

SHOOSMITHS

Global privacy and data update

February 2025

www.shoosmiths.com

FOR
WHAT
MATTERS



Legislation



Guidance & consultations



Enforcement & legal action

THE **BIG** STORY



Apple withdraws UK advanced encryption following IPA notice

21 FEBRUARY 2025



Industry & sector news



INDEX

Quick read: what you need to know about February 2025

Cybersecurity

Apple withdraws its advanced UK encryption service after the government issues a notice under new IPA powers.

The ESAs confirm the DORA timetable to designate critical third-party suppliers to financial entities.

The Spanish Data Protection Authority publishes decisions fining twenty banks in a group following cyberattacks.

New laws

The White House issues an Executive Order to stop action by US regulators.

Mexico removes the national data protection regulator and overhauls its transparency and data protection rules.

Claimants bring at least 12 Privacy Act claims for permitting DOGE access to records.

AI

The European Commission withdraws the AI Liability Directive and ePrivacy reforms, and publishes guidance on prohibited AI practices and guidelines on “AI systems” under the EU AI Act.

Virginia becomes the second US state to pass a comprehensive law regulating AI systems.

The AI Office holds a webinar on AI literacy attended by around 1,500 organisations.

Tracking

Google lifts its ban on device fingerprinting from 16 February 2025.

The CJEU upholds EDPB decisions demanding €390m fines and further investigation of Meta targeted advertising.

A US Court of Appeals upholds the \$725m settlement for users harmed by Cambridge Analytica profiling.

Online safety

A Dutch group brings class actions against TikTok and X under the Digital Services Act.

The Australian Commissioner fines Telegram AUD967,000 for late reporting under online safety laws.

A CJEU Advocate General opines on the liability of “hosting services”.

Fines and legal action



The Austrian DSB fines a health company for appointing its managing director as DPO.

The South Korean PIPC fines payment providers €5.5m and orders destruction of a financial scoring model for consent failures.

The CJEU issues its ruling on calculating GDPR fines for controllers within a group and a new ruling on automated decision making.

Index

Legislation

9	 Commission withdraws ePrivacy and AI Liability reforms.....	EU
10	 Germany delays transposition of NIS2.....	EU (Germany)
11	 Mexico overhauls transparency and data protection laws.....	MEXICO
12	 Commission rejects draft RTS under DORA.....	EU
13	 LIBE Committee asks Commission to review EU/US DPF.....	EU/US
14	 DUA Bill goes to second reading in House of Commons.....	UK
15	 White House issues Executive Order to stop regulatory action.....	US
16	 Virginia becomes second state to pass comprehensive AI law.....	US (Virginia)

Key:

- General 
- Accountability & governance 
- Commercialisation & competition 
- Data rights 
- Marketing, adtech & cookies 
- Artificial intelligence 
- Law enforcement & intelligence 
- Cybersecurity 
- Sensitive data & vulnerable individuals 
- Transfers 

Index

Guidance & consultations























18	 DSIT publishes first International AI safety report.....	UK
19	 AP publishes guidance on AI literacy.....	EU (Netherlands)
20	 DSIT announces code of practice for AI cybersecurity.....	UK
21	 AI Office publishes AI literacy digest.....	EU
22	 Commission publishes guidance on prohibited AI.....	EU
23	 ICO publishes direct marketing advice generator.....	UK
24	 ICO publishes guidance on employment records.....	UK
25	 OECD launches global framework for AI safety.....	GLOBAL
26	 CNIL publishes recommendations on AI and GDPR.....	EU
27	 Commission issues guidelines on “AI systems” under AI Act.....	EU
28	 Government releases AI playbook for public sector.....	UK
29	 EDPB adopts statement on age assurance.....	EU
30	 Parliament calls for evidence on DUA Bill.....	UK
31	 Commission endorses DSA code on disinformation.....	EU
32	 ESAs confirm DORA timetable for critical suppliers.....	EU
33	 AI Office holds AI literacy webinar.....	EU
34	 ICO issues Tech Horizons 2025.....	UK
35	 Commission proposes blueprint for large scale cyber attacks.....	EU

Key:











- General 
- Accountability & governance 
- Commercialisation & competition 
- Data rights 
- Marketing, adtech & cookies 
- Artificial intelligence 
- Law enforcement & intelligence 
- Cybersecurity 
- Sensitive data & vulnerable individuals 
- Transfers 

Index

Enforcement & legal action







37	 DPAs issue fines for monitoring employees.....	EU (Italy/France)
38	 DPA fines controller €70,000 for circulating contracts.....	EU (Spain)
39	 DPA fines hospital for unlawful surveillance.....	EU (Poland)
40	 AEPD fines banking group after cyber-attack.....	EU (Spain)
41	 DSB fines health company for appointing the MD as DPO.....	EU (Austria)
42	 AEPD fines insurance company €5m for inadequate security.....	EU (Spain)
43	 Court finds land registry numbers are personal data.....	EU (Poland)
44	 CJEU upholds EDPB rulings on Meta.....	EU
45	 Garante orders investigation into DeepSeek AI.....	EU (Italy)
46	 ICO gets leave to appeal Clearview AI decision.....	UK
47	 Garante announces €890,000 fine for unwanted telemarketing.....	EU (Italy)
48	 SOMI brings class action against TikTok and X under DSA.....	EU (Germany)
49	 AG gives opinion on pseudonymisation.....	EU
50	 Advocate General opines on liability of “hosting services”.....	EU
51	 PIPC fines payment providers €5.5m and orders model destruction.....	SOUTH KOREA
52	 CJEU confirms that GDPR fines cover group undertakings.....	EU
53	 Court of Appeals confirms \$725m Cambridge Analytica settlement.....	US
54	 CJEU receives referral on interpretation of EU AI Act.....	EU
55	 Data protection authorities investigate DeepSeek.....	GLOBAL
56	 Commissioner fines Telegram AUD967,000 under Online Safety Act.....	AUSTRALIA
57	 Claimants open legal actions against DOGE under Privacy Act.....	US
58	 CJEU rules on DSAR information required for automated decisions.....	EU

Key:

General	
Accountability & governance	
Commercialisation & competition	
Data rights	
Marketing, adtech & cookies	
Artificial intelligence	
Law enforcement & intelligence	
Cybersecurity	
Sensitive data & vulnerable individuals	
Transfers	

Index

Industry & sector news

60	 Meta publishes Frontier AI Framework.....	US
61	 Ransomware report finds payments drop significantly.....	GLOBAL
62	 Google lifts ban on device fingerprinting.....	GLOBAL
63	 App Store removes apps not complying with DSA.....	EU
64	 WhatsApp reaches VLOP threshold under the DSA.....	EU
65	 Apple withdraws UK advanced encryption following IPA notice	UK

Key:

- General 
- Accountability & governance 
- Commercialisation & competition 
- Data rights 
- Marketing, adtech & cookies 
- Artificial intelligence 
- Law enforcement & intelligence 
- Cybersecurity 
- Sensitive data & vulnerable individuals 
- Transfers 



Legislation



Commission withdraws ePrivacy and AI Liability reforms

29 January 2025

Key details

The European Commission has announced its work programme for 2025. The programme includes withdrawal of the proposed AI Liability Directive, apparently in concession to US tech interests. The Directive was designed to harmonise fault-based civil liability for AI systems. It is also abandoning the planned update to the ePrivacy Directive governing cookies and tracking, started in 2017, due to “no foreseeable agreement” and being “outdated”.

The programme includes the following proposed new laws and plans:

- improving cross-border digital infrastructure (Digital Networks Act)
- promoting investment in AI gigafactories and setting standards for cloud services in the EU (Cloud and AI Development Act)
- improving AI capability (AI Factories and Apply AI strategy)
- preserving strategic sovereignty over quantum tech (EU Quantum Strategy and Quantum Act)
- creating a “28th legal regime” to harmonise corporate, insolvency, employment, and tax laws for selected innovative companies (the Competitiveness Compass, and the Innovation Act).

These initiatives are expected to be implemented between Q4 2025 and Q1 2026.

Links to further information

[Work programme 2025](#)

[Annex](#) (including withdrawals)

SHOOSMITHS SAYS...

The Commission refusing liability.



Germany delays transposition of NIS2

30 January 2025

Key details

The German implementation of EU laws to increase cybersecurity in critical infrastructure, the NIS2 and CER Directives, has been delayed by the dissolution of the government and the general election on 23 February 2025 following the collapse of negotiations between the governing parties, the so-called “traffic light coalition”.

The country missed the 17 October 2024 transposition deadline and is the subject of ongoing formal procedures by the Commission. The previous government instituted a draft law, but this is likely to be modified by the next federal government. Adoption of the new law is expected by Q3 2025 at the earliest, leaving companies in an uncertain position over compliance.

Although most other member states missed the deadline, the major economies are largely on track to agree and implement the required laws without significant further delay.

In the meantime, Romania completed its national implementation of the NIS2 Directive on 30 January 2025 with the adoption of Government Emergency Ordinance no. 155/2024. The National Cyber Security Directorate (DNSC) is designated as the competent authority.

Links to further information

[Romania press release](#)

SHOOSMITHS SAYS...

Traffic lights stuck at red.



Mexico overhauls transparency and data protection laws

31 January 2025

Key details

The government of Mexico has announced the removal of the national data protection regulator, the National Institute for Access to Information and Protection of Personal Data (NAIH), and allocation of its responsibilities across various agencies, including “Transparency for the People”, the Anti-Corruption and Good Government Secretariat, and 16 new bodies embedded in federal institutions, autonomous bodies, and political parties.

It also plans to reform legislation on transparency and data protection.

The proposed reforms will first be reviewed by the Senate before moving to the Chamber of Deputies.

This move is apparently motivated by cost-cutting but concerns have been raised about the lack of independence and impartiality in the new system, particularly in view of direct government control over public information leading to reduced transparency and potential manipulation of government data.

SHOOSMITHS SAYS...

Interesting times for the US’s biggest trading partner.

Links to further information

[Press release](#)



Commission rejects draft RTS under DORA

31 January 2025

Key details

The European Commission has rejected the draft Regulatory Technical Standards (RTS) on subcontracting ICT services under the Digital Operational Resilience Act (DORA), which took effect on 17 January 2025. This rejection leaves financial entities in an uncertain position over this aspect of DORA compliance.

The standards will apply to “critical” third-party providers of ICT services, including cloud computing services, software, data analytics, and data centres, which serve in-scope financial entities. The draft RTS sets out how financial entities should manage and assess risks when subcontracting these ICT services for critical functions, including pre-contractual due diligence and contract management.

The Commission objection is based on alleged overreach by the European Supervisory Authorities (ESAs), and in particular the requirement in Art. 5 of the draft RTS to oversee the entire supply chain. The Commission’s position is that this exceeds their powers under Art. 30(5) of DORA by introducing conditions unrelated to subcontracting. The ESAs have six weeks to respond to the Commission request for removal.

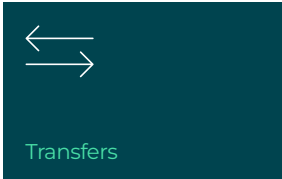
Links to further information

[Commission letter](#)

[Draft RTS](#)

SHOOSMITHS SAYS...

Evidence of more DORA friction between the Commission and the ESAs.



LIBE Committee asks Commission to review EU/US DPF

6 February 2025

Key details

The European Parliament LIBE Committee has written formally to the European Commission asking it to review the “essential equivalence” of US data protection law following the dismissal of three members of the US oversight committee, the PCLOB, which forms a key element of the EU/US adequacy decision, the Data Privacy Framework (DPF).

The letter has not been published but the Committee has confirmed sending it in its minutes, linked.

The legality of the EU/US DPF data transfer mechanism is currently the subject of a legal challenge in the CJEU, *Latombe v Commission*, brought by a French MP. An application for interim relief to suspend the framework was rejected in October 2023, but the case remains open. The court has not yet set a date for the main hearing.

SHOOSMITHS SAYS...

The US adequacy decision continues its slow-motion journey over the cliff.

Links to further information

[Minutes](#)



DUA Bill goes to second reading in House of Commons

12 February 2025

Key details

The UK Data (Use and Access) Bill has completed its first two readings in the House of Commons after passing its third reading in the Lords. The bill is expected to progress quickly and may become law by mid-2025.

The bill reforms various aspects of UK data protection legislation and proposes increased flexibility on legitimate interests for data processing, processing for scientific research, purpose compatibility, DSAR response times, cookie consent, and automated decision-making.

The ICO has also published its response to the bill following amendments in the Lords. It largely supports the current proposals, though with ongoing concerns which include diluting underlying data protection principles for over 18s, the extension of soft-opt in rights to charities when direct marketing, and removal of the general prohibition on automated decision-making. It also notes the Lords' proposal for the ICO to regulate the transparency of web crawler use, to allow rights holders to assert and enforce copyright.

A private members' bill on AI in the public sector has also passed through the House of Lords and into the Commons. The Public Authority Algorithmic and Automated Decision-Making Systems Bill, introduced on 9 September 2024, would regulate automated decision-making in the public sector by requiring impact assessments, transparency standards, monitoring, and audits. It is not clear whether it will progress.

Links to further information

[Bill](#)

[ICO response](#)

SHOOSMITHS SAYS...

DUA leaper.



White House issues Executive Order to stop regulatory action

19 February 2025

Key details

The White House has issued an Executive Order requiring the new heads of federal agencies to identify any regulations which they deem unconstitutional, unlawful or unduly burdensome, or which unjustifiably impede technological innovation, with a view to rescission or modification.

The agencies have also been ordered to stop civil or criminal enforcement proceedings that do not comply with the constitution, laws, or “Administration policy”.

The effect of the Order, which may be subject to legal challenge, is not yet clear, but it will probably cause some enforcement action underway by bodies such as the Federal Trade Commission, Federal Communications Commission and the Securities and Exchange Commission to be paused pending the regulatory review and clarification of the legal position.

WHAT THEY SAY...

“the deconstruction of the overbearing and burdensome administrative state”

Links to further information

[Executive Order](#)

[Fact sheet](#)



Virginia becomes second state to pass comprehensive AI law

19 February 2025

Key details

The legislature of Virginia has passed the High-Risk Artificial Intelligence Developer and Deployer Act (House Bill 2094) regulating the use of AI systems in the state.

The definition of AI system in the Act is largely taken from the EU AI Act. The law will cover developers of high-risk AI systems doing business in the state and deployers of such systems who make a “consequential decision” in the state in respect of incarceration, education, housing or employment, or financial, lending, legal, insurance, or healthcare services. There are provisions to exempt certain services which are already subject to other legislation.

In-scope developers have transparency requirements, and deployers are subject to a duty of care towards consumers and must perform risk assessments as part of a risk management programme.

The Act is subject to approval by the state governor. If passed it is due to come into force on 1 July 2026. It will be enforceable only by the Attorney General and subject to a cure period of 45 days.

The Act would be broadly comparable to laws already passed in Colorado governing the use of AI systems across various sectors. Fourteen states have similar laws under consideration. Utah and California have passed laws requiring AI labelling, and there are various sector-specific AI laws also passed in several states.

Links to further information

[Bill tracker](#)

SHOOSMITHS SAYS...

As with privacy laws, some US states developing their own fragmented laws on AI.



Guidance & consultations



DSIT publishes first International AI safety report

29 January 2025

Key details

The UK's Department for Science, Innovation and Technology (DSIT) has published the first independent International AI Safety Report which contains a global scientific assessment of advanced AI risks. The report, developed with input from experts across 30 countries, together with the UN, EU, and OECD, focuses on general-purpose AI (GPAI), and has been released in preparation for the third AI Action Summit in France in February 2025. It does not contain policy recommendations, only current risks and mitigation strategies.

It notes that in the past few months the emergence of more powerful models, in particular Open AI o3 (which has not been publicly released) has increased risks relating to energy use, the labour market and loss of control. It highlights particular risks arising from development of "AI agents" which are instructed to achieve goals autonomously. It also notes that "developers still understand little about how their general-purpose AI models operate".

It also concludes that risk mitigation strategies are developing but not yet effective, and that privacy-enhancing methods from other research fields are not yet applicable to GPAI due to computational requirements.

Links to further information

[Press release](#)

[International AI safety report](#)

WHAT THEY SAY...

"the global handbook on AI safety"

Jurisdiction: **EU (Netherlands)**



AP publishes guidance on AI literacy

30 January 2025

Key details

The Dutch Data Protection Authority (the AP) has issued the first member state guidance on the AI literacy requirements in Art. 4 of the EU AI Act. Developers and deployers of AI systems where output is used in the EU must ensure that staff have the necessary skills to operate AI systems responsibly by 2 February 2025.

The guidance outlines a multi-year plan for organisations which is wider than strict literacy goals, and involves AI mapping, identifying key roles, prioritising risks, training, governance policies, monitoring, and ongoing evaluation.

WHAT THEY SAY...

“AI literacy is not an end goal, but a continuous process”

Links to further information

[Press release](#)

[Guidance](#) (Dutch only)



DSIT announces code of practice for AI cybersecurity

31 January 2025

Key details

The UK government has announced a new code of practice for AI cybersecurity which will be submitted as a global standard through the European Telecommunications Standards Institute (ETSI).

The code covers the entire AI lifecycle, including staff awareness, secure development, human oversight, testing, and end-of-life disposal. It comes with an implementation guide with practical steps, examples and links to further resources.

At the same time, the government announced its response to the public consultation on a new Code of Practice on Cyber Governance, which aims to help all organisations embed cybersecurity knowledge and practice at board level. It is designed for organisations of at least 50 people and those providing critical services. The government says it will publish the final code in early 2025, and will clarify how the code relates to cyber resiliency rules in the upcoming Cyber Security and Resilience Bill.

WHAT THEY SAY...

“a world-first cyber security standard”

Links to further information

[Press release](#)



AI Office publishes AI literacy digest

4 February 2025

Key details

The EU Commission has published a digest of practices by fifteen participants in the AI Pact, providing practical examples of approaches to AI literacy in various sectors across industry. The examples come from companies operating in insurance, online booking, healthcare, ICT, construction and energy.

SHOOSMITHS SAYS...

Participants in the AI Pact teaching a lesson in AI literacy.

Links to further information

[Press release](#)



Commission publishes guidance on prohibited AI

4 February 2025

Key details

The Commission has published the first guidelines on prohibited AI practices under Art. 5 of the EU AI Act, applicable from 2 February 2025.

The guidance requires each party in the supply chain to take the measures to ensure responsible use “for which they are best placed”. It notes that harms often arise from how AI systems are used in practice, and that providers have responsibility not to put on the market or into service systems which are likely to be used in a prohibited manner (para 40). As well as design and contractual measures, they are also expected to “take appropriate measures” if they know of misuse by customers.

Sections 3 and 4 of the guidance cover the prohibitions most likely to affect commercial use. They cover manipulative and exploitative techniques such as subliminal advertising, and impersonating chatbots, where these are reasonably likely to cause significant harm. Examples include a well-being chatbot which inadvertently encourages over-exercise in

a vulnerable person (84) and a child’s toy which encourages compulsive play through “personalised and unpredictable” rewards. Incidental hallucinations are expressly excluded.

It includes in depth discussion of the difference between “lawful persuasion” and banned manipulative practices in advertising, and analysis of banned “social scoring” techniques, such as the use of unrelated financial information to price insurance premiums (170).

Sections 5 to 10 cover the various prohibited uses of AI systems in law enforcement and related purposes, such as real-time remote FRT and predictive policing.

The Commission notes that legal interpretation can only be determined by the CJEU; however, the guidelines are likely to shape member state regulation of Art. 5.

Although enforcement mechanisms will not be in place until 2 August 2025, the rules are now applicable and are enforceable by affected parties in national courts (432).

WHAT THEY SAY...

“insights into the Commission’s interpretation of the prohibitions”

Links to further information

[Press release](#)

Jurisdiction: **UK**



ICO publishes direct marketing advice generator

5 February 2025

Key details

The UK ICO has launched a new tool designed to give basic advice to SMEs on whether their marketing activities are compliant with relevant data protection laws.

It uses a set of yes/no questions to link users to relevant advice on the ICO website. The tool is under development and the ICO welcomes feedback on how useful it is.

WHAT THEY SAY...

“learn how to market your organisation and use personal information in the right way”

Links to further information

[Press release](#)

[DM advice generator](#)



ICO publishes guidance on employment records

6 February 2025

Key details

The UK Information Commissioner's Office (ICO) has released guidance for employers on managing employment records in compliance with the UK GDPR and the Data Protection Act 2018. It sets out principles which apply to any working relationship including workers in the gig economy, volunteers and contractors.

The guidance looks at various aspects of data protection law which are in play in dealing with workers' records, including identifying an appropriate lawful basis for processing, retention and anonymisation of records, security, and conditions for keeping special category data such as health records.

It provides guidance for specific situations which can cause difficulty, in particular dealing with references, diversity monitoring, pensions, insurance, TUPE transfers, and staff information during mergers and acquisitions.

WHAT THEY SAY...

“a balance between your need to keep employment records and every worker’s right to a private life”

Links to further information

[Guidance](#)



OECD launches global framework for AI safety

7 February 2025

Key details

The OECD has launched the first global framework for company reporting on the development of safe, secure, and trustworthy AI, based on the G7 Hiroshima AI Process for advanced AI systems. It enables companies to make a public declaration about their AI risk management practices to foster trust and accountability in AI development. It could also be used as an internal assessment questionnaire for AI policy.

Developers including Amazon, Google, Anthropic, Microsoft and OpenAI have committed to completing the inaugural framework, which aims to align AI governance across international systems. Companies are encouraged to submit their first reports by 15 April 2025, with annual updates thereafter.

The previous day, the OECD released a policy brief and recommendation on sharing data for AI. It provides a useful overview of the global challenges in accessing data for building AI models and sets out FAIR (findable, accessible, interoperable, and reusable) data principles for trustworthy AI. It notes that UK companies are advanced in the use of big data analytics, but behind competitors in adoption of AI generally.

Links to further information

[Press release](#)

[Sample questionnaire](#)

[Policy brief](#)

[Recommendation](#)

SHOOSMITHS SAYS...

Quiet progress away from the AI shouting match.



CNIL publishes recommendations on AI and GDPR

7 February 2025

Key details

The French data protection authority, the CNIL, has published two guides on AI and the GDPR, to coincide with the AI Action Summit in Paris.

The first guide looks at transparency notices when processing personal data for AI systems, including web scraping. It considers when direct contact with individuals is disproportionate or unnecessary under Art. 14(5)(b) of the GDPR. The second guide focuses on how to ensure that individuals can exercise data protection rights such as access and rectification in the context of AI system development and use. It includes analysis of situations where data subject rights are suspended under Art. 11 where a controller no longer requires identification of data subjects. It takes a more pragmatic stance on some issues than other EU regulators.

Many contributors to the third “AI Action Summit” in Paris emphasised the importance of deregulation of AI. The UK and US, unlike other delegates including China, declined to sign the summit declaration on the grounds of security and innovation.

SHOOSMITHS SAYS...

AI-full tower.

Links to further information

[CNIL press release](#)

[AI privacy notices](#)

[AI data subject rights](#)

[AI Action Summit](#) (French only)



Commission issues guidelines on “AI systems” under AI Act

10 February 2025

Key details

The European Commission has issued draft guidelines which set out its view of the meaning of “an AI system” under Art. 3(1) of the EU AI Act. The definition broadly covers machine systems displaying autonomy and capable of making inferences which generate outputs that can influence physical or virtual environments.

The guidelines discuss each element of the definition to help providers and other relevant parties determine whether a software system qualifies as an AI system. For example, it clarifies that “machine” will include quantum systems, and says that systems must operate “with some reasonable degree of independence of actions” to be in-scope.

It puts out of scope:

- systems for improving the functional operation of other systems, for example used in weather prediction or resource management
- systems which just “present data in an informative way”
- “classical heuristics” models like chess programmes without adaptability and not learning from experience
- “simple prediction systems” used in financial forecasting.

Some of the distinctions are based on acknowledgement that while technically within scope, some AI systems are not powerful or novel enough to require additional regulation.

It also says that “the vast majority” of systems within the meaning of Art. 3(1) “will not be subject to any regulatory requirements under the AI Act” (presumably excepting the provisions in Art. 4 on AI literacy). The Commission reminds readers that the guidelines are non-binding, and that interpretation is determined by the courts, not the Commission. They are likely to evolve over time as new questions and use cases arise.

Links to further information

[Press release](#)

SHOOSMITHS SAYS...

The Commission generating its own output on the AI Act.



Government releases AI playbook for public sector

10 February 2025

Key details

The UK Government Digital Service (GDS) has published an Artificial Intelligence Playbook for the UK Government to support public sector employees in understanding, procuring, and deploying AI solutions. It applies to all public sector bodies, as well as private companies supplying AI solutions to government.

The playbook:

- outlines ten principles for responsible AI use
- explains AI concepts, benefits and limitations in government use
- provides guidance on procuring and developing AI
- highlights legal, ethical, data protection, privacy, and security considerations.

It marks a contrast in emphasis to the recent UK government AI Action Plan by focusing on AI safety rather than economic growth. It is likely to be useful to any organisation supplying into the public sector. The report does not refer to the recently renamed AI Security Institute (UK AISI) whose focus is now the safety of frontier models including weaponised use and cyberattacks.

Links to further information

[Playbook](#)

WHAT THEY SAY...

“you must ensure that AI systems generate a net positive impact”



Sensitive data &
vulnerable individuals

EDPB adopts statement on age assurance

12 February 2025

Key details

The EDPB has adopted a statement setting out guidance on age assurance. It comes a few weeks after Ofcom issued new guidance on age assurance as part of children's risk assessment under the UK Online Safety Act.

Age verification can pose problems from a data protection point of view as it may involve additional processing of information relating to a child which can then be used for tracking or profiling.

The guidance comes in response to increasing legal pressure to implement age assurance, which the EDPB believes is likely to cause security issues. For example, under s. 35(1)(j) of the Digital Services Act, age verification is one of the mitigation measures which very large online platforms and services can take to address specific systemic risks identified in risk assessments of their services.

The EDPB notes the need for a governance framework for organisations undertaking age assurance, and the need to ensure that processing is auditable.

SHOOSMITHS SAYS...

Addressing an
age-old problem.

Links to further information

[Press release](#)

[Statement](#)



Parliament calls for evidence on DUA Bill

13 February 2025

Key details

The UK Parliament's Public Bill Committee has called for evidence from those with relevant expertise and experience, or a special interest, in the UK's data reform bill. This is likely to be the last stage of consideration of the Data (Use and Access) Bill.

The House of Commons report, [linked](#), contains useful summaries of the aims and effect of the bill, and of its recent passage through the House of Lords.

The consultation is open now and closes between 4 and 18 March 2025, depending on how long the Committee takes to conclude its work. The Committee will not be holding oral evidence sessions.

SHOOSMITHS SAYS...

**Speeding along the
DUA carriageway.**

Links to further information

[Call for evidence](#)

[HCL report](#)



Commission endorses DSA code on disinformation

13 February 2025

Key details

The European Commission has endorsed a voluntary code of practice on disinformation under the Digital Services Act (DSA) which will take effect on 1 July 2025.

Established under Arts 45 to 47 of the DSA, codes are voluntary, although refusal to comply by very large platforms and search engines may be taken into account when determining infringement, and adherence may be put forward as a risk mitigation measure (see Recitals 103-104).

The disinformation code includes commitments such as enhancing political advertisement transparency, reducing fake accounts, improving user tools for identifying disinformation, and adequate support for independent fact-checking. Compliance will be subject to annual independent audit.

It joins an existing code on countering illegal hate speech. The Commission is also publicising workshops to develop a code of conduct for online advertising under the DSA and may also develop a code for accessibility.

SHOOSMITHS SAYS...

Meta is a signatory to the Code, which was developed in 2021-2022.

Links to further information

[Press release](#)

[Press release: online advertising](#)



ESAs confirm DORA timetable for critical suppliers

18 February 2025

Key details

The European Supervisory Authorities have confirmed their timetable for the process to designate critical third-party suppliers to financial entities under DORA.

The planned timetable is:

- national authorities will submit information from their registers by 30 April 2025
- the ESAs will use this information to classify and inform potential critical third-party suppliers (CTPPs) by 31 July 2025
- CTPPs will have six weeks to contest registration (until mid-September)
- designation will be confirmed by the end of 2025.

The ESAs will organise an online workshop to help CTPPs in Q2 2025, on a date to be published. Once designated, CTPPs will be subject to a high level of scrutiny including direct regulatory supervision, regular audits, and stringent cyber resilience obligations. The designation is likely to cover the largest cloud and cybersecurity providers. ICT suppliers to the financial sector not designated as critical will still be affected by new mandatory contract requirements, with enhanced requirements for ICT suppliers supporting critical or important functions.

WHAT THEY SAY...

“the objective is to designate the CTPPs and to start the oversight engagement this year”

Links to further information

[Press release](#)



AI Office holds AI literacy webinar

20 February 2025

Key details

The EU AI Office has hosted a webinar on the AI literacy requirements in Art. 4 of the EU AI Act, attended by around 1,500 organisations and other interested parties.

The main concerns of participants were the mechanics of enforcement, extra-territorial effect, and the training requirements in practical terms.

Key takeaways were:

- organisations are required to ensure understanding of AI opportunities as well as risks
- the AI literacy requirement is likely to require new contractual obligations across the supply chain, at least for high-risk systems
- “other persons” included in the duty will be service providers, contractors and customers
- literacy goes “hand in hand” with the other requirements of the Act, so literacy will reflect the nature of the system and the deployment so organisations should take a risk-based approach
- there will not be a certification system for training providers
- “best efforts” does not mean perfection, but is likely to be linked to regularity of engagement
- there is no express documentation requirement although this will be an important demonstration of accountability.

The Commission reminded participants that the obligation does not cover AI models, just AI systems, and that although “private” enforcement for failure to comply is possible from 2 February 2025, “public” enforcement via regulators cannot begin until member states have appointed and established their regulators and penalties, due by 2 August 2025.

Links to further information

[Webinar](#)

“any company using ChatGPT will require AI literacy training”



ICO issues Tech Horizons 2025

20 February 2025

Key details

The ICO has issued its most recent Tech Horizons report which explores emerging technologies likely to pose the greatest challenges from a privacy and data perspective.

The report highlights the following key technologies emerging over the next two to seven years:

- connected transport
- quantum detection and imaging
- digital diagnostics, therapeutics and healthcare infrastructure
- synthetic media.

It identifies three major risks in relation to these technologies:

- new types of information (such as brain patterns)
- information on a huge scale
- complex data sharing arrangements.

The report includes analysis of the data protection risks associated with connected vehicles, including the need for consent to collection founded in the PECRs, and the problems of excessive data collection, biometric data, and information relating to passengers especially if they are children. The report also provides updates on various technologies considered in its previous reports such as health tech, drones and immersive technologies.

“we support innovators to embed safeguards during the design phase”

Links to further information

[Report](#)



Commission proposes blueprint for large scale cyber attacks

24 February 2025

Key details

The European Commission has published an updated draft of its 2017 Cybersecurity Blueprint, designed to explain how member states and institutions should work together in the event of a crisis-level cyber incident.

The draft Council Recommendation complements provisions in NIS 2 which require member states to collect and share information on cyber preparedness within critical infrastructure, and recommends common exercises, taxonomy, and the use of EU-based DNS infrastructure. It also calls for greater co-operation between civilian and military actors, including NATO.

Regarding the European financial services sector, the European Cybersecurity Agency, ENISA, has published its first cybersecurity review. It contains analysis of major threats and incidents in the sector between January 2023 and June 2024. ENISA notes that banks remain key targets, and although ransomware attacks have reduced, major disruption and losses are still caused by malware, most often through phishing and similar attacks. It concludes that adherence to the GDPR, NIS and DORA is “crucial for maintaining cybersecurity resilience”.

Links to further information

[Press release](#)

[Draft recommendation](#)

[ENISA report](#)

SHOOSMITHS SAYS...

Europe preparing to defend itself in the cyber, as well as the physical, sphere.



Enforcement & legal action

Enforcement & legal action

Jurisdiction: **EU (Italy/France)**

DPAs issue fines for monitoring employees

19 December 2024

Key details

The data protection authorities of Italy and France have both imposed fines on employers for breaches of the GDPR related to employee monitoring.

The Garante fined a refuse treatment company €20,000 for keeping logs of browsing activity on work devices for 30 days without properly defining its purposes or complying with national employment law. It also failed to adequately respond to a data subject rights request by simply informing the data subject that the relevant information had been erased. The Garante found breaches of Arts 5, 12 and 17 of the GDPR.

The CNIL fined a real estate company €40,000 for excessive employee surveillance, including software that tracked activity and took regular screenshots, and filming employees without justification. The software inaccurately measured “inactive” periods and employee performance based on predetermined criteria. The CNIL also found breaches of transparency, security, and DPIA requirements under the GDPR.

Links to further information

[Garante order](#)

[CNIL announcement](#)

SHOOSMITHS SAYS...

The European DPAs
continuing to crack down
on monitoring.



DPA fines controller €70,000 for circulating contracts

14 January 2025

Key details

The AEPD (Spanish data protection authority) has issued a fine of €70,000 to a solar panel provider for breaching the data minimisation principle under the GDPR. The company had arranged for a Pdf of a contract to be sent to all 100 participants of a neighbourhood solar project, including as an Annex a spreadsheet containing the full name, ID number, mobile phone number, e-mail address, postal address and signature of all parties.

The solar provider said that this information was a legal requirement for setting up the project, and that it was required as part of the e-signature process, certified under the eIDAS regulation. The AEPD rejected this, finding that information beyond the name was not part of the information necessary to send to individual participants, but was information relevant only to the energy distributors. It therefore found an infringement of Art. 5(1)(c) of the GDPR, leading to the fine, which was reduced to €42,000 for admission and early payment.

SHOOSMITHS SAYS...

A warning about excessive information in multi-party contracts.

Links to further information

[AEPD decision](#) (Spanish only)

Jurisdiction: **EU (Poland)**



DPA fines hospital for unlawful surveillance

17 January 2025

Key details

Poland's data protection authority, the UODO, has publicised a fine of around €272,000 imposed on a medical centre for unlawful video surveillance and inadequate data protection after memory cards from neonatal department cameras were lost.

The UODO found that the centre had not followed the national laws applicable to the installation of CCTV and therefore had no lawful basis for processing personal data, including special category data, under Arts 6 and 9 of the GDPR. It also failed to inform employees and parents about the surveillance contrary to Arts 12 to 14, and breached security requirements, leading to violations of Arts 24, 25 and 32.

SHOOSMITHS SAYS...

Exposing some of the challenges with staff and patient surveillance.

Links to further information

[Decision](#)

Jurisdiction: **EU (Spain)**

AEPD fines banking group after cyber-attack

17 January 2025

Key details

The Spanish Data Protection Authority (the AEPD) has published decisions imposing fines on twenty banks forming part of a group following cyberattacks that exploited vulnerabilities in the banks' systems, with varying degrees of impact. Each bank had a data processing agreement with the same processor.

The banks claimed that the incidents should be treated together, but the AEPD noted that each constituted a separate action involving a different controller. In each case the authority found a breach of the confidentiality principle in Art. 5(1)(f) of the GDPR. The fines ranged from just over €6,000 to €500,000, with some controllers being found also to have breached security and notification provisions in Arts 32 and 33.

SHOOSMITHS SAYS...

Fining with exemplary granularity.

Links to further information

[AEPD pages](#) (Spanish only)



DSB fines health company for appointing the MD as DPO

20 January 2025

SHOOSMITHS SAYS...

DSB KOs MD DPO.

Key details

The Austrian Data Protection Authority, the DSB, has publicised fining a diagnostic lab €5,000 for appointing its managing director as the Data Protection Officer in breach of the requirement for independence in Art. 38(6) of the GDPR.

The company argued that combining roles improved efficiency, particularly during the pandemic. However, the DSB found that the managing director's responsibilities in overseeing data processing conflicted with the DPO's independent monitoring role. It cited CJEU case law from 2023 (*X-FAB Dresden*) which found that while a DPO could have other duties, these must not lead to a conflict of interest.

The DSB noted that roles in senior management, such as the management board, the CFO and department heads will usually be posts incompatible with DPO status. Company shareholders may also be conflicted out.

Links to further information

[Judgment](#) (German only)

[CJEU case](#)

Jurisdiction: **EU (Spain)**

AEPD fines insurance company €5m for inadequate security

27 January 2025

Key details

The Spanish data protection authority, the AEPD, has fined an insurance company €5m after a security breach which potentially affected up to 1.6m people.

It followed a data breach starting in September 2022 and detected the following month which involved a brute force attack on company systems after a third party gained unauthorised access to a broker's login details. Leaked Information included names and addresses, financial information and IBANs (international bank account numbers). It also emerged that the company was failing to limit broker access to information about former customers.

The AEPD found breaches of:

- Art. 5(1)(f) (confidentiality, €1m fine)
- Art. 32 (security, €1m)
- Art. 25 (design, for failing to limit access to data, €2m)
- Art. 35 (DPIA, €1m).

The authority found that a DPIA should be carried out by an insurance company – and any other large organisation – in relation to any insurance-related information (not just health insurance) because of the scale of processing and the likelihood of cyberattack.

The fine was reduced to €4m after voluntary payment.

Links to further information

[AEPD resolution](#) (Spanish only)

SHOOSMITHS SAYS...

The takeaway – DPIAs are increasingly demanded for any large-scale data project.

Enforcement & legal action

Jurisdiction: **EU (Poland)**

Court finds land registry numbers are personal data

28 January 2025

Key details

Poland's data protection authority, the UODO, has issued a statement in support of a recent ruling by the Supreme Administrative Court confirming that land and mortgage register numbers, as listed in Poland, constitute personal data under the GDPR.

The case arose after a company was fined around €23,800 for putting the numbers, with links through to the national land registry, on a website, on the grounds that disclosure gave access to personal details including names, national ID numbers and mortgage information. On appeal, the court upheld this position and the fine.

The ICO position on UK Land Registry numbers is not definitive. Like other numbers, to the extent that they "relate to" a person, they may be personal data; specifically where they reveal information about the activities of individuals. In the context of charging for information about property (though not of Land Registry information specifically) this was discussed in a 2024 case, linked, at paras 724-746.

SHOOSMITHS SAYS...

Expect more issues like this as data holders charge commercial rates for information under statutory control.

Links to further information

[Press release](#)[Surrey searches case](#)

Marketing, adtech &
cookies

CJEU upholds EDPB rulings on Meta

29 January 2025

Key details

The CJEU has upheld in full the decisions of the EDPB which instructed the Irish regulator to impose a larger fine and take further action against Meta in 2022.

The case was brought by the Data Protection Commission in Ireland in response to the EDPB's binding decision that Meta and WhatsApp could not rely on Art. 6(1)(b) of the GDPR (contractual necessity) as a lawful basis for personal data processing for targeted advertising. The EDPB also instructed the DPC to increase the penalties on Meta (to €210m relating to Facebook and €180m in relation to Instagram) and to conduct further investigations into its handling of special category personal data. These further instructions were challenged by the DPC as being beyond the EDPB's remit.

The Court found that the EDPB's actions aligned with the GDPR's primary objective of safeguarding individual data subject rights. It also clarified that the one-stop-shop mechanism was a "procedural simplification" that could not take precedence over the "essential objectives" of the underlying law, and that regulators do not have "absolute independence" outside scrutiny. The costs of the action were ordered to be paid by the Irish regulator.

Links to further information

[Judgment](#)

[EDPB 2022 press release](#)

[DPC 2023 press release](#)

SHOOSMITHS SAYS...

The one-stop shop
continuing to lose force.



Garante orders investigation into DeepSeek AI

30 January 2025

Key details

The Italian data protection authority, the Garante, has issued an order against two DeepSeek AI companies in China. The company released its AI-powered apps which include text, code and maths generators in late January, leading to major disruption in US tech markets, and concerns over the transfer of personal data to China, with global security and privacy implications.

The order:

- declares that current processing activities are in violation of Arts 31, 12, 13, 14, 6, 32 and 27 of the GDPR
- orders the companies to stop processing the personal data of subjects located in the Italian territory with immediate effect
- alleges that they are bound by the extra-territorial effect of the GDPR under Art. 3(2), although this is denied by the companies.

Other global actions in response to DeepSeek AI include a ban in Taiwan for public institutions, an order to stop governmental use in Australia, and restrictions on use by various offices, agencies, the military and NASA in the US. The Dutch data protection authority, the AP, has published a warning to users about the implications of uploading personal information to the app, and says it is seeking other DPA views on co-ordinated action.

Links to further information

[Garante order](#)

[AP warning](#)

WHAT THEY SAY...

“the system lives off the information you put into it”

Jurisdiction: **UK**



ICO gets leave to appeal Clearview AI decision

31 January 2025

Key details

The ICO has announced that, at second attempt, it has been given leave to appeal the judgment of the First Tier Tribunal (FTT) which overturned the ICO's £7.5m fine of Clearview AI Inc.

The US company was fined in 2022 for unlawfully processing the personal data of people in the UK to develop a facial recognition database which was then used for law enforcement purposes in several jurisdictions.

Background information about the FTT decision overturning the fine can be found in the linked Shoosmiths article. Its decision raised important issues about the scope of the UK GDPR in the context of law enforcement purposes and national security.

A date for the hearing is yet to be set.

SHOOSMITHS SAYS...

Waiting for a clearer view from the Upper Tribunal.

Links to further information

[Press release](#)

[Shoosmiths article](#)

Marketing, adtech &
cookies

Garante announces €890,000 fine for unwanted telemarketing

31 January 2025

Key details

The Italian data protection authority, the Garante, has announced fining an electricity company €890,000 for GDPR breaches related to unlawful telemarketing.

The decision followed two complaints from individuals. In the first case, the company relied on a Facebook campaign to collect names and addresses of people who apparently consented to receive follow-up marketing. In the second case, a complainant received 20 communications from the company within a four-month period even though they had not consented to marketing, following a clerical error.

The Garante therefore found violations of GDPR Arts 5, 6, 7, and 24, for not having a lawful basis to process personal data and failing to ensure compliance at the design stage; of Arts 24 and 28 for failing to properly oversee internal and external data processors; and of Arts 12 and 15-22 for inadequate subject rights procedures.

SHOOSMITHS SAYS...

Crossed wires over
direct marketing.

Links to further information

[Order](#)



SOMI brings class action against TikTok and X under DSA

5 February 2025

Key details

The Dutch Foundation for Market Information Research (SOMI) has launched four cross-border class actions on behalf of users in Germany against TikTok and X alleging breaches of the Digital Services Act, the GDPR, and the AI Act.

SOMI is registered as qualified to bring representative actions under the Collective Redress Directive (2020/1828). According to an announcement from its legal team, linked, the group allegations include:

- TikTok recommender systems are exploitative and constitute a banned AI system under Art. 5 of the EU AI Act
- both platforms spread disinformation and carry covert and foreign-sponsored political advertising, contrary to the AI Act, the DSA and the GDPR.

Damages being claimed could reach up to tens of billions of euros. In addition, the group is asking for a stop to unlawful profiling, stricter controls on foreign influence and greater protection of children. Affected users can register for the class action through the Federal Office of Justice in Bonn or the SOMI website or app. The group has already started a similar action against TikTok in Belgium.

Links to further information

[Press release](#)

[SOMI](#)

SHOOSMITHS SAYS...

More evidence of growing class action culture in some EU member states.



AG gives opinion on pseudonymisation

6 February 2025

Key details

An Advocate General (AG) of the CJEU has provided their opinion in an appeal case (C-413/23 *EDPS v. SRB*) which considers data protection in the context of pseudonymisation. It concerns information sent to a banking regulator which was pseudonymised and passed to third parties without informing the individuals involved.

The AG opined that:

- “filtered, categorised and aggregated” opinions or other information can in principle “relate to” a person (39)
- in principle, pseudonymised data “may fall outside the scope of the concept of ‘personal data’” (52)
- the duty to inform data subjects about recipients of personal data also applies to recipients of pseudonymised information. This is despite the wording of the relevant provision (equivalent to Art. 14(1)(e) of the GDPR) since the duty arises prior to the act of pseudonymisation and will therefore always refer to personal data.

If followed, the findings will partially overturn the General Court ruling which judged that the information received was anonymised.

Contrary to expectation, the opinion does not explore the tests of the “means reasonably likely to be used” in Recital 16 (26 of the GDPR) following the *Breyer* case, due to the findings above. Such analysis may follow if the appeal court declines to follow the AG opinion.

Links to further information

[AG opinion](#)

SHOOSMITHS SAYS...

Potentially rewriting the book on pseudonymisation, but let's wait to see what the court rules.



Sensitive data &
vulnerable individuals

Advocate General opines on liability of “hosting services”

6 February 2025

Key details

The Advocate General of the CJEU has issued their opinion clarifying the responsibilities of “hosting services” under the Electronic Commerce Directive (the ECD, 2000/31/EC) and under the GDPR.

The case (C-203/22 *X v. Russmedia Digital*) involved an online marketplace for users to post ads offering sexual services. A user posted details of a third party without their consent. The marketplace removed the ad, but it was replicated on other sites, leading to a data subject claim for damages which was referred by a Romanian court to the CJEU.

The AG opined that:

- an online marketplace operator can be a mere neutral “hosting service” exempt from liability under the ECD even where it reserves rights to copy, distribute, modify, translate and remove the content
- such an operator is a processor of personal data contained in ads (with users being controllers) and has no duty to moderate content under the GDPR
- as processor they might be liable for security breaches under Art. 32, but not otherwise
- the operator would be a data controller to the extent that it then processed the data for its own purposes but would not be responsible for subsequent processing by others outside its control.

The opinion will influence a future CJEU preliminary ruling but will not bind the court. The AG noted that the relevant duties in the ECD have now been largely superseded by the Digital Services Act, which also contains provisions exempting hosting services from liability where they comply with obligations regarding illegal content.

Links to further information

[Press release](#)

[AG opinion](#)

SHOOSMITHS SAYS...

A reminder of the limits of duties for hosting services.

Enforcement & legal action

Jurisdiction: **SOUTH KOREA**



PIPC fines payment providers €5.5m and orders model destruction

11 February 2025

Key details

The South Korean Personal Information Protection Commission (PIPC) has fined Apple and another payment provider a total of KRW 8.375 billion (around. €5.5m) for breaching the Personal Information Protection Act (PIPA) by transferring personal information to Apple and Apple's software services provider, based in Singapore, without consent. The arrangement permitted creation of a payment scoring model.

It also ordered the software company to destroy the "NSF scoring" model (a model evaluating the financial behaviour of users) created using the unlawfully transferred data.

SHOOSMITHS SAYS...

Data protection regulators breaking the mould.

Links to further information

[Press release](#)



CJEU confirms that GDPR fines cover group undertakings

13 February 2025

Key details

The CJEU has issued its preliminary ruling on the calculation of fines of controllers within a group under the GDPR.

The case, (C-383/23 *Ilva A/S*) concerned a furniture retailer which was fined by a Danish court for improper retention of customer data. The public prosecutor then sought a higher fine calculated using the total turnover of the company's group, leading to a CJEU referral. The group in question had a turnover of €881m taking it over the €500m threshold for calculating fines based on a percentage of turnover (rather than the €20m blanket maximum for smaller undertakings).

The court found that:

- the calculation of fines involves a two-step process: determining the maximum fine, then determining the actual fine
- both these stages should be based on an assessment of the "undertaking" for the purposes of EU competition law (which may include an entire group, depending on various factors including "decisive influence").

This means that not only calculation of the maximum, but also the fine itself, may take into account worldwide turnover of the preceding year of a group whose members are connected through general commercial, rather than specific data protection, activities. The ruling goes further than the AG opinion of September 2024 which applied this rule only to establishment of the maximum. The court's reasoning was based on the need for fines to be "effective, proportionate and dissuasive" under Art. 83(9) of the GDPR.

It is likely to be a barrier to arguments that group companies which are not involved in data protection activities should be exempt from fine calculations.

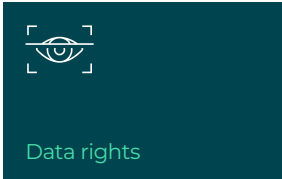
Links to further information

[Decision](#)

SHOOSMITHS SAYS...

The CJEU taking aim at large corporates organising for GDPR fine immunity.

Jurisdiction: **US**



Court of Appeals confirms \$725m Cambridge Analytica settlement

13 February 2025

Key details

The US Ninth Circuit Court of Appeals has upheld a \$725m settlement between Meta and users harmed by the activities of Cambridge Analytica. The original settlement was approved by a district court in 2022, and followed allegations that Facebook allowed

the UK company to use the personal information of up to 87m users without consent for the purposes of profiling and political targeting prior to the first election of President Trump in 2016.

The Court of Appeals found:

- the settlement amount was not a “clear abuse of discretion” by the court
- an allocation of 25% of the settlement sum to lawyers was reasonable
- allocation of damages based on the time spent with an activated Facebook account was fair.

SHOOSMITHS SAYS...

The closing chapters of the first major scandal over election interference.

Links to further information

[Memorandum](#)



CJEU receives referral on interpretation of EU AI Act

14 February 2025

Key details

The CJEU has been asked by a court in Bulgaria to give a preliminary ruling on a number of matters raising important questions about EU law relating to automated decision-making in consumer contracts.

The case, (C-806/24 *Yettel Bulgaria*) concerns the use of automated decision-making (ADM) in calculating early termination charges for a phone contract.

The court has been asked to consider questions on the interplay of consumer and AI law, including:

- whether rights regarding automated decision-making come within the Consumer Rights Directive
- the meaning of the right “to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken” in Art. 86 of the EU AI Act
- whether the Art. 85 right to complain also requires the court to order a deployer to remedy the system in question
- how human review and ethical requirements under the AI Act apply to consumer contracts.

It is notable that the Bulgarian court has invoked the EU AI Act rather the ADM provisions in Art. 22 of the GDPR. There is no explanation of why the system in question is an “AI system” for the purposes of Art. 3. The rights in Art. 85 and 86 apply from 2 August 2026.

Links to further information

[Request](#)

SHOOSMITHS SAYS...

More questions than answers when it comes to AI.

Enforcement & legal action

Jurisdiction: **GLOBAL**



Data protection authorities investigate DeepSeek

17 February 2025

SHOOSMITHS SAYS...

[DeepSeek diving.](#)

Key details

Several data protection authorities around the world have opened investigations into DeepSeek AI following its recent launch.

Actions include:

- **South Korea:** the Personal Information Protection Commission (PIPC) has ordered temporary suspension of DeepSeek services pending investigation; the company appointed an in-country representative on 10 February
- **Texas:** the Attorney General has launched an investigation into DeepSeek for violating the Texas Data Privacy and Security Act and has requested Google and Apple to make enquiries before hosting DeepSeek apps
- **Japan:** the Personal Information Protection Commission has published information about DeepSeek's use of servers in China and the fact that it is subject to Chinese domestic laws.

Investigations are underway in Italy, the Netherlands and Germany, with warnings issued in Poland and Luxembourg.

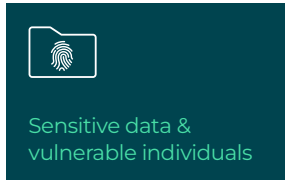
Links to further information

[South Korea press release](#)

[Japan press release](#)

[Texas press release](#)

[Germany press release](#)



Commissioner fines Telegram AUD967,000 under Online Safety Act

24 February 2025

Key details

The eSafety Commissioner in Australia has announced imposing a fine of around €575,000 on messaging service Telegram as a result of failures to provide information within the statutory period under the Australian Online Safety Act.

The company was one of several including Meta, WhatsApp, Google and Reddit which were served information notices under Part 4 of the Act, which requires in-scope online services to comply with “basic online safety expectations” and to report periodically to the Commissioner about their compliance.

The Commissioner says they will publish a summary of the platforms’ responses shortly. X’s response will not be published as it is the subject of a legal challenge.

The Act was subject to a recent review, linked, which recommends imposing an overarching duty of care, requiring risk assessments, simplifying the Act and strengthening enforcement powers to provide maximum fines of the greater of 5% of annual turnover and AUD50m.

Links to further information

[Press release](#)

[Online Safety Act 2021](#)

[OSA review report](#)

SHOOSMITHS SAYS...

Key enforcement under the world’s first online safety legislation.



Claimants open legal actions against DOGE under Privacy Act

26 February 2025

Key details

Various groups have initiated at least twelve legal actions to stop the newly formed Department of Government Efficiency (DOGE) from accessing government records relating to individuals, alleged to be data breaches under the Privacy Act 1974.

The groups include several federal worker associations, a student association, rights groups, unions and attorneys general from nineteen states.

The Privacy Act was passed following the Watergate scandal in 1974 when President Nixon unlawfully accessed federal records for political reasons. The Act controls the use and transfer of information held in a federal agency “system of records”. Disclosure generally requires consent, unless it is subject to a statutory exemption.

To date, some but not all applications for temporary restraint have been successful. On 21 February 2025 rights group EPIC was not granted a temporary restraining order in relation to access to the Treasury Department and Office of Personnel Management. The claims will nevertheless proceed. The Act provides for individual fines of up to \$5,000 and for civil damages claims.

Links to further information

[Privacy Act, as amended](#)

[EPIC press release](#)

SHOOSMITHS SAYS...

More twists and turns for the artful DOGE-er.

Jurisdiction: **EU**

CJEU rules on DSAR information required for automated decisions

27 February 2025

Key details

The Court of Justice of the European Union (CJEU) has ruled on the information which must be provided to data subjects in response to rights requests under Art. 15 which involve automated decision-making (ADM).

The case arose when a data subject was unexpectedly denied a phone contract due to lack of creditworthiness, based on automated credit-scoring. They asked under Art. 15(4) of the GDPR for “meaningful information about the logic involved” in the refusal. The credit scorer declined to provide certain information on the grounds that it constituted a trade secret protected under Austrian law from disclosure.

In the ruling, (Case C 203/22 *Dun & Bradstreet Austria*), the CJEU largely followed the AG opinion in finding:

- information about ADM must be in concise, transparent, intelligible and easily accessible form
- controllers must supply “all relevant information concerning the procedure and principles relating to the use of personal data”

- controllers should find simple ways to explain the rationale or criteria relied on, and not provide complex mathematical formulas, or detailed descriptions of every step
- complexity is not an excuse
- information must be sufficient to enable data subject to express a point of view, contest the decision and ensure accuracy.

In practice, it seems that the controller should explain the actual (flawed) logic used as well as the theory behind what should have happened. Rights extend to the profile created by the controller, not just the information on which it was based.

In addition, the court confirmed that member states cannot impose blanket rules about protecting trade secrets; where there is a likely conflict of interest the matter must be referred to a competent authority or court for determination.

Links to further information

[Judgment](#)

[Press release](#)

SHOOSMITHS SAYS...

The logical end point: controllers who can't explain their ADM may not be able to use it lawfully.



Industry & sector news



Meta publishes Frontier AI Framework

3 February 2025

Key details

Meta has published a new framework on frontier AI, explaining how it assesses risks arising from model development, particularly relating to chemical and biological warfare and malicious cyber use. The report is part of the Frontier AI Safety Commitments signed in May 2024 after the Seoul Summit.

Meta confirms that there are thresholds of risk beyond which it will either stop development or not release a model iteration. It does not quantify these thresholds, nor does it consider other emerging risks identified by the UK DSIT International AI safety report, such as labour market disruption or energy use.

SHOOSMITHS SAYS...

As yet, not a great deal to go on.

Links to further information

[Announcement](#)

[Framework](#)

Jurisdiction: **GLOBAL**



Ransomware report finds payments drop significantly

5 February 2025

Key details

A report published by Chainalysis has found that ransomware payments dropped by 35% to \$814m in 2024 despite an increase in ransomware attacks and wider publication of information relating to victims.

The decline in payments is attributed to stronger law enforcement action such as against LockBit and BlackCat/ALPHV, improved international cooperation, the discovery of over-reporting by attackers, and increasing refusal to pay. It marks the first drop in ransomware payments since 2022.

The report also notes increased cyber resiliency among targets, and growing difficulty in laundering payments through digital wallets and cryptocurrency due to more co-ordinated international policing.

SHOOSMITHS SAYS...

Ransomware: an industry yet to recover from disruption to its major players.

Links to further information

[Report](#)



Marketing, adtech & cookies

Google lifts ban on device fingerprinting

16 February 2025

Key details

Google's starting date for lifting its prohibition of device fingerprinting, 16 February 2025, has now passed.

The technique, disallowed by Google since 2019, involves tracking and linking devices through information inferred by algorithms from how devices are set up, such as the font, browser version, screen size and orientation, and graphics. It potentially enables targeted advertising without the use of cookies, and without identifying an individual user.

The ICO issued a statement in December 2024 saying that the technique would be difficult to operate lawfully in the UK. It is also likely to come under challenge in Europe where, as in the UK, Art. 5(3) of the ePrivacy Directive requires consent to any technology accessing information from end-user devices. Device fingerprinting is considered in the EDPB Guidelines on Art. 5(3) which were updated in October 2024 in response to new technologies.

Proposed changes to the UK ePrivacy rules in the draft Data (Use and Access) Bill would make explicit that the rules apply to "monitoring information automatically emitted by" a device, making clear that fingerprinting techniques are covered. However, the Bill also grants the Secretary of State power to amend the exceptions by secondary legislation, subject to prior consultation with the ICO.

Links to further information

[EDPB Guidelines on Art. 5\(3\)](#)

[Data \(Use and Access\) Bill](#)

SHOOSMITHS SAYS...

Pointing the way to a whole handful of legal challenges.



App Store removes apps not complying with DSA

18 February 2025

Key details

Apple has removed apps not providing trader information in response to the rules in Arts 30 and 31 of the EU Digital Services Act (DSA) requiring trader traceability. According to reports this has resulted in over 135,000 removals from the App Store in the EU.

The rules apply to providers of online platforms allowing consumers to conclude distance contracts with traders. Traders offering services or promoting messages to EU users must provide their contact, payment and registration details to platforms, and certify compliance with EU law. If platforms do not receive this information or cannot verify it they must suspend the service. The rules came into effect for existing traders on 17 February 2025, with new traders bound since 17 February 2024.

Under the Digital Services Act, all in-scope intermediary services, hosting services and online platforms must publish their first set of transparency reports on content moderation activity under Arts 15 and 24 of the DSA by 16 April 2025.

SHOOSMITHS SAYS...

Big scale digital regulation having some bite for consumers.

Links to further information

[Announcement](#)



WhatsApp reaches VLOP threshold under the DSA

18 February 2025

Key details

WhatsApp has reported that it now has 46.8m users in the EU, making it liable to be designated as a Very Large Online Platform under the EU Digital Services Act (DSA).

Under Art. 33(4) of the DSA, the Commission must adopt a decision designating a platform as a VLOP once the 45m “monthly active recipients” threshold has been reached. Unlike designation of gatekeepers under the Digital Markets Act, designation is automatic and does not require assessment of the influence of the platform concerned.

VLOPs, like very large search engines, have additional DSA obligations including risk assessment and mitigation, crisis response, audit, governance and transparency requirements. Obligations begin four months after notification of designation. A list of the 26 current very large platforms and services is published by the Commission, [linked](#).

WHAT THEY SAY...

“they must comply with the most stringent rules of the DSA”

Links to further information

[DSA list](#)



Apple withdraws UK advanced encryption following IPA notice

21 February 2025

Key details

Apple has announced that it is withdrawing an advanced encryption service in the UK, believed to be as a result of being served a notice by the UK government under new powers in the Investigatory Powers Act 2016 (IPA).

The government has reportedly issued a “Technical Capability Notice” (TCN) to Apple regarding its Advanced Data Protection (ADP) system which encrypts information backed up in the cloud. The powers were created in April 2024 by the Investigatory Powers (Amendment) Act, passed just after announcement of the general election by the previous government, and require overseas telecoms providers to take specified actions in relation to encryption technology. The aim of the powers is to ensure that material is potentially available to law enforcement and intelligence services.

The industry body Tech UK warned the government in 2023 about the effect of the amended IPA on innovation and trade, and the risk of diverting attention in the private sector to “fulfilling the surveillance needs of the government”.

Further analysis is in the linked Shoosmiths article.

SHOOSMITHS SAYS...

Crunch time for encryption in the UK.

Links to further information

[Investigatory Powers Act 2016](#)

[Details of ADP](#)

[Shoosmiths article](#)



**Sherif
Malak**
PARTNER

T +44 (0)20 7205 7053
M +44 (0)7799 265 100
E sherif.malak@shoosmiths.com



**Alice
Wallbank**
PROFESSIONAL SUPPORT LAWYER

T +44 (0)3700 864 276
M +44 (0)7514 731 187
E alice.wallbank@shoosmiths.com

This document is a general guide for informational purposes only. It does not constitute legal advice, nor should it be regarded as a substitute for legal advice. Shoosmiths accepts no responsibility for, and will not be liable for any losses arising from, any action or inaction taken as a result of the information contained in this document. It is recommended that specific professional advice is sought. The information stated is as at the date indicated on the relevant page.

Issued: March 2025

©Shoosmiths LLP 2025

SHOOSMITHS

www.shoosmiths.com

**FOR
WHAT
MATTERS**