntamente com as explicações que a acompanham. Esta apresentação não pretende, em nenhum caso, constituir uma assessoria jurídica.

La información contenida en esta presentación se ha obtenido de fuentes generales, es meramente expositiva, y se debe interpretar junto con las explicaciones que la acompañan. Esta presentación no pretende constituir en ningún caso un asesoramiento jurídico.

The information provided in this presentation has been obtained from general sources. It is for guidance purposes only and should be interpreted in relation to the explanations given. This presentation does not constitute legal advice under any circumstances.

CUATRECASAS