



SHOOSMITHS

Global privacy and data update

January 2025

www.shoosmiths.com

FOR
WHAT
MATTERS



Legislation



Guidance & consultations



Enforcement & legal action

THE **BIG** STORY



Chinese DeepSeek
AI app disrupts US
markets

28 JANUARY 2025



Industry & sector news



INDEX

Quick read: what you need to know about January 2025

AI

The release of **DeepSeek AI disrupts US tech markets** and leads to regulator complaints in Europe.

President Trump **issues new Executive Orders** affecting data protection and AI development.

The UK government publishes its **AI Opportunities Action Plan** to ramp up AI adoption across the UK.

The European AI Office publicises first **AI literacy event** under the EU AI Act.

Transfers

The incoming US President takes two actions which may **risk EU/US free data flows**.

The European Court **orders the Commission to pay damages** for unlawful US transfers using Facebook.

NOYB challenges six companies on **data transfers to China**.

Cybersecurity

The **Network Data Security Management Regulations** come into force in China.

Spain announces its **draft law on NIS 2** cyber standards and incident reporting for critical systems and infrastructure.

Legal obligations for the financial sector are triggered as the EU cyber resiliency **rules in DORA become applicable**.

The UK Home Office considers new laws to **block ransomware payments**.

Children

Ofcom triggers **obligations for online age assurance** under the Online Safety Act.

The US Federal Trade Commission **finalises COPPA amendments** extending protection of personal information of children under 13.

Meta announces the **end of third-party fact-checking** and some content moderation in the US.

New DP laws and guidance

Data protection **laws come into effect in four US states** imposing obligations on businesses to protect personal information.

The MeitY issues details of its **data protection rules in India**.

The European Data Protection Board publishes its first dedicated **guidance on pseudonymisation**.

The UK ICO publishes **guidance on “consent or pay”** systems.

Legal action

Finnish DPA **fines a website €950,000** for failing to protect open URLs.
















Net neutrality rules are overturned by US appeals court leaving broadband providers outside FCC control.

The CJEU rules that **gendered titles for online purchases** will not usually pass the GDPR necessity test.











The US Supreme Court **upholds the TikTok ban**, while the UK High Court rules on the **scope of DSAR responses**.

Index

Legislation














9	 Data protection laws come into effect in four states	US
10	 Network Data Security Regulations take effect	CHINA
11	 SREN digital law comes into effect	FRANCE
12	 Digital replica bill comes into effect	US (New York)
13	 PIPA comes into effect	BERMUDA
14	 New rules on transfer of passenger information come into force	EU/UK
15	 Spain announces draft law on NIS 2	EU (Spain)
16	 Cyber regulations come into effect	EU
17	 Ofcom triggers obligations for online age assurance	UK
18	 FTC finalises COPPA amendments	US
19	 DORA applies in the EU	EU
20	 EU prepares to adopt Health Data Space	EU
21	 DUA Bill progresses in House of Lords	UK
22	 President Trump replaces Executive Order on AI	US
23	 President issues orders which may undermine US adequacy	US

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





















25	 Institutes publish evaluation of OpenAI o1 model.....	UK/US
26	 MeitY consults on draft data protection rules.....	INDIA
27	 CMA publishes digital markets regime plans.....	UK
28	 DSIT announces AI Opportunities Action Plan.....	UK
29	 Home Office consults on blocking ransomware payments.....	UK
30	 DSIT confirms new fees for ICO registration.....	UK
31	 EDPB issues draft guidance on pseudonymisation.....	EU
32	 EDPB publishes case digest on DSARs.....	EU
33	 EDPB publishes survey report on DSARs.....	EU
34	 AI Office publicises AI literacy event.....	EU
35	 ICO publishes guidance on “consent or pay”.....	UK
36	 EDPB reports on bias and data subject rights in AI.....	EU
37	 Commissioner publishes response on AI Action Plan.....	UK

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

39	 DPA finds Google US is a joint controller.....	EU (Austria)
40	 AP fines Netflix €4.75m for inadequate privacy policy.....	EU (Netherlands)
41	 CNIL fines lead generation company for scraping.....	EU (France)
42	 Finnish DPA fines website €950,000 for open URLs.....	EU (Finland)
43	 Net neutrality rules overturned by US appeals court.....	US
44	 CJEU orders Commission to pay damages for unlawful US transfer.....	EU
45	 CJEU clarifies “excessive” DPA complaints in Art. 57.....	EU
46	 CJEU rules on indicators of gender identity.....	EU
47	 Estonian DPA fines genetic testing company €85,000.....	EU (Estonia)
48	 AG sues insurers for unlawful use of driving data.....	US (Texas)
49	 Court allows class privacy action against Google.....	EU (Netherlands)
50	 NOYB challenges six Chinese companies on data transfer.....	EU
51	 FTC takes action against car manufacturer over geolocation data.....	US
52	 Supreme Court upholds TikTok ban.....	US
53	 DPA issues fine for unlawful use of biometric data.....	EU (Spain)
54	 UODO fines bank for insufficiently senior DPO.....	EU (Poland)
55	 ICO fines company £200,000 for text marketing.....	UK
56	 CMA launches SMS investigation into Google and Apple.....	UK
57	 High Court rules on consent for direct marketing.....	UK
58	 High Court rules on DSAR responses.....	UK

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	 Location data broker reports major breach.....	GLOBAL
61	 Meta announces changes to content moderation in US.....	US
62	 Advocacy groups publish open letter on food delivery and AI fairness.....	EU/UK
63	 IAB responds to EDPB on consent or pay.....	EU
64	 Chinese DeepSeek AI app disrupts US markets.....	US/CHINA

Key:

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



Legislation



Data protection laws come into effect in four states

1 January 2025

Key details

Data protection legislation has come into effect in four US states: Iowa, Nebraska, Delaware, and New Hampshire. The laws aim to enhance consumer data rights and impose obligations on businesses to protect personal data, though each state has its own specific provisions and focus areas.

The Iowa Consumer Data Protection Act grants consumers rights to access, copy, delete, and opt out of targeted advertising or data sales. It requires businesses to implement security practices and provide clear privacy notices but does not include rules on profiling or require risk assessments.

The Nebraska Data Privacy Act, Delaware Personal Data Privacy Act, and the New Hampshire Act Relative to the Expectation of Privacy are more prescriptive and provide consumers rights to access, correct, delete, and obtain copies of data, and to opt out of targeted advertising, data sales, or profiling. They mandate privacy notices and data protection risk assessments.

None of the states have included a private right of action. New Hampshire and Delaware permit a cure period for violations until the end of 2025, while Iowa and Nebraska provide for perpetual (90 and 30 day) cure periods before the Attorney General can take action on behalf of state consumers.

Nineteen US states now have privacy legislation either in effect (12) or passed (7). A further four states have laws in preparation. Laws in New Jersey are due to take effect on 15 January 2025.

On 1 January 2025, the Protecting Youth From Social Media Addiction Act in California partially came into force following a legal challenge on the grounds of free speech. Although technically in force, its effect is suspended pending an appeal court review in February. It would prohibit social media platforms from providing addictive feeds to minors without parental consent and restrict notifications during certain hours.

SHOOSMITHS SAYS...

State laws becoming ever more important as the prospect of US federal legislation fades.

Links to further information

[Iowa Act](#)

[Delaware Act](#)

[California Bill](#)

[Nebraska Act](#)

[New Hampshire Act](#)



Network Data Security Regulations take effect

1 January 2025

Key details

In China the Network Data Security Management Regulations have come into force, following publication in September 2024. The regulations refine and clarify existing obligations under the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL).

The rules apply to data processing within China, personal information of individuals in China, and data processing outside China that harms national security, public interests, or the rights of Chinese citizens or organisations.

The regulations:

- clarify privacy notice, portability and consent requirements
- exempt data exporters from safeguards where transfers are to fulfil legal requirements (although it is not clear whether this only applies to Chinese laws)
- specify notification requirements for processors outside China required to have an in-country representative
- require handlers of personal information of more than 10m individuals to comply with obligations relating to “important data handlers”.

The regulations require data processors to strengthen data security through measures such as encryption, backups, access controls, and security authentication to prevent tampering, breaches, and unauthorised use. New rules on cyber incident reporting are expected in 2025.

Links to further information

[Press release](#)

SHOOSMITHS SAYS...

Expect enforcement of reporting requirements for offshore controllers caught by the rules.



SREN digital law comes into effect

1 January 2025

Key details

Law No. 2024-449 Securing and Regulating the Digital Space (the SREN law) has taken effect in France. It transposes and glosses various provisions of EU law such as the EU Digital Services Act, Data Act and Digital Markets Act, and provides new rules on cloud services and protecting minors.

The law empowers ARCOM (the Audiovisual and Digital Communication Regulatory Authority) to mandate age verification for accessing online adult content. The law creates new offences for online harassment and bullying on social media, and revenge porn, with increased penalties for deepfake content. New rules require education on “digital citizenship” in schools, and there are new controls on online gaming involving tradeable NFTs.

The SREN law also sets out new rules for cloud computing services including limiting switching fees, ensuring interoperability and portability, and regulating terms and conditions. Public sector controllers are subject to new rules for storing sensitive data including protection from third country access.

SHOOSMITHS SAYS...

A comprehensive reform of French digital markets and services.

Links to further information

[Law No. 2024-449](#)



Digital replica bill comes into effect

1 January 2025

Key details

New York's Senate Bill 7676B regulating contracts for the use of digital replicas of performers has come into effect. The law amends the state General Obligations Law (GOB) Chapter 24-A, by voiding contract provisions which allow digital replicas to replace work otherwise performed by the individual unless:

- the provisions include specific use descriptions for the replica (unless these are consistent with the contract and fundamental character of the recording)
- the individual is represented by counsel or a labour organisation.

The Act defines a 'digital replica' as 'a digital simulation of the voice or likeness of an individual that so closely resembles the individual's voice or likeness that a layperson would not be able to readily distinguish the digital simulation from the individual's authentic voice or likeness.'

The law does not address the use of deepfakes without any contract at all. Current UK law provides various recourses for unauthorised deepfake use based on defamation, IP rights, data protection and content moderation rules under the Online Safety Act. The UK government announced plans for additional laws relating to the criminal use of deepfake content on 7 January 2025.

Links to further information

[Law](#)

SHOOSMITHS SAYS...

If you can make it there, you can't remake it anywhere.



PIPA comes into effect

1 January 2025

Key details

Bermuda's Personal Information Protection Act 2016 (PIPA) which regulates the use of personal information has come into effect. The country is a British Overseas Territory (BOT) and therefore not directly subject to the UKGDPR. It already has sectoral legislation, particularly in banking and financial services, but from 2025, PIPA will prevail over other data protection laws.

The Act applies to organisations handling personal information in Bermuda, with exclusions for personal, journalistic, or archival uses, and business contact data. It grants individuals rights such as access, rectification, and erasure of their data and requires organisations to appoint a privacy officer, have privacy notices, report data breaches and respond to data subject rights requests.

Enforcement is overseen by the Privacy Commissioner (PrivCom), with penalties for violations including fines up to BMD 250,000 (around €243,000) and criminal liability for senior stakeholders who connive in a corporate offence.

Links to further information

[PIPA 2016](#)

[Shoosmiths article](#)

SHOOSMITHS SAYS...

[Let's chat BOT.](#)



New rules on transfer of passenger information come into force

8 January 2025

Key details

Both the UK and the EU have brought into effect updated rules on the collection and transfer of advance passenger information (API) and Passenger Name Record (PNR) data by transport carriers. The laws clarify and standardise the collection and transfer of personal data relating to passengers to enhance border security to prevent terrorism and serious crime.

In the UK, the Immigration and Police (Passenger, Crew and Service Information) Order 2024, coming into force on 17 December 2024, revokes the previous SI which dates from 2008. It provides for:

- PNR (essentially, passport) information to be provided on demand by carriers to immigration officers (Schedule 1)
- specified API to be transferred on demand if it is collected by the carrier (Schedule 2). There is a wider category of information (in Schedule 3) which can be demanded if collected by the carrier, but which is subject to greater protection, and includes all booking details, other passengers, emergency contacts, and onward addresses.

In the EU, two regulations covering API used for border control, and for the prevention of terrorism and serious crime, have been published in the Official Journal. They cover a narrower range of API than in the UK legislation, specified in Art. 4 of Regulation 2025/12. These regulations will enter into force on 28 January 2025 and largely become applicable two years after the relevant infrastructure becomes operational. The EU rules for PNR data are set out in the PNR Directive 2016.

Links to further information

[UK statement](#)

[SI 2024/1227](#)

[Commission information](#)

[Regulation – EU – 2025/12](#)

[Regulation – EU – 2025/13](#)

SHOOSMITHS SAYS...

The UK and EU travelling further apart.



Spain announces draft law on NIS 2

14 January 2025

Key details

Spain's Council of Ministers has approved a draft law to transpose the updated Network and Information Systems Directive, NIS 2, which mandates cyber standards and incident reporting for critical systems and infrastructure across the EU.

The law:

- creates the National Cybersecurity Centre to act as competent authority
- will affect entities with tax residence in Spain or which offer services or operate in the country
- designates the entities and sectors which will be covered, including the nuclear industry
- sets out the role of the information security officer or function for designated entities.

The Council also approved an urgent administrative procedure for the draft law and opened it to consultation, closing on 10 February 2025. The original deadline for transposition was 17 October 2024, and Spain is among 24 countries which were the subject of initial procedures by the Commission in December for failure to fully transpose the Directive. In addition, member states have until 17 April 2025 to designate certain “essential” and “important” entities to the Commission and other relevant bodies. In-scope companies must submit registration information to the NCC to enable it to compile the list, so timelines are likely to be short.

Links to further information

[Press release](#) (Spanish only)

[Law](#) (Spanish only)

SHOOSMITHS SAYS...

Racing to get down the Spanish steps.



Cyber regulations come into effect

15 January 2025

Key details

The EU has published the Cyber Solidarity Act and amendments to the Cybersecurity Act in the Official Journal, bringing them into force from 4 February 2025. Although not directed at businesses, they contain mechanisms enabling more co-ordinated and standardised response to cyber threats across the EU.

The Managed Security Services Amendment (Regulation 2025/37) amends the Cybersecurity Act (2019/881) to permit the creation of future European certification schemes for managed security services, such as incident response and penetration testing. The Commission also announced a review of the Cybersecurity Act to assess the effectiveness of existing and new certification schemes.

The Cyber Solidarity Act (Regulation 2025/38) establishes a number of supra-national mechanisms to promote cyber solidarity across the EU. These are a pool of trusted incident response service providers (the Cyber Emergency Mechanism), a cybersecurity alert system through national and cross-border cyber hubs which will use advanced techniques to detect and respond to threats (the European Cybersecurity Shield), and co-ordinated review of significant and large-scale incidents at the request of national authorities or the Commission (the Cybersecurity Incident Review Mechanism).

Links to further information

[Regulation 2025/37](#)

[Regulation 2025/38](#)

WHAT THEY SAY...

“increasing cyber threats can have a devastating societal and economic impact”



Ofcom triggers obligations for online age assurance

16 January 2025

Key details

Ofcom has published two guides which trigger child access risk assessments and age verification obligations for in-scope user-to-user and online search engines. Services must carry out the relevant assessments by 16 April 2025.

Age assurance guidance sets out ways in which age assurance can be assessed to determine if it is “highly effective” or not. If it does not reach this standard, then in-scope user-to-user and search services must conduct further parts of the “Children’s Access Assessment” (CAA) to check whether the service is ‘likely to be accessed by children’ and subject to the relevant children’s safety duties.

The relevant tests are different from the ICO tests for services “likely to be accessed by children” under the Children’s Code, and will require a separate assessment, though they will use similar evidence and analysis.

The approach is designed to incentivise the use of effective age verification techniques.

Ofcom has given notice that it will be accessing regulated online services to monitor content, logging in as a user under the name “Ofcom”. It has also issued resources including a toolkit for organisations to check their compliance against the new rules on illegal content.

WHAT THEY SAY...

“robust age checks are a cornerstone of the Online Safety Act”

Links to further information

[Guidance – age assurance](#)

[Press release](#)

[Guidance – access](#)

[Notice on access](#)



Sensitive data &
vulnerable individuals

FTC finalises COPPA amendments

16 January 2025

Key details

The US Federal Trade Commission (FTC) has announced final amendments to the Children's Online Privacy Protection Act (COPPA) Rule following public consultation. The underlying rule, which prohibits unfair or deceptive acts or practices in connection with the collection, use, and disclosure of personal information from and about children under 13, was last amended in 2013. Key changes:

- require website and online service operators to obtain additional opt-in parental consent before sharing children's personal information with third parties for targeted advertising
- narrow current permissions for personal data use
- exempt "mixed audience" websites for users not identified as under 13 through compliant age verification, to promote neutral age-gating
- expand the definition of "personal information" to cover biometric identifiers such as fingerprints
- limit data retention to as long as reasonably necessary to fulfil a specific purpose and prohibit indefinite retention of data collected from a child
- require COPPA "Safe Harbor" programmes (voluntary codes) to disclose membership lists and provide additional reports to the FTC.

After consideration, the FTC has not regulated push notifications aimed at children or introduced specific requirements for educational technology companies operating in schools.

The amended COPPA Rule will take effect 60 days after publication in the Federal Register. Organisations covered under the Rule will have up to one year from the publication date to achieve full compliance although faster compliance is required for those in Safe Harbor programmes.

Links to further information

[Final rule](#)

[Press release](#)

SHOOSMITHS SAYS...

COPPA bottomed out.



DORA applies in the EU

17 January 2025

Key details

The cyber resiliency rules in the EU Regulation on digital operational resilience for the financial sector (DORA) and its accompanying Directive have become applicable in EU member states, triggering legal obligations to comply. The new laws aim to achieve higher levels of cyber security for financial institutions, by instituting rules for governance and risk management, incident reporting, testing, supply chain risks and sharing information about threats and vulnerabilities.

DORA directly affects in-scope financial entities including financial services providers based in, or providing services in, the Union. It also covers their “critical” third-party ICT suppliers (CTPPs) including cloud service and managed services providers, who will be subject to increased due diligence, audit and contractual controls by customers.

Not all standards have been finalised, although the Commission expects compliance with the draft versions until the review process is complete.

Competent authorities in member states are due to publish lists of “systemic” financial entities by 31 March 2025, and submit registers of CTPP information to the European Supervisory Authorities by 30 April 2025.

Penalties set by member states include periodic penalty payments of up to 1% of the average daily worldwide turnover for CTPPs, together with fines and potential criminal penalties for financial entities, to be determined by member states.

Links to further information

[DORA](#)

[Commission overview](#)

SHOOSMITHS SAYS...

Opening the DORA to safer banking and financial services.



EU prepares to adopt Health Data Space

21 January 2025

Key details

The Council of the EU has adopted the European Health Data Space (EHDS) regulation which aims to improve access to and exchange of electronic health data across the EU. The regulation will allow individuals to access and control their health data across member states in standardised format and enable secure re-use of anonymised data for research and innovation purposes.

The Data Space will:

- permit individuals to access their health records from anywhere in the EU and exercise control over use of their data
- make some secure and anonymised data available to scientific researchers and policymakers
- compel member states to provide rights of opt-out for secondary use of health data (Art. 71(1)). States may apply exemptions within certain parameters (Art. 71(4))
- require electronic health record systems to comply with EU-wide standards to ensure seamless cross-border data exchange (called “interoperability”).

The regulation will enter into force 20 days after publication in the Official Journal. Member states must establish digital health authorities to manage and enforce the rules within two years; rules governing access bodies will take effect over seven years.

The European Commission has also launched an EU Action Plan to improve cybersecurity for hospitals and healthcare providers. Key measures include establishing a dedicated Cybersecurity Support Centre, financial aid to smaller providers, rapid response services and coordinated ransomware reporting, to be initiated in 2025-26.

Links to further information

[Text](#)

[Action plan](#)

[Council press release](#)

WHAT THEY SAY...

“will enhance the quality and efficiency of medical care, while ensuring that our health system remains resilient to future challenges”



DUA Bill progresses in House of Lords

21 January 2025

Key details

The report stage of the Data (Use and Access) Bill in the House of Lords is scheduled to take place on 21 January 2025. This follows a line-by-line examination of the bill which concluded during the committee stage on 18 December 2024.

This is a further opportunity for the House of Lords to closely scrutinise elements of the bill and make changes. A major early theme of debate has been the importance of upholding data protection standards in view of the government's ambition to "mainline AI into the veins" of the nation expressed in the AI Opportunities Action Plan in early January.

WHAT THEY SAY...

"it is a matter of regret that we are not simultaneously looking at an AI Bill"

Links to further information

[Bill and progress](#)



President Trump replaces Executive Order on AI

23 January 2025

Key details

The new US president has issued several new Executive Orders in his first few days in the White House which affect data protection and AI development. “Removing Barriers to American Leadership in Artificial Intelligence” requires various executive bodies to create a national AI strategy within 180 days to strengthen US global AI dominance to support economic growth, and national security.

It was preceded on 20 January by the revocation of various Executive Orders including EO 14110 on safe, trustworthy and secure AI. Issued in October 2023, this was designed to co-ordinate AI strategy at federal level to address national security and consumer protection.

The President also issued an Executive Order to clarify regulations for digital financial technologies, supporting open access to blockchain networks, establishing a federal framework for digital asset regulation, and prohibiting central bank digital currencies (CBDCs). These centralised currencies are under development principally in China, with Europe and the UK also developing schemes.

A further EO underlined the commitment to free speech and is aimed at content moderation on social media.

Links to further information

[EO on AI](#)

[Revocation of EOs](#)

[EO on digital financial
technology](#)

[ICO guide to CBDCs](#)

[EO on freedom of speech](#)

SHOOSMITHS SAYS...

Playing the Trump card.



Transfers

President issues orders which may undermine US adequacy

27 January 2025

Key details

The incoming US President has taken two actions which may put at risk the adequacy decision in place between the EU and US.

First, the Privacy and Civil Liberties Oversight Board has announced the dismissal of its three Democratic party members. The Board was instituted to oversee federal powers under anti-terrorism legislation and plays an important part in the functioning of the EU/US Data Privacy Framework (DPF) which allows certain EU to US personal data transfers without further safeguards.

The EU Commission adequacy decision cites the PCLOB as “an independent agency within the executive branch composed of a bipartisan, five-member Board appointed by the President for a fixed six-year term with Senate approval”. This status is challenged by the dismissals, which have been criticised as unlawful.

There has been no revocation of Executive Order 14086, which is the foundational EO for the transfers mechanism issued in 2022 by President Biden. However, in a second move President Trump has also ordered a review within 45 days of all “National Security Memoranda”. These include NSM 14, which also underlies the EU/US DPF in regulating signals intelligence activity.

The EU Commission has not yet commented officially. It has power to revoke the adequacy finding at any time. The actions make it more likely that the European Court of Justice will overturn the DPF, leaving exporters of personal data into the US requiring additional measures or appropriate safeguards, such as SCCs or BCRs, if they cannot rely on a derogation.

Links to further information

[PCLOB press release](#)

[NSM 14](#)

SHOOSMITHS SAYS...

The safest course – put in place alternative transfer mechanisms if you want to carry on exporting to the US.



Guidance & consultations



Institutes publish evaluation of OpenAI o1 model

18 December 2024

Key details

The UK and US Artificial Intelligence Safety Institutes (AISIs) have published the results of a joint evaluation of OpenAI's o1 model. The exercise compared the model to reference models such as OpenAI GPT-4o and Anthropic Claude 3.5 Sonnet on capabilities including the ability to hack into systems, demonstrating understanding of biological research, and software engineering/AI development tasks.

As this is the first such joint testing exercise, these specific results may not be in themselves significant, however, the research is the start of benchmarking for AI capabilities which may have a safety aspect. The inclusion of biological research tasks reflects possible use of AI in developing biological weapons.

By way of example, against 40 public cybersecurity (hacking) challenges, the model achieved a 45% success rate in US testing against 35% by the best reference model, and UK testing reported a 36% success rate on 47 challenges at the "cybersecurity apprentice" level, against 16% by the best-performing reference model. 100% represents the best equivalent human performance.

Links to further information

[Evaluation](#)

[Press release](#)

SHOOSMITHS SAYS...

Foundations for future testing of foundation models.



MeitY consults on draft data protection rules

3 January 2025

Key details

India's Ministry of Electronics and Information Technology (MeitY) has issued draft Digital Personal Data Protection Rules 2025 which are open to public consultation.

The draft Rules are made using powers in s.40 of the Digital Personal Data Protection Act 2023 and expand on certain concepts introduced in the underlying legislation.

The rules cover:

- requirements for consent management companies including conditions for registration (Schedule One)
- data fiduciary (controller) obligations including consent notices, robust security measures, deletion and the requirement to pre-notify deletion to data principals (subjects)
- obtaining evidence of parental or guardian consent to process children's data
- notification of any personal data breach to the regulator and affected individuals without delay
- publication of Data Protection Officer contact information and data principal request procedures
- annual audits and Data Protection Impact Assessments (DPIAs) to be carried out by significant data fiduciaries (designated controllers of sensitive data)
- retention periods for certain classes of data kept by e-commerce, gaming and social media sites (Schedule Three).

It also specifies the constitution of the Data Protection Board of India, and appeal procedures. Public comments on the draft Rules are invited until 18 February 2025.

Although no timetable has been set, business obligations are expected to come into effect after a transition period of up to two years.

Links to further information

[Rules](#)

[Explanatory note](#)

SHOOSMITHS SAYS...

Putting meat on the bones of India's foundational data protection law.



CMA publishes digital markets regime plans

7 January 2025

Key details

The UK Competition and Markets Authority has announced its plans for designation of entities with “strategic market status” in 2025 under the Digital Markets, Competition and Consumers Act 2024, which came into force on 1 January 2025. It follows the publication of detailed guidance in December 2024.

The CMA will start investigations into two areas of digital activity in January 2025, and a third in mid-2025. Investigations must take no longer than nine months. Possible interventions following designation include orders to prevent preferencing, making switching provider easier, and enabling effective competition particularly for smaller companies reliant on the digital ecosystem. The regime is a more flexible enactment of principles in the EU Digital Markets Act.

The CMA has since launched investigations into Google search, and the mobile ecosystems created by Google and Apple.

WHAT THEY SAY...

“a level playing-field for the many start-ups and scale-ups across the UK tech sector”

Links to further information

[Announcement](#)

[Guidance](#)



DSIT announces AI Opportunities Action Plan

12 January 2025

Key details

The UK government has published its “AI Opportunities Action Plan”, announced in the Autumn Budget Statement. The plan aims to “ramp up AI adoption across the UK” and sets out policy principles which will underpin ambitious targets to increase AI adoption and use across the UK economy.

The plan calls on government to:

- identify five “high-impact public datasets” to make available to AI innovators quickly, using “privacy-preserving versions”
- create and license a copyright-cleared British media asset training data set, and reform text and data mining laws (the latter is already under public consultation)
- fund regulators to scale up AI capabilities, and ensure they enable innovation
- encourage sandboxes in challenging but high-growth areas like autonomous vehicles, drones and robotics
- consider a central AI regulator with a “higher risk tolerance” to permit sandboxing outside current rules
- create a “UK Sovereign AI” unit to drive investment, expand capacity of the AI Research Resource, and make it easier to build data centres.

The ICO has issued a statement in response, [linked](#), noting the guidance it has already issued on data protection and AI, and that “data protection is essential to realising this opportunity”.

It follows the publication on 10 January of the government response to the SIT Committee report on AI Governance, confirming that AI-specific legislation with “binding regulations on the companies developing the most powerful AI models” will shortly be open to consultation.

Links to further information

[Action plan](#)

[Response on AI Governance](#)

[ICO statement](#)

SHOOSMITHS SAYS...

Putting the case for massive AI investment, regardless of the consequences.



Home Office consults on blocking ransomware payments

14 January 2025

Key details

The UK Home Office, in collaboration with the National Cyber Security Centre (NCSC), has launched a public consultation aimed protecting public and critical infrastructure by limiting the power of certain organisations to make ransomware payments.

The three proposals are:

- a ban on ransomware payments for all public sector bodies and “critical national infrastructure” entities, which may include their critical supply chain
- mandatory reporting of ransomware and engagement with the National Crime Agency, in all sectors, and enabling the NCA to block payments to criminal or sanctioned groups
- requiring reporting of ransomware incidents above a threshold for all, or some, sectors.

Stakeholders including businesses, public authorities, and cybersecurity professionals, are invited to provide feedback on these measures until 8 April 2025, with a particular call to multinational organisations, and on the interaction with data protection compliance rules. The rules will align with the proposed Cyber Security and Resilience Bill (proposed NIS 2-type laws for the UK) to avoid unnecessary reporting burdens for organisations.

Links to further information

[Statement](#)

[Consultation](#)

WHAT THEY SAY...

“helping to break the ransomware business model”

Jurisdiction: **UK**



DSIT confirms new fees for ICO registration

16 January 2025

Key details

The UK Department for Science, Innovation, and Technology (DSIT) has announced a forthcoming 29.8% increase in data protection fees to be paid by data controllers to the Information Commissioner's Office (ICO). This increase is intended to ensure the ICO has sufficient resources to fulfil its obligations, accounting for inflation and wider responsibilities under the new Data (Use and Access) Bill. The increase is less than the 37.2% initially proposed.

Tier 1 fees will rise from £40 to £52, Tier 2 from £60 to £78, and Tier 3 from £2,900 to £3,763. The current fee structure, exemptions, and direct debit discount will remain unchanged. The changes will be put in place through regulations to be enacted early in 2025.

WHAT THEY SAY...

“uplifts are necessary to ensure that the ICO is financially sustainable in the longer term”

Links to further information

[Press release](#)



Accountability & governance

EDPB issues draft guidance on pseudonymisation

16 January 2025

Key details

The European Data Protection Board (EDPB) has published its first dedicated draft guidance on pseudonymisation, and considers how it can help fulfil various GDPR compliance responsibilities including lawfulness of processing, security, and transfers of personal data.

The guidelines look at the GDPR definition of pseudonymisation – processing so personal data can no longer be attributed to a specific data subject (Art 4(5)) – and confirm that pseudonymised data is subject to the GDPR, as is the “additional information” which can enable re-identification, although they may be subject to different requirements from the underlying personal data, depending on the context.

The guidance introduces a number of concepts, such as:

- the “pseudonymisation domain”, which is a flexible definition of the set of people having access only to pseudonymised data, and may include unauthorised recipients and overseas authorities
- “consistent pseudonymisation” which is using the same identifiers to enable linkage of data sets by one or more controllers.

The EDPB notes that:

- pseudonymisation may enable a controller to rely on legitimate interests to process data
- pseudonymised data may be personal even where additional information is destroyed, and can only be considered anonymous if it passes the Recital 26 test
- a lawful basis for processing will extend to the process of pseudonymisation
- when considering if breaches involving pseudonymised data are reportable under Arts 33 and 34, controllers must look at the risks of analysis by an unauthorised person.

It focuses on the risks and benefits of sharing pseudonymised data across controllers, and techniques for securing it, including the use of trusted third parties and “transaction pseudonyms” to prevent unauthorised linkage. It recommends contractual arrangements and effective enforcement between parties within the pseudonymisation domain regardless of processing role. The Annex contains practical examples including sharing data for medical research.

The consultation closes on 28 February 2025.

Links to further information

[Guidelines](#)

[Press release](#)

WHAT THEY SAY...

“how pseudonymisation can help organisations meet their obligations”



EDPB publishes case digest on DSARs

16 January 2025

Key details

The European Data Protection Board (EDPB) has published a One-Stop-Shop case digest focusing on the right of access under Art. 15 of the GDPR. The digest provides a useful summary and reminder of recent regulator and court findings in relation to DSARs in the multinational context.

The digest, part of the Support Pool of Experts programme, is a compilation of decisions made by supervisory authorities under the one-stop-shop (OSS) mechanism and looks at problems and enforcement across the DSAR lifecycle. Cited decisions cover all aspects of the right of access and consider underlying CJEU case law. Given the OSS context, the cases are mostly concerned with complaints, the private sector, and social media and online environments.

It notes in particular that:

- most OSS DSAR complaints also involve other data protection issues such as Art. 5 (lawfulness, fairness and transparency)
- there are difficulties handling DSARs made to central data processors which should be directed at individual controllers
- DSARs made on behalf of children continue to cause difficulty.

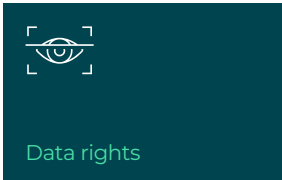
Links to further information

[Case digest](#)

[Press release](#)

SHOOSMITHS SAYS...

[A one-stop-shop for rulings on DSARs.](#)



EDPB publishes survey report on DSARs

16 January 2025

Key details

The EDPB, the European Data Protection Board, has reported on the current state of play on how controllers are managing data subject access requests, following a survey of 1,185 controllers carried out with 30 supervisory authorities across the EU.

It found that controllers have particular problems understanding the scope of access rights, retention of request data, and internal procedures, and a general lack of awareness of EDPB Guidelines 01/2022.

Recommendations include that:

- controllers should clearly define the scope of a request and ensure they are prepared to handle requests promptly
- retention periods for access request communications should be granular, justified and documented, and requests stored separately from other data subject information
- internal procedures should be formalised, with proper training to recognise and process access requests from all submission channels.

The EDPB notes that regulatory action is often prompted by complaints about inadequate DSAR responses from individuals and suggests ways of managing requests through voluntary portals to reduce the risk. It found surprisingly low levels of requests among some large controllers – 74% of controllers said that they received no more than ten DSARs in 2023 – suggesting that they were not properly recognising them, although generally compliance was best among controllers receiving a large number of requests.

Links to further information

[Report](#)

WHAT THEY SAY...

“Regulators plan to initiate formal investigation into matters of concern as a result”



AI Office publicises AI literacy event

20 January 2025

Key details

The AI Office is publicising an open event on AI literacy obligations under the EU AI Act, to be held on 20 February 2025.

Under Art. 4 of the Act, in-scope organisations using AI systems should use their best efforts to ensure that staff and others operating systems on their behalf have a sufficient level of AI literacy to make “an informed deployment” of AI systems.

Anyone using an AI system for commercial activity where the output produced by the AI system is used in the Union (regardless of intent) may be in scope of the literacy requirement, excepting certain activities such as pure R&D or national security deployments. The rule will apply regardless of where the system itself is based or where staff live.

Art. 4 applies from 2 February 2025, with enforcement mechanisms set to be put in place by member states by 2 August 2025. The AI Office has said it will be supporting compliance of developers and users “by the end of 2025”.

SHOOSMITHS SAYS...

When it comes to AI, we're all going back to school.

Links to further information

[Announcement](#)



Marketing, adtech & cookies

ICO publishes guidance on “consent or pay”

23 January 2025

Key details

As part of its online tracking strategy, the UK Information Commissioner’s Office (ICO) has published new guidance on the use of “consent or pay” (COP) systems which require online service users either to consent to the use of personal data for targeted advertising or pay a fee.

The ICO’s position is that COP systems can be compliant with data protection laws, but only if they are designed in particular ways. “TIOLI” (take it or leave it) approaches, which require consent to tracking but offer no alternative, cannot be compliant.

Key points are:

- COP is not necessarily banned for large platforms
- binary COP systems will find it harder to demonstrate freely given consent, especially where the “pay” alternative bundles the core product price and the price for personal data
- the “pay” option linked to a core service must not require consent to personalised advertising, not unnecessarily reduce the overall product or service quality, and not have an inappropriately high fee.

Much of the advice is concerned with pricing models, particularly for subscription services. The approach centres on accurate pricing of the “price” for personal data (as distinct from the price of the service) which may be based on consumer perception but must not be based on actual behaviour where nudge tactics have been used.

Platforms must be assessed for power imbalance, based both on competition law principles and considerations under data protection law. It does not appear to ban COP outright for children, although the guidance, including the relationship with the principles in the Children’s Code, will require careful consideration.

The ICO has also published its online tracking strategy, which will include investigations of consent management and data management platforms, apps and connected TVs, and steps to tackle cookie compliance across the UK’s top 1000 websites.

WHAT THEY SAY...

“we expect organisations to give people meaningful control over how they are tracked online”

Links to further information

[Consent or pay](#)

[Online tracking strategy](#)

[Cookie compliance](#)



EDPB reports on bias and data subject rights in AI

23 January 2025

Key details

The European Data Protection Board (EDPB) has published reports on AI bias and the exercise of data subject rights in AI. They have been produced to assist the EDPB but do not necessarily reflect its views.

The report on bias evaluation examines sources of AI bias and the state of the art in techniques for bias mitigation, which are currently limited. It highlights that simply removing sensitive variables is ineffective and suggests advanced methods such as fine-tuning and reinforcement learning with human feedback for generative AI.

The report on data subject rights explores challenges in managing rights to erasure and rectification in the context of AI systems. It looks at various techniques being developed to allow “deletion” or “unlearning” of personal data used to train an AI model. It also explores available measures to limit personal data outputs in generative AI, noting that these are “much less mature” than unlearning techniques. It “strongly” recommends the use of anonymised data for model training.

WHAT THEY SAY...

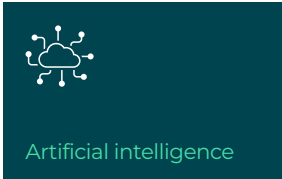
“design choices might have performance trade-off but are an aspect of data protection by design”

Links to further information

[Press release](#)

[AI bias report](#)

[AI and data subject rights report](#)



Commissioner publishes response on AI Action Plan

24 January 2025

Key details

The ICO has published its response to the UK government on its AI Opportunities Action Plan. The ICO will:

- support a statutory Code of Practice on AI
- guide SME compliance in AI development through a “Data Essentials” programme
- support legislation to permit an “experimentation regime” with a time-limited derogation from specific regulatory requirements to test new ideas, under strict governance controls supervised by the ICO.

The letter also says that the regulator will:

- promote contextual models – such as tracking for “privacy-preserving ad measurement” by selective enforcement
- publish new and updated guidance on international data transfers, making it quicker and easier for businesses to transfer data safely.

SHOOSMITHS SAYS...

Treading a careful path through conflicting aims.

Links to further information

[Letter](#)



Enforcement & legal action

Jurisdiction: **EU (Austria)**

DPA finds Google US is a joint controller

17 December 2024

Key details

The Austrian data protection authority, the DSB, has issued a finding that Google LLC in the US and Google Ireland Ltd are joint controllers of personal data in the EEA.

The decision, published by NOYB, follows a complaint made by a data subject in Austria supported by the rights group. The decision challenges previous determinations by the Irish DPC that the US company only processed on behalf of Google Ireland, acting as sole controller. The DPA cited the IAB Europe ruling (linked) to find that the US company easily passed the tests for joint control established in CJEU case law.

Based on the new analysis, the DPA has ordered the US company to respond fully to the DSAR in question and ordered compliance within two weeks. The ruling challenges claims by US-based multinational digital providers that EEA subsidiaries are sole controllers, thereby permitting direct enforcement by data protection authorities outside the main establishment, here, Ireland. Google LLC is expected to appeal.

SHOOSMITHS SAYS...

Part of on ongoing efforts by EEA regulators to overcome Irish leniency on its big data companies.

Links to further information

[Ruling](#) (German only)

[IAB Europe ruling](#)

Accountability &
governance

AP fines Netflix €4.75m for inadequate privacy policy

18 December 2024

Key details

The Dutch Data Protection Authority, the AP, has issued details of a fine of €4.75m imposed on the streaming service Netflix International BV for an inadequate privacy policy and failure to respond adequately to data subject rights requests, for periods between May 2018 and July 2020.

Following an investigation started in 2019 prompted by complaints from a data subject, the AP found that the privacy notice and DSAR response:

- did not name individual recipients of personal data as required by Art. 13(1)(e) and Art. 15(1)(c) of the GDPR (notably the AP did not follow the CJEU in distinguishing between a privacy notice and more granular requirements in a DSAR response)
- did not provide specific retention periods – a reference to “applicable laws” was not sufficient
- did not provide sufficient information about third country transfers and appropriate safeguards, nor about the legal bases for processing.

The decision acknowledges the difficulty of providing full privacy information through a TV operated by remote control but it was nevertheless found not to be sufficiently full or well-organised.

Unusually, the decision contains an apology to the controller and data subjects over for the long time the complaint took to resolve.

Links to further information

[Press release](#)

WHAT THEY SAY...

“a company with millions of customers worldwide has to explain properly to its customers how it handles their personal data”



CNIL fines lead generation company for scraping

19 December 2024

Key details

The French data protection authority, the CNIL, has publicised a €240,000 fine imposed earlier in December on a lead generation company for breaches of the GDPR after unlawfully processing LinkedIn users' contact details.

The company marketed a Chrome extension permitting customers to get professional contact details of people on LinkedIn, using a database of 160m contacts created from LinkedIn and other scraped information. The database included data from people who had chosen to restrict access to contact details, including choosing to share with only "first and second level relations", i.e. immediate contacts, and their immediate contacts.

The CNIL found that the company:

- could not rely on legitimate interests for processing such users' personal data as users had a reasonable expectation that contact details would not be processed, which was binding on third parties (Art. 6)
- triggered excessive retention periods by resetting a 5-year period every time a person changed position or employer (Art. 5(1)(e))
- only posted a privacy notice four years after starting the collection, and provided it in English only (Arts 12 and 14)
- failed to specify third party recipients in DSAR responses (Art. 15).

The investigation was triggered by complaints from users. The company has until 18 June 2025 to bring processing into compliance.

Links to further information

[Press release](#)

[Ruling](#)

SHOOSMITHS SAYS...

A reminder that third parties relying on legitimate interests must take account of choices made by data subjects.



Finnish DPA fines website €950,000 for open URLs

23 December 2024

Key details

The Finnish DPA has fined a loan comparison service provider €950,000 for breaches of the GDPR including inadequate safeguards to protect loan application data.

Following a complaint in 2022, an investigation revealed that URLs allocated to customers for loan applications were available on the open internet without a login requirement, leading to potential exposure of data including personal ID numbers, income details and marital status. Despite the controller claiming that it had put in place a firewall to prevent brute force attacks, the DPA found evidence of automated requests, indexing by search engines, and millions of unauthorised access attempts.

It therefore found that the company failed to implement adequate security measures contrary to Arts 5, 25, and 32 of the GDPR. The DPA had already ordered the controller to halt processing and notify affected customers in mid-2024. The problems pre-dated acquisition of the business by the controller in 2022, but the DPA considered that the controller was responsible for an infringement which had effectively been taking place since 2017.

SHOOSMITHS SAYS...

Useful reminder that open URLs pose a security risk.

Links to further information

[Decision](#)

Accountability &
governance

Net neutrality rules overturned by US appeals court

2 January 2025

Key details

The US Court of Appeals for the Sixth Circuit has ruled that the Federal Communications Commission (FCC) cannot impose “net neutrality” rules. The case, brought on behalf of several broadband industry associations, has overturned a 2024 FCC Order called “Safeguarding and Securing the Open Internet” which classified ISPs as “telecommunications services” rather than mere “information services” under the Communications Act 1934, putting them under full FCC control.

The FCC’s underlying aim was to prevent internet providers from blocking, slowing, or exercising price controls over broadband services in order to indirectly control content or preference their own services. The ruling relied on a recent decision from the US Supreme Court (*Loper Bright v. Raimondo*) which constrains regulator powers in respect of contested legislation.

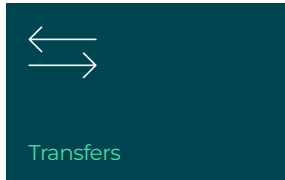
Various states have enacted net neutrality rules, and there is a call to enshrine net neutrality into federal law from the FCC ([linked](#)).

SHOOSMITHS SAYS...

The bonfire of the US regulators already smouldering.

Links to further information

[FCC statement](#)



CJEU orders Commission to pay damages for unlawful US transfer

8 January 2025

Key details

The Court of Justice of the European Union (CJEU) has ruled that the European Commission was in breach of data protection laws applicable to EU institutions by enabling attendees to sign up to a conference using Facebook without ensuring adequate safeguards for transfer to the US.

The case was brought by the founder of a German consumer rights group over transfers made in 2022 before adoption of the EU/US Data Privacy Framework. He made a number of claims for damages and rectification for breach of Regulation 2018/1725 (the EUPDR), not all of which were successful.

The CJEU found:

- the Commission responded late (outside one month but within three months) to a data subject rights request; however, there was no evidence of non-material damage in this case

- mere risk of US transfer did not constitute an infringement of Art. 46: when the user's personal data, his IP address, was stored on AWS servers in Germany the claimant could not demonstrate that access was in fact granted to US authorities
- however, the Commission failed to put in place SCCs or another appropriate safeguard for the optional Facebook login
- this transfer put the applicant into a "position of some uncertainty" over personal data processing, giving rise to a claim for non-material damage, assessed as worth €400.

The court did not analyse whether the Commission was a joint controller with Facebook; rather it found that the Commission "created the conditions" of transfer, noting that Art. 46 of the EUPDR requires conditions of transfer to be fulfilled by controller and processor (also reflecting the position in Art. 44 of the GDPR).

SHOOSMITHS SAYS...

The CJEU flexing its muscles again over US transfers.

Links to further information

[Judgment](#)

[Press release](#)



CJEU clarifies “excessive” DPA complaints in Art. 57

9 January 2025

Key details

The Court of Justice of the European Union (CJEU) has clarified the meaning of “excessive requests” to supervisory authorities and the opportunities for DPAs to charge fees under Art. 57(4) of the GDPR.

Case C-416/23 (Austrian DPA v FR) involved complaints dismissed by the Austrian Data Protection Authority after a data subject made 77 requests to it regarding a number of different controllers over 20 months.

The CJEU ruled that:

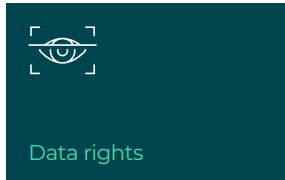
- the rules about excessive “requests” in Art. 57(4) also cover “complaints” lodged with a supervisory authority under Art. 57(1) and Art. 77(1)
- following existing DSAR case law, “excessive” cannot refer solely to quantity, but must have proven abusive intent
- “abusive” intent is likely to be characterised by requests which do not relate to data subject rights but which are aimed at hindering or paralysing the authority’s functions
- mere “hogging” of DPA resources is not enough to be excessive
- if requests are excessive, DPAs can choose whether to impose reasonable fees or refuse action, provided it is a reasoned decision and measures are justified, necessary, and proportionate.

Links to further information

[Judgment](#)

SHOOSMITHS SAYS...

The takeaway – data subjects may hog resources but can’t hinder functions.



CJEU rules on indicators of gender identity

9 January 2025

Key details

The Court of Justice of the European Union has ruled that collecting gendered titles such as “Mr.” or “Ms.” is not ordinarily necessary under the GDPR. The case (*Mousse v CNIL and SNCF Connect*) arose when a rights group representing non-binary people objected to the requirement to identify as either “M.” or “Mme” on the SNCF (national railway) online ticketing platform.

The CNIL had found in 2021 that such processing was lawful under Art. 6(1)(b) (contractual necessity) on the grounds that the railway offered gender-segregated services, and that it did not breach the data minimisation principle in Art. 5(1)(c) as using titles was a commonly accepted practice.

The Court held that:

- personalising commercial communication based on presumed gender identity is not objectively indispensable for fulfilling a transport contract
- processing such personal data cannot be justified as a legitimate interest if customers are not properly informed, if processing is not necessary, or if customer rights prevail for example through potential discrimination
- “common practices and social conventions” are not part of the necessity test in Art. 6(1), although they may be part of coining appropriate inclusive expressions.

The Court noted that the final determination must be made by the French court. The judgment does not prevent organisations from processing gendered titles with consent, for example where there is an option to purchase without giving a title. There may also be situations where processing is objectively necessary, for example when offering gender-segregated services.

Links to further information

[Press release](#)

[Judgment](#)

SHOOSMITHS SAYS...

For online purchases, unless you have an objectively indispensable reason, you must offer a neutral or no-title alternative.

Enforcement & legal action

Jurisdiction: **EU (Estonia)**

Estonian DPA fines genetic testing company €85,000

10 January 2025

Key details

Estonia's Data Protection Inspectorate, the DPI, has announced an €85,000 fine of a genetic testing company for infringing the GDPR in connection with a data breach reported in November 2023. The breach resulted from a cyberattack on the company's systems which led to the exposure of around 100,000 files containing sensitive personal data including genetic and health information.

The DPI's investigation found that the processor failed to implement adequate security measures. €5,000 of the fine was attributable to appointment of a Data Protection Officer (DPO) who had conflicts of interest due to their senior role within the organisation, contrary to the requirements for independence in Art. 38 of the GDPR. The regulator emphasised that DPOs must not hold a position on the management board to avoid impairing impartiality. It also noted that the choice of DPO must relate to the sensitivity and scale of the processing, presumably to permit the officer to fulfil their tasks in accordance with Art. 39(2).

Links to further information

[Press release](#)[DPO guidance](#)

SHOOSMITHS SAYS...

A reminder of the basics of the DPO role.

Enforcement & legal action

Jurisdiction: **US (Texas)**



AG sues insurers for unlawful use of driving data

13 January 2025

Key details

The Texas Attorney General (AG) has filed a lawsuit against an insurance group for unlawfully collecting, using, and selling the driving data of over 45m people in the US.

The lawsuit alleges that the group paid app developers to embed tracking software in mobile phone apps to monitor location data, alongside information about the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy, without the phone user's knowledge. This data was apparently used to create "the world's largest" driving behaviour database used by the group and other insurers to assess premiums.

The claim is based on breaches of the Texas Data Privacy and Security Act (TDPSA) which requires clear notice and informed consent before collecting or using sensitive data such as geolocation. It also alleges that the insurance group's practice of buying driver data direct from manufacturers breaches state data and insurance law.

It is the first action taken under the TDPSA, which entered into force on 1 July 2024.

WHAT THEY SAY...

“the first enforcement action ever filed by a State Attorney General to enforce a comprehensive data privacy law”

Links to further information

[Press release](#)

[Claim](#)

Jurisdiction: **EU (Netherlands)**Marketing, adtech &
cookies

Court allows class privacy action against Google

15 January 2025

Key details

An Amsterdam court has allowed a representative claim brought by two organisations to proceed against various Google group companies for unlawfully infringing the privacy of Android phone users. The class action, backed by a litigation funder, represents over 100,000 Dutch Android users who claim that Google's processing of personal data infringes the GDPR and national data protection law.

The court's central finding was that the claims of all data subjects in the group were "similar" as required under Dutch law and could therefore be considered together. Even though individuals would be subject to slightly different processing at different times, all the claims were "legal actions aimed at protecting similar interests". The court potentially allowed for damages both for substantive and non-material damage, at levels which could be grouped into different classes under national law.

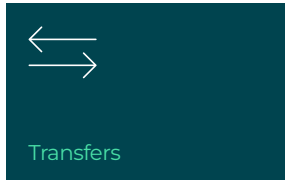
In the UK the civil procedure rules require representatives to have the 'same interest', inhibiting claims.

SHOOSMITHS SAYS...

The low countries
opening the floodgates
to class claims.

Links to further information

[Ruling](#)



NOYB challenges six Chinese companies on data transfer

16 January 2025

Key details

The Austrian rights group NOYB has published complaints against six Chinese companies, including TikTok, Shein, and Xiaomi, to various European data protection authorities over unlawful transfers to China of personal data subject to the GDPR.

The key allegations are:

- transfers are made using SCCs under Art. 46 of the GDPR as there is no adequacy decision, but these are “severely compromised” by Chinese national law
- particular concerns are localisation requirements, lack of effective data subject rights, and unfettered access by Chinese authorities, contrary to EU data protection requirements.

The complaints call for immediate cessation of transfers, compliance orders and fines of up to 4% of global revenue. This is NOYB’s first action against Chinese firms, following previous actions against US companies based on unlawful transfers.

The complaints have been made to data protection authorities in Greece, Austria, the Netherlands, Belgium and Italy on the basis of data subject residence. NOYB is attempting to avoid the case being transferred to the Irish regulator under the one stop shop mechanism by arguing that the EU-based subsidiary companies are not “main establishments” for the purposes of Art. 56. For example, it cites the Irish Tik Tok entity comprising only a “mailbox address” to a law firm.

Links to further information

[Statement](#)

WHAT THEY SAY...

“the rise of Chinese apps opens a new front for EU data protection law”



FTC takes action against car manufacturer over geolocation data

16 January 2025

Key details

The Federal Trade Commission (FTC) has published a proposed order and settlement with General Motors (GM) group companies for wrongfully collecting and selling drivers' precise geolocation and driving behaviour data through services which provide emergency assistance and traffic navigation in connected vehicles.

The FTC alleged that the group used a misleading enrolment process contrary to the Federal Trade Commission Act, resulting in consumers not being aware of the data collection and use, which included sharing with insurance companies to decide premiums.

Under the proposed settlement, the affected companies must:

- not share data with consumer reporting agencies for a period of five years
- obtain explicit prior consent before collecting data except for specified uses relating to safety and legal claims
- allow consumers to withdraw consent, and access and delete their data
- provide options to limit location data collection and decline enrolment.

Following publication on the Federal Register, the proposed order will be open for public comment for 30 days before being finalised.

WHAT THEY SAY...

“the FTC’s first action related to connected vehicle data”

Links to further information

[Press release](#)

[Proposed order](#)



Sensitive data &
vulnerable individuals

Supreme Court upholds TikTok ban

17 January 2025

Key details

The US Supreme Court has refused to overturn laws requiring TikTok's owners to transfer control to a US company under the Protecting Americans from Foreign Adversary Controlled Applications Act, passed in April 2024.

Following a number of failed legal challenges on the grounds of free speech, the group had asked for a delay in exercise of the effective ban on US operations, due to take effect on 19 January 2025. However, the Supreme Court unanimously refused to overturn the law, finding it constitutional. The court noted that under its assessment of Chinese laws, data was "susceptible to being used to further the interests of the Chinese Government".

TikTok temporarily suspended the site on 18 January resulting in the site being unavailable and the app being removed from the Apple App Store and Google Play Store in the US.

The ban was originally proposed by President Trump in 2020. The President has since indicated that TikTok would be given a 90-day reprieve and that he would prefer 50% US ownership. Relying on this assurance and a new Executive Order, the sites are operational again, although the legal basis for ignoring the Supreme Court decision is not clear and is likely to cause ongoing concern. TikTok is still not available on major app stores in the US.

SHOOSMITHS SAYS...

A first: Max Schrems and the US Supreme Court coming to the same conclusion (though for different reasons).

Links to further information

[Opinion](#)

Jurisdiction: **EU (Spain)**

DPA issues fine for unlawful use of biometric data

17 January 2025

Key details

The Spanish data protection authority, the AEPD, has imposed a €220,000 fine on a paper manufacturer for infringement of the GDPR. It follows an investigation after a former employee complained about the company's use of a facial recognition system for clocking in employees.

The company had been using the system since before 2016. When the company was sold in 2022 the new owner instituted a replacement system not based on biometric recognition, but this was not in place until 9 months later. It did not carry out a DPIA, even when the likely infringement was detected. The AEPD also found that the controller failed to respond adequately to the employee's subject access request, sending it late and to the wrong address.

The controller was therefore fined €220,000 for breaching Art. 35 and Art. 15 of the GDPR (for the DPIA and DSAR failings respectively) and was ordered to confirm compliance with the access request within 30 days.

It follows a similar AEPD fine in December 2024 of a football club for unlawful use of a biometric system to access its stadium.

Links to further information

[Ruling](#) (Spanish only)

[Ruling \(football club\)](#) (Spanish only)

SHOOSMITHS SAYS...

Clocking on to GDPR
compliance a bit late.



UODO fines bank for insufficiently senior DPO

20 January 2025

Key details

The UODO, the Polish data protection authority, has published details of a fine of PLN 576,220 (approx. €135,000) imposed on a bank for GDPR breaches. The violations included:

- putting the data protection officer in a role which required reporting to the security director responsible for data processing, rather than directly to senior management (Art. 38(3), accounting for 45% of the fine)
- failing to carry out a DPIA and not recording credit scoring and risk profiling activities carried out on customers (breaching Arts 35, and 30(1)). The bank also failed to assess the security implications of this data processing.

An aggravating factor was the length of non-compliance – over three years – even though there was no evidence of damage to data subjects as a result of the breaches.

SHOOSMITHS SAYS...

A reminder of the importance of DPO independence.

Links to further information

[Press release](#)

[Decision](#)



Marketing, adtech & cookies

ICO fines company £200,000 for text marketing

22 January 2025

Key details

The UK Information Commissioner's Office (ICO) has announced a £200,000 fine of a marketing company engaging in nuisance text messaging.

Responding to over 38,000 complaints, the ICO found that the company was instigating the transmission of over half a million texts per day between September 2022 and December 2023 without valid consent, contrary to Regulation 22 of the Privacy of Electronic Communications Regulations 2003 (PECRs).

The investigation included executing a search warrant and seizure of devices from the registered address of the company. The ICO found Skype messages admitting non-compliance, redaction of supplier information sent to the FCA, and hiding behind unregistered SIM cards. The ICO states that it found that the company directors knowingly facilitated unlawful activity for financial gain, although it does not have any further information about criminal prosecution.

WHAT THEY SAY...

“our commitment to protect people by unpicking tangled webs of deceit”

Links to further information

[ICO statement](#)

[Enforcement notice](#)

Enforcement & legal action

Jurisdiction: **UK**

CMA launches SMS investigation into Google and Apple

23 January 2025

Key details

The UK Competition and Markets Authority (CMA) has announced that it is investigating Apple and Google in relation to alleged dominance in mobile operating systems, app stores, and browsers, under new powers in the Digital Markets, Consumers and Competition Act (DMCC).

It will determine if the companies hold “strategic market status” (SMS) in these markets and if so whether they are leveraging their market power unfairly or imposing exploitative terms on app developers. The CMA will also consider whether to impose “conduct requirements” such as granting competing apps easier access to key functionalities or enabling app downloads outside proprietary app stores.

The CMA will conclude its investigations by 22 October 2025. It is already investigating Google in relation to search services under the DMCC.

The CMA has also indicated in a report issued on 29 January 2025 (linked) that it is considering designating AWS and Microsoft as having SMS in relation to cloud services.

WHAT THEY SAY...

“UK revenue for app development is estimated to be around £28 billion”

Links to further information

[Press release](#)[Cloud services decision](#)



Marketing, adtech & cookies

High Court rules on consent for direct marketing

23 January 2025

Key details

The England and Wales High Court has found that a gambling company unlawfully processed a recovering gambling addict's personal data for profiling and direct marketing, as the consent obtained did not meet the required standards under data protection law.

The court determined that UK data protection law requires a “relatively high and context-specific standard of consent”. In this case, the claimant's behaviour impaired their ability to freely give consent; in addition the controller could not rely on Art. 6(1)(f) as a lawful basis as it had no legitimate interest in marketing gambling advertisements to problem gamblers.

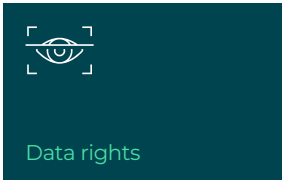
The court granted declaratory relief to the claimant, with compensation dependent on evidence of harm caused by the unlawful processing, and the issue of causation.

WHAT THEY SAY...

“direct marketing to gamblers occupies a far place along a spectrum”

Links to further information

[Judgment](#)



High Court rules on DSAR responses

27 January 2025

Key details

The High Court of England and Wales has published a judgment which examines the nature of personal data and the scope of DSAR responses. It arose when an individual challenged the response given by HMRC to an access request in the context of his tax affairs.

The court found:

- providing mere “snippets” of information (such as initials or a name with no context) in a DSAR response may not suffice if additional information is essential for the requester to assess lawfulness or exercise their rights
- for the definition of personal data, the ICO’s approach on the meaning of “relating to” was correct, such that a house valuation could be personal data about its owner in some contexts (tax affairs) but not in others (a survey of local house prices)
- information about an underlying decision-making process may, but does not always, constitute the affected individual’s personal data.

In this case, the court found that HMRC had not responded sufficiently to the request. It followed reasoning in CJEU cases which were not binding, finding them “persuasive”. This suggests that the EU court will continue to have significant influence on UK data protection law.

Links to further information

[Judgment](#)

SHOOSMITHS SAYS...

A high value decision on some taxing DSAR issues.



Industry & sector news



Location data broker reports major breach

4 January 2025

Key details

Gravy Analytics, a US-based location data broker, has reported a major personal data breach to the Norwegian and UK data protection authorities following the theft of location data from various consumer apps, including fitness, health, dating, and transit apps, reportedly including Spotify, Vinted, Candy Crush, and Tinder. The breach resulted from a misappropriated key allowing access to information stored on AWS.

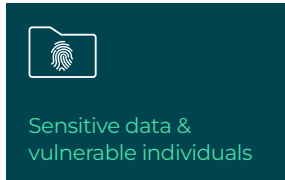
The breach follows an announcement on 3 December 2024 by the US Federal Trade Commission of a proposed order banning Gravy and a subsidiary from selling location data without consumer consent, contrary to the FTC Act. The breach has raised concerns about how such data is collected, sold, and used especially for vulnerable groups. The FTC states that the companies process “more than 17 billion signals from around a billion mobile devices daily”.

Links to further information

[FTC press release](#)

SHOOSMITHS SAYS...

A beef with Gravy.



Meta announces changes to content moderation in US

7 January 2025

Key details

Meta has announced that it is ending its third-party fact-checking programme in the US and replacing it with a Community Notes model inspired by practices on X.

It says that it is aiming for transparency and reduced bias. Restrictions on mainstream topics like immigration and gender identity will be lifted, with enforcement focused on illegal and severe violations. Meta will target user-reported issues, have a higher threshold for content removal and issue more details about enforcement errors. Political content (called “Civic Content” by Meta) will be personalised, allowing users to see more or less of it based on preferences.

The policy has raised significant concern in Europe and elsewhere, notably Brazil. There is no indication that content moderation practices outside the US will be changed immediately. In Europe, future policy may depend on the success of Commission enforcement of the EU Digital Services Act, which contains various obligations for very large online platforms relating to content and recommender systems. The UK Online Safety Act largely governs illegal, rather than harmful, content, although it notes that “tech firms will need to make sure their moderation teams are appropriately resourced and trained”.

Links to further information

[Announcement](#)

[Ofcom press release on OSA](#)

SHOOSMITHS SAYS...

Meta-morphosis.



Advocacy groups publish open letter on food delivery and AI fairness

13 January 2025

Key details

Twelve organisations, including unions, Privacy International and Amnesty International, have issued an open letter to three market-leading food delivery platforms asking them to address algorithmic transparency to improve worker protection and comply with upcoming laws.

The organisations criticise the platforms for automating decisions that affect pay and work allocation without clear explanation, increasing the precarity of work in the gig economy.

The letter asks for:

- a public register of algorithms used to manage workers
- clear explanations for algorithmic decisions and guidance on how to challenge them
- independent testing of algorithms by workers, representatives, and public interest groups.

The signatories argue that responsible platforms should lead by example and pre-empt stricter regulation including under the EU AI Act and Platform Workers Directive.

WHAT THEY SAY...

“current systems withhold vital information from workers”

Links to further information

[Open letter](#)

Marketing, adtech &
cookies

IAB responds to EDPB on consent or pay

16 January 2025

Key details

The Interactive Advertising Bureau (IAB Europe), an advertising industry body, and its allies have responded to the EDPB on 'consent or pay' models. It follows the publication of the EDPB Opinion in April 2024 which found that a binary choice between consent and pay would not lead to valid consent for large platforms "in most cases".

The IAB's position is that:

- 'freely given consent' should be based on an understanding that users can choose between options, or seek alternative services instead
- businesses should not be required to offer services for free or at a loss
- personalised ads are crucial for revenue and free or cheap online services may not be financially viable based on contextual ads alone
- consent or pay models have already been recognised as potentially lawful by the CNIL and Norwegian DPA, and by the CJEU in its July 2023 Bundeskartellamt ruling.

The paper criticises the EDPB approach, pointing out its lack of mandate in competition law and control of digital markets. The ICO has since published its own guidance on consent or pay models (also in the update this month).

Links to further information

[Press release](#)[Feedback paper](#)

SHOOSMITHS SAYS...

The IAB refusing to consent to the EDPB's view or pay the consequences.



Chinese DeepSeek AI app disrupts US markets

28 January 2025

Key details

US tech markets have been severely affected by massive uptake of DeepSeek, a new AI capability developed by two Chinese companies, which caused the biggest single day loss in US market history – \$600 billion – by a chip manufacturer.

The app provides various freely available generative capabilities including a ChatGPT-style LLM, code generator, and maths calculator. The company claims that it has been developed with less compute power, time and money than US equivalents, saying it was developed for “less than \$6m”. While not verified, the company appears to have achieved considerable savings by applying novel technology, leading President Trump to welcome it as a “wake up call” to US developers.

The app’s privacy policy describes the data which is collected from users and confirms that it is stored in servers in China under the control of two Chinese registered companies. It includes profile information, user prompts, technical information, usage information, cookies and payment information. Security concerns will only increase after the company paused registrations for new users after reporting “large scale malicious attacks”.

The Italian data protection authority, the Garante, has since announced that it has issued an order to the companies to cease processing on the grounds that they are bound by the extra-territorial effect of the GDPR under Art. 3(2), although this is denied by the companies.

Links to further information

[Privacy policy](#)

[Company announcement](#)

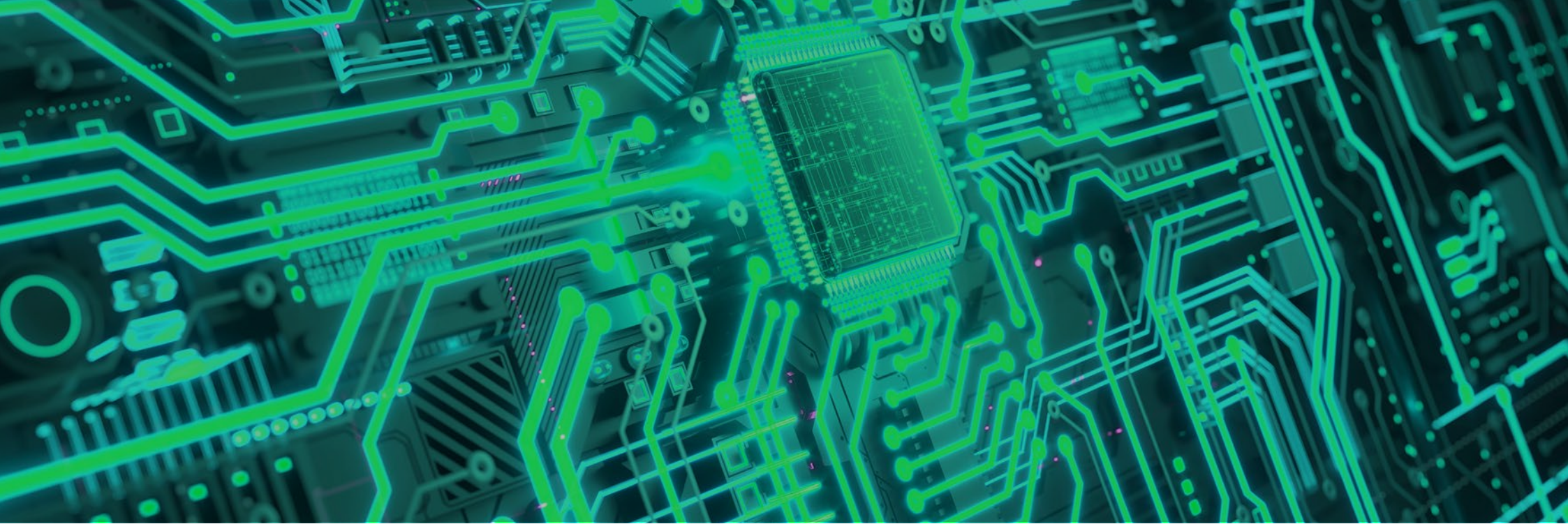
[Garante order](#)

[ICO guide to international transfers](#)

[Shoosmiths article](#)

SHOOSMITHS SAYS...

China crisis.



**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: February 2025

©Shoosmiths LLP 2025

SHOOSMITHS

www.shoosmiths.com

**FOR
WHAT
MATTERS**