



SHOOSMITHS

# Global privacy and data update

December 2024

[www.shoosmiths.com](http://www.shoosmiths.com)

FOR  
WHAT  
MATTERS



Legislation



Guidance & consultations



Enforcement & legal action

## THE **BIG** STORY



EDPB publishes  
opinion on AI models

18 DECEMBER 2024



Industry & sector news



INDEX

# Quick read: what you need to know about in December 2024

## AI

The EDPB publishes its opinion on the use of personal data for AI models.

South Korea approves new laws to regulate AI.

The UK expects its first class action over use of personal data in developing AI systems.

The Italian regulator issues a fine over the use of ChatGPT and issues a formal warning to a media group about sharing editorial content with OpenAI.

## Breaches

New York agrees a \$11.3m settlement with two insurance companies following cyberattacks on car insurance quoting systems.

Spain fines a telecoms company €1.3m for a data breach affecting millions launched through a phishing attack on an employee.

The Irish DPC announces finances of €251m on Meta for data breaches on Facebook.

## Cybersecurity

The US Treasury confirms a “major cybersecurity incident” attributed to China.

Canada passes laws on cyber resiliency in the telecommunications, energy, nuclear, transport, and banking sectors.

The European Commission starts legal action for failing transpose the NIS 2 Directive against 23 EU member states.

## Court action

NOYB announces approval as a “qualified entity” for “representative” (class) actions across the EU.

Apple agrees to settle a class action based on allegations that Siri “spies” on users.

TikTok requests an emergency injunction to delay the effect of the January US ban.

## Transfers

The US Department of Justice issues its final rule on sensitive transfers of data to “countries of concern”.

The EDPB drafts guidelines on how the private sector should respond to requests for information under Art. 48 of the GDPR, and calls for greater scrutiny of adequacy decisions.

## Marketing

The CNIL announces a €50m fine for inbox advertising by Orange email.


The South Korean PIPC fines four car insurance companies over marketing practices.

The UK ICO opens a consultation on cookies and tracking technologies, and criticises Google’s plans to allow device fingerprinting.

The California privacy regulator pursues four data brokers for failure to register under the “Delete Act”.

# Index

## Legislation















9	 Monaco updates data protection laws.....	<b>MONACO</b>
10	 EU establishes standards for digital wallets.....	<b>EU</b>
11	 Regulations to determine turnover for SMS laid before Parliament.....	<b>UK</b>
12	 Greece transposes NIS 2 Directive into national law.....	<b>EU (Greece)</b>
13	 Hungary advances new NIS 2 draft cybersecurity law.....	<b>EU (Hungary)</b>
14	 New Canadian cybersecurity bill passes Parliament.....	<b>CANADA</b>
15	 Ofcom publishes first Online Safety Act codes.....	<b>UK</b>
16	 Commission sends formal notices on DSA to member states.....	<b>EU</b>
17	 South Korean assembly passes AI bill.....	<b>SOUTH KOREA</b>
18	 DoJ issues final rule on sensitive data transfers.....	<b>US</b>

**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

20	 Financial regulators finalise guidance on critical suppliers.....	<b>UK</b>
21	 ENISA releases cybersecurity investment report.....	<b>EU</b>
22	 DRCF issues paper on synthetic media .....	<b>UK</b>
23	 EDPB publishes letter on DPA role in AI Act.....	<b>EU</b>
24	 EDPB drafts guidelines on responding third country requests under Art. 48.....	<b>EU</b>
25	 ESAs publish reminder on critical suppliers under DORA.....	<b>EU</b>
26	 EDPB publishes letter on adequacy decisions .....	<b>EU</b>
27	 ICO extends public sector approach to fining.....	<b>UK</b>
28	 ICO responds to consultation on generative AI.....	<b>UK</b>
29	 Government proposes copyright rules for AI development .....	<b>UK</b>
30	 DSIT publishes algorithmic transparency records.....	<b>UK</b>
31	 EDPB publishes opinion on use of personal data for AI models.....	<b>EU</b>
32	 Commission publishes second draft GPAI Code of Practice.....	<b>EU</b>
33	 ICO opens consultation on cookies and tracking technologies.....	<b>UK</b>

**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

35	Garante orders bank to notify data subjects after breach.....	<b>EU (Italy)</b>
36	DPC fines council for unauthorised CCTV.....	<b>EU (Ireland)</b>
37	FCC proposes \$735,000 fine of Hong Kong video doorbell company.....	<b>US</b>
38	DPA issues €5,000 fine for assumption of consent.....	<b>EU (Spain)</b>
39	Tech companies face class action over AI training data.....	<b>UK</b>
40	Insurance companies settle data breach for \$11.3m.....	<b>US (New York)</b>
41	Commission starts NIS 2 enforcement against 23 member states.....	<b>EU</b>
42	CJEU clarifies Art. 14 of the GDPR.....	<b>EU</b>
43	Belgian DPA fines loyalty scheme €5,000 for GDPR violations.....	<b>EU (Belgium)</b>
44	Garante warns news company over data sharing with OpenAI.....	<b>EU (Italy)</b>
45	NOYB announces “QE” status for representative actions.....	<b>EU</b>
46	Garante issues €842k fine for unlawful telemarketing.....	<b>EU (Italy)</b>
47	FTC proposes consent order for false FRT claims.....	<b>US</b>
48	AEPD fines phone company €1.3m for security failings.....	<b>EU (Spain)</b>
49	Court of Appeal confirms 2019 fine for data breach.....	<b>UK</b>
50	Orange mail attracts €50m fine for inbox advertising and cookies.....	<b>EU (France)</b>
51	Court of Appeal refuses class MOPI claim.....	<b>UK</b>
52	CNIL issues formal notices over cookie banners.....	<b>EU (France)</b>
53	PIPC fines car insurance companies over marketing.....	<b>SOUTH KOREA</b>
54	DPC fines Meta €251m for “View As” data breaches.....	<b>EU (Ireland)</b>
55	Garante fines estate agency over data kept on paper.....	<b>EU (Italy)</b>
56	APD announces €200,000 fine for hospital ransomware.....	<b>EU (Belgium)</b>
57	Bavarian DPA orders corrective measures on Worldcoin.....	<b>EU (Germany)</b>

### 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

58	 Garante announces €15m fine for ChatGPT.....	<b>EU (Italy)</b>
59	 California settles four actions for failure to register by data brokers.....	<b>US (California)</b>
60	 Apple settles Siri “spying” class action.....	<b>US (California)</b>

## Industry & sector news

62	 TikTok announces controls on beauty filters for under 18s.....	<b>GLOBAL</b>
63	 VW suffers vehicle geolocation data breach.....	<b>EU</b>
64	 Doughnut franchise files SEC report after cyber attack.....	<b>US</b>
65	 TikTok asks for emergency injunction to stop ban.....	<b>US</b>
66	 ICO responds to Google plans on fingerprinting.....	<b>UK</b>
67	 US Treasury confirms hack by Chinese state actors.....	<b>US</b>

**Key:**

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



# Legislation





## Monaco updates data protection laws

28 November 2024

### Key details

The Principality of Monaco has updated its data protection laws to bring them further into line with the GDPR and has announced that it expects to ratify Convention 108.

The law introduces new requirements for personal data processing heavily based on the GDPR, and in particular:

- mandates the appointment of a DPO
- increases fines to a maximum of €10m
- puts in place a regime for the international transfer of personal data
- creates a new regulator, the APDP, to replace the current CCIN.

The alignment with the GDPR is hoped to result in an adequacy decision from the EU to permit international transfers of personal data subject to the GDPR into Monaco without additional safeguards. The Principality currently has no trade agreements with the EU due to concerns over financial regulation and the risk of creating backdoors into more highly regulated regions.

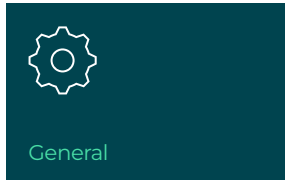
### Links to further information

[Text of law](#) (French only)

[Press release](#)

### WHAT THEY SAY...

**“will contribute to the appeal and development of Monaco’s economic status”**



## EU establishes standards for digital wallets

28 November 2024

### Key details

The European Commission has adopted implementing regulations which will permit development of European Digital Identity (eID) Wallets.

Made under the European Digital Identity Framework, the new laws will make wallets available from 2026 to provide secure payment and authentication services across the EU. Each member state must provide at least one wallet designed to agreed standards. The wallet will be available to any EU citizen, resident or business in the EU, but use will be optional.

The aim is that companies will adopt it in response to public demand and to avoid dependence on third party solutions which rely on data monetisation.

Possible uses include travel and residency authentication, banking and payment authorisation, and accessing public services and benefits.

Key features of wallets are:

- interoperability across the EU
- free of charge and non-discriminatory use
- local data storage
- use without tracking or profiling
- a privacy dashboard to control data sharing.

The regulations will be published in the Official Journal of the European Union shortly and will take effect 20 days after publication.

### Links to further information

[Press release](#)

### WHAT THEY SAY...

**“offers private users and businesses a universal, trustworthy and secure way to identify themselves”**



## Regulations to determine turnover for SMS laid before Parliament

29 November 2024

### Key details

The UK government has laid before Parliament the final text of regulations made under the Digital Markets, Competition and Consumers Act 2024 (DMCC) concerning the designation of companies with “strategic market status” (SMS).

The SMS regime is due to come into force on 1 January 2025. It is designed to permit the Competition and Markets Authority to regulate digital markets more effectively by identifying and controlling the most influential entities, similar to the gatekeeper regime under the EU Digital Markets Act.

Under s.7 of the DMCC, a company can only be designated as having SMS if it passes the turnover condition, in addition to other factors. The regulations set out SMS turnover designation thresholds, currently triggered by group turnover of over £1 billion in the UK or £25 billion globally (para 2). They also set out how turnover will be estimated (Schedule 1) as well as specifying turnover for determining penalties under the digital markets regime.

### SHOOSMITHS SAYS...

Enabling the UK to send strong messages through SMS.

### Links to further information

[Regulations](#)



## Greece transposes NIS 2 Directive into national law

4 December 2024

### Key details

The European Commission has issued an implementing regulation setting out transparency reporting standards for providers of intermediary services and online platforms under the EU Digital Services Act (DSA).

All in-scope intermediary services must disclose content moderation activities (Art. 15), with additional disclosure duties for hosting services. Online platforms must also share information about numbers of active users and dispute handling (Art. 24). VLOPs and VLOSEs must comply with further rules in Art. 42.

The reports must be publicly accessible and retained for five years. Duties begin on 1 July 2025, with transitional provisions to ensure that all service providers, including very large platforms and search engines which have been under transparency obligations for some time, can align with the new procedures and reporting periods.

The Regulation includes templates for quantitative and qualitative data.

### WHAT THEY SAY...

**“it may sound technical,  
but it concerns a huge part  
of our daily lives”**

### Links to further information

[Press release](#)

[Laws](#)



## Hungary advances new NIS 2 draft cybersecurity law

4 December 2024

### Key details

The Hungarian Parliament has advanced a new law on cybersecurity to its Legislative Committee, due to come into force on 1 January 2025.

Hungary originally transposed the NIS 2 Directive in 2023 via its “Act XXIII of 2023 on cybersecurity certification and supervision”. However, there were concerns about the lack of tailoring into member state law, and the European Commission began enforcement action in November 2024 against Hungary (along with most other member states) for failure to fully transpose in time.

This new cybersecurity law introduces a more comprehensive framework. It includes additional security provisions including some relating to post quantum encryption, due to come into force on 1 June 2025.

SHOOSMITHS SAYS...

**Hungary for more cybersecurity.**

### Links to further information

[Law](#)



## New Canadian cybersecurity bill passes Parliament

5 December 2024

### Key details

Bill C-26, enacting the Critical Cyber Systems Protection Act, has passed the Canadian Parliament. It creates a framework for cyber resiliency within “critical cyber systems” in the telecommunications, energy, nuclear, transport, and banking sectors.

Designated operators must implement a cybersecurity programme, mitigate supply chain and third-party risks, and report incidents affecting critical cyber systems to the Communications Security Establishment and the appropriate regulator within 72 hours. The government has powers to expand the list of “vital” systems and services within the scope of Canadian Parliamentary powers, which may exclude some commercial and health sectors.

Part 1 of the Bill also strengthens government powers in relation to the cybersecurity of telecommunications service providers, including inspection and remedial powers, and suspension of services.

Penalties in the Act may reach CAD15m per violation. Applicable dates will be determined when Royal Assent to the Bill is granted.

### WHAT THEY SAY...

**“cyber systems are critically important to vital services and vital systems”**

### Links to further information

[Bill](#)

[Tracker](#)



## Ofcom publishes first Online Safety Act codes

16 December 2024

### Key details

Ofcom has released its illegal harms guidance and codes of practice under the UK Online Safety Act, marking the beginning of enforceable standards and triggering compliance obligations for in-scope platforms. In-scope services must complete a risk assessment by 16 March 2025 to identify and address threats posed by illegal content to both children and adults.

The Act applies to providers of user-to-user services and search services, and will include social media, messaging services, gaming, search engines, and pornography sites. Duties under the OSA begin on the day when a relevant code of practice comes into force. Compliance with a code of practice is not compulsory but will be evidence of compliance (sections 49 to 51).

The package of measures includes codes of practice on illegal content for user to user and search services, and guidance on risk assessment and risk profiles, the register of risks, record-keeping and review, and enforcement.

Ofcom expects to issue further guidance relating to age-assurance for pornography platforms (January 2025), protecting women and girls (February 2025) and further protections for children (April 2025). It will issue further codes in Spring 2025 on terrorism and CSEA content, triggering further duties.

The regulator has also opened a consultation, closing on 10 March 2025, on the framework for Technology Notices, which can require companies to use or develop specified technology to address terrorism-related and CSEA content.

### Links to further information

[Press release](#)

[Guidance and codes](#)

### WHAT THEY SAY...

**“for too long, sites and apps have been unregulated... that changes from today”**

Accountability &  
governance

## Commission sends formal notices on DSA to member states

16 December 2024

### Key details

The European Commission has started the procedures compelling member states to meet their obligations under the EU Digital Services Act (DSA) and Data Governance Act (DGA).

In respect of the DSA, which regulates search services and platforms hosting user content, the Commission sent a formal notice to Bulgaria and a reasoned opinion (the next step) to Belgium, Spain, the Netherlands, and Poland. These countries have not nominated or empowered a Digital Services Coordinator, or have failed to establish penalties for DSA violations, by the February 2024 deadline.

The Commission is already using the DSA to regulate very large search engines and platforms for example through disclosing information and amending terms and conditions of use. Member states must now set up enforcement regimes for obligations such as content moderation relating to smaller but in-scope online platforms hosting user content.

Under the DGA, which promotes data sharing between public sector bodies, the Commission has issued a reasoned opinion to ten countries for failure to appoint or empower an authority responsible for enforcing the Act.

The failures may ultimately lead to court action and daily fines in affected member states.

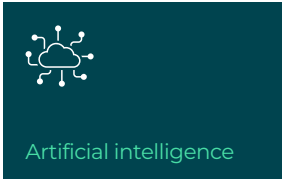
### Links to further information

[DSA press release](#)[DGA press release](#)

SHOOSMITHS SAYS...

The Commission urging member states to share its success in using the DSA.





## South Korean assembly passes AI bill

26 December 2024

### Key details

The National Assembly of South Korea has approved a bill to regulate AI. The “AI Basic Act” covers “high impact” systems in certain sectors including healthcare, energy, biometrics and public services, and various deployments of generative AI.

AI “business operators” providing products or services using high-impact or generative AI must notify users in advance. Operators of high impact systems also have to undertake various risk assessment and product compliance activities. Some non-Korean operators will be required to appoint in-country agents when deploying AI systems in South Korea. The Act provides for fines of up to around €20,000 for violation.

The Bill requires government review and publication in the Official Gazette before becoming law. It is likely to come into effect in early 2026.

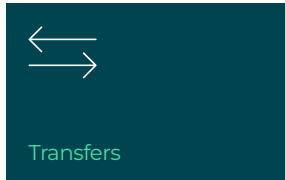
The Act also establishes a National Artificial Intelligence Commission to promote adoption and regulate covered technologies. South Korea hosted the second major international summit on AI in May 2024, following the inaugural Bletchley Park meeting 6 months earlier.

### Links to further information

[Bill information page](#)

### SHOOSMITHS SAYS...

Foundational AI approach from the home of the Seoul summit.



## DoJ issues final rule on sensitive data transfers

27 December 2024

### Key details

The US Department of Justice has issued its final rule implementing Executive Order 14117 on sensitive transfers of data to “countries of concern”.

It confirms controls over activities which risk access to bulk sensitive data by entities, individuals or governments in China (including Hong Kong), Russia, Iran, North Korea, Cuba and Venezuela. The DoJ has confirmed that it has particular concerns about the use of bulk datasets for the development of AI by hostile powers and subsequent targeting of key individuals in government.

Affected data includes human genomic (called “omic”) data, biometric identifiers, precise geolocation data, personal health data, personal financial data, and certain covered personal identifiers such as IP and email addresses when used in combination and above certain thresholds. It also controls access to non-bulk data concerning the location of government facilities or personnel.

Any contracts to non-US entities involving data likely to be covered will require restrictions on onward transfer to countries of concern. In addition, contracts involving “restricted transactions” such as covered supply and employment agreements must comply with CISA security standards. The rule is likely to cover a wide range of data transactions.

The rule will take effect 90 days after publication.

### Links to further information

[Press release](#)

[Rule](#)

### WHAT THEY SAY...

**“Americans’ personal data is no longer permitted to be sold to hostile foreign powers”**



## Guidance & consultations



## Financial regulators finalise guidance on critical suppliers

12 November 2024

### Key details

UK financial regulators have published a joint policy statement and oversight approach report on the designation and regulation of critical third parties (CTPs) supplying IT services to the financial services sector. The regime, established under the Financial Services and Markets Act 2023 (FSMA), focuses on entities whose service disruptions could impact financial stability.

The final rules and guidance will become effective on 1 January 2025, with HM Treasury due to make the first designations thereafter. The regulators: the Bank of England, the Financial Conduct Authority (conduct in financial services), and the Prudential Regulation Authority (banking stability) each have their own guidance based on common principles under the FSMA and will undertake enforcement following designation of a critical third-party supplier. The oversight approach report explains common principles such as the interpretation of “materiality”, “concentration” and other factors relevant to the test of criticality under the FSMA.

The framework will apply to technology providers including cloud services, AI and market data providers. CTPs will be subject to rules on operational risk, resilience, and incident reporting. CTPs already subject to relevant regulation will not be separately designated. Multinational CTPs may be subject to separate regimes, for example under the Digital Operational Resilience Act (“DORA”) in the EU.

### Links to further information

[Policy statement](#)

[Oversight approach](#)

### SHOOSMITHS SAYS...

The UK hand in hand (but slightly out of step) with the EU on the regulation of digital providers.



## ENISA releases cybersecurity investment report

21 November 2024

### Key details

ENISA, the EU Cybersecurity Agency, has published a report looking at the current state of investment in cybersecurity by highly critical entities subject to the Network and Information Systems Directive (NIS 2). It is designed to encourage strategic investment in cyber security by providing substantive evidence for stakeholders on NIS-driven investments.

The report contains data from 1,350 organisations across all member states and every NIS 2 sector of high criticality plus the manufacturing sector. Key findings are:

- most organisations expect to increase IT security spending as a result of NIS 2
- 90% of entities expect an increase in cyberattacks in 2025
- 92% of affected entities are generally aware of NIS 2
- awareness and engagement in newly in-scope sectors is lower than in established sectors, especially wastewater (60%), manufacturing (62%), and public administration (73%)
- only 51% of organisations have dedicated cybersecurity training for leadership, although 85% are involved in approving risk management measures
- 80% have not yet conducted supply chain audits for AI-related vulnerabilities.

### Links to further information

[Press release](#)

[ENISA report](#)

### WHAT THEY SAY...

**“the NIS 2 Directive signifies a turning point in Europe’s approach to cybersecurity”**



Artificial intelligence

## DRCF issues paper on synthetic media

26 November 2024

### Key details

The Digital Regulation Cooperation Forum (the DRCF) has released a paper on the future of synthetic media. The report examines the potential evolution of synthetic media, possible applications, and regulatory implications over the next three to five years.

It uses Ofcom's definition of synthetic media as "an umbrella term for video, image, text, or audio generated entirely or partially by AI algorithms". Beneficial uses include digital twins for product development, synthetic datasets for AI training to reduce the use of personal data, and developments in creative entertainment and personalised services.

The report notes the cross-cutting nature of risks posed, such as the FCA's concerns about market volatility due to misinformation, which might also constitute regulated content under the Online Safety Act. Unlawful processing of personal data may also constitute a misleading commercial practice under UK law.

The report notes that the ICO will consider the data protection implications of methods used to identify synthetic media and deepfakes in an upcoming Technology Horizons Report due in early 2025. The paper does not reflect official policy of the DRCF or its member regulators, the ICO, CMA, FCA and Ofcom.

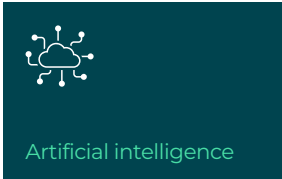
### SHOOSMITHS SAYS...

Useful synthesis of regulatory approaches in emerging tech use cases.

### Links to further information

[Paper](#)

Jurisdiction: **EU**



## EDPB publishes letter on DPA role in AI Act

28 November 2024

### Key details

The EDPB has published its letter to the AI Office setting out some principles for the regulation of AI from a data protection point of view.

The EDPB confirms that:

- regulatory co-operation will be a strategic priority
- the EDPB has started work on guidelines on the interplay between the GDPR and the AI Act
- it is the designated regulator of high-risk systems in relation to law enforcement, border control, the administration of justice and democratic processes.

The EDPB issued an Opinion on data protection in AI models on 18 December 2024.

WHAT THEY SAY...

**“considering the strong entanglement between the AI Act and data protection law”**

### Links to further information

[Letter](#)



Transfers

## EDPB drafts guidelines on responding third country requests under Art. 48

3 December 2024

### Key details

The European Data Protection Board (EDPB) has issued draft guidelines on Art. 48 of the GDPR which it has put out to public consultation.

Art. 48 requires that disclosures of personal data to authorities outside the EU made in response to a court order or administrative decision can only be made based on an international agreement, such as a mutual assistance treaty (MLAT), either at member state or EU level. The EDPB notes the increasing number of international treaties which set up mechanisms for direct transfer between public authorities and the private sector across territories.

The guidelines apply to public authority requests made to private sector organisations in the EU. The EDPB clarifies that:

- where there is an applicable MLAT, companies should generally refuse direct requests
- if there is no treaty or it does not contain appropriate safeguards, then another Chapter V transfer condition must be found (the EDPB does not consider Art. 48 a complete prohibition)
- where the Art. 48 condition is satisfied, transfers must still have a lawful basis for processing under Art. 6, and adhere to the principles in Art. 5
- a request does not in itself constitute a lawful basis for transfer
- where there is a treaty with appropriate safeguards, Art. 6(1)(c) is likely to be the appropriate lawful basis
- controllers may not store personal data on the basis of legitimate interests in order to be able to respond to future requests, although Art. 6(1)(f) may be an appropriate ground for a specific request “in exceptional circumstances”.

Public comments are invited on the guidelines until 27 January 2025.

### Links to further information

[Guidelines](#)

### SHOOSMITHS SAYS...

Key guidance on how companies should answer requests for information from overseas authorities.





## ESAs publish reminder on critical suppliers under DORA

4 December 2024

### Key details

The European Supervisory Authorities (ESAs) which regulate the financial sector have issued a statement regarding the upcoming application of the EU Digital Operational Resilience Act (DORA), which is a regime of cybersecurity, incident reporting and cyber supply chain management for financial entities.

They warn that in-scope financial entities must:

- identify and address any gaps in their operations to meet DORA requirements by 17 January 2025
- be able to classify and report their major ICT-related incidents from 17 January 2025
- maintain registers of their contractual arrangements with ICT third-party providers (CTPPs) by early 2025; supervisory authorities will report these to the ESAs by 30 April 2025.

Critical suppliers should assess their operations against DORA requirements and be ready for the first designation of CTPPs which is expected in the second half of 2025.

WHAT THEY SAY...

**“DORA does not provide for a transitional period”**

### Links to further information

[Statement](#)



Transfers

## EDPB publishes letter on adequacy decisions

5 December 2024

### Key details

The EDPB has published its letter to the Commission regarding the January 2024 review of the eleven existing adequacy decisions under the 1996 Directive and has suggested areas which require closer monitoring. The review applies to all current EU adequacy decisions except Japan and South Korea which were designated more recently.

The EDPB notes in particular that:

- the review did not provide a full report of national laws and practices in the territories concerned
- it would welcome a more comprehensive assessment of each country individually
- the reports are not consistent in their approach to all data protection concepts across every jurisdiction.

With respect to the data protection frameworks in the eleven countries, it calls for a fuller examination of:

- legal grounds for processing
- restrictions of data subject rights
- rules on automated decision making in light of AI development
- applicable legal frameworks, especially transfer mechanisms, which “appear to be, in some cases, very different from the ones set out under EU law”
- the use of personal data for law enforcement, national security, and intelligence purposes, and access to personal data transferred under adequacy decisions by relevant authorities.

### Links to further information

[Press release](#)[Letter](#)

### SHOOSMITHS SAYS...

A clear reminder that adequacy is a political as much as a legal decision.



## ICO extends public sector approach to fining

9 December 2024

### Key details

The UK Information Commissioner's Office, the ICO, has issued a statement confirming that the two-year trial of the "public sector approach" which effectively suspends or reduces fines in the public sector will continue but undergo public consultation on its scope and the factors that would make issuing a fine appropriate.

It follows a review of the approach, which noted that:

- public reprimands led to some improved procedures and security measures by public bodies
- the current approach led to limited awareness among wider public sector organisations
- there was a need for clear parameters to determine which organisations and infringements will fall within the more lenient policy.

The consultation closes on 31 January 2025.

### WHAT THEY SAY...

**"I have been conscious of the diversity of opinion on the approach and its impact"**

### Links to further information

[ICO statement](#)



## ICO responds to consultation on generative AI

12 December 2024

### Key details

The Information Commissioner's Office (ICO) has published its response to consultations on the application of the UK GDPR and the Data Protection Act 2018 to the deployment of generative AI.

The ICO's response summarises key feedback from over 200 stakeholders and outlines its position on areas like the lawful basis for using web-scraped data to train AI and incorporating individual rights into AI models. The only substantive changes to its previous positions are:

- confirmation that legitimate interests is the only available lawful basis for web scraping, but with more emphasis on the necessity aspect, and the difficulty of passing balancing tests without transparency
- a clarification that Art. 11 of the UK GDPR cannot be used to bypass obligations with respect to data subject rights.

The ICO highlights lack of transparency in the industry, especially regarding training data, which is eroding public trust. It calls on AI developers to provide clear, accessible information about data usage and ensure compliance with data protection laws, including embedding data protection by design.

The ICO plans to update its guidance based on the consultation outcomes.

### Links to further information

[Blog](#)

[Consultation response](#)

### SHOOSMITHS SAYS...

Confirmation of key positions for AI development.



## Government proposes copyright rules for AI development

17 December 2024

### Key details

The UK government has launched a consultation to clarify copyright laws for creative industries and AI developers.

The key proposals under consultation are:

- introducing a “text and data mining” exception to copyright law to permit use for commercial AI purposes
- allowing creators to opt-out by reserving rights to use their copyright material
- requiring AI developers to provide more information about the data used for training their models
- requiring labelling of AI generated content along the lines of the EU AI Act.

The government also aims to make it easier for creators to strike licensing deals with AI developers. Finally, it is seeking views on whether to legislate to protect individuals’ rights in the context of digital replicas, such as deepfake content, and on the regulation of computer-generated works.

The proposals are modelled in part on the EU position. The consultation acknowledges the difficulties in establishing technical standards and platforms for managing access controls and licensing. Reaction to the proposals has been mixed, with some smaller content creators concerned that “opt-out” rather than “opt-in” mechanisms will be difficult to manage and not deter scraping by powerful AI developers.

The consultation closes on 25 February 2025.

### Links to further information

[Press release](#)

[Consultation](#)

### WHAT THEY SAY...

**“it will require practical and technical solutions as well as good policy”**



## DSIT publishes algorithmic transparency records

17 December 2024

### Key details

The UK Department for Science, Innovation and Technology (DSIT) has published an updated list of records describing “algorithmic tools” used by government departments. These “algorithmic transparency records” include information on various government deployments of technologies such as chatbots, digital assistants, and systems for triage and automated document review.

The records provide a useful methodology for assessing commonly used AI tools which could also be of use to address various compliance requirements in the private sector.

For each tool, the records explain how and what data has been used to train the models in question, the technology used, benefits, a summary of key DPIA findings, and risk management measures. They also disclose which department(s) are responsible for and use the tool, together with its function, scope, what it replaced, which alternatives were considered, and how it makes decisions.

The list includes:

- chatbots from Network Rail and the Ministry of Justice
- HR and triage tools at various departments, including HM Treasury and the Foreign Office
- tools aiding NICE staff, visa applications, and pension calculations.

The government announced in its AI White Paper response in February 2024 that use and publication of the records is a requirement for central government departments, extending to the whole public sector in due course. A record is required for tools which have significant influence on a decision-making process with public effect or directly interact with the public. There are exemptions including for law enforcement deployments and commercially sensitive information.

### Links to further information

[Summary](#)

[Records](#)

### SHOOSMITHS SAYS...

Useful tools to build a trustworthy AI compliance framework.



## EDPB publishes opinion on use of personal data for AI models

18 December 2024

### Key details

The European Data Protection Board has published its opinion on the use of personal data for the development and deployment of AI systems. It is in response to specific questions asked by the Irish DPC under Art. 64 of the GDPR.

The opinion considers:

- whether AI models contain personal data, and when they can be considered “anonymous”
- legitimate interests as a possible lawful basis for model development and deployment, including application of the three-step test
- the effect of unlawful processing on subsequent use of an AI model.

The opinion is aimed at deployers rather than developers. The EDPB’s central view is that deployers will be able to use systems based on fully anonymised models regardless of any unlawful development, provided that they properly assess anonymity. Deployers of non-anonymous models must assess whether they were developed unlawfully and if so may be prevented from lawful use. The lawfulness of initial processing will also be a relevant factor in carrying out a legitimate interests assessment.

It notes that a declaration of conformity with the GDPR will be required for high-risk systems under the EU AI Act.

The opinion touches on, but does not explore in detail, lawful bases for web-scraping, use of special category data, rights to object to processing carried out on the basis of legitimate interests, data protection by design, joint controllership, automated decision-making, and purpose compatibility. The EDPB is currently developing guidelines on some of these specific questions including web-scraping.

### Links to further information

[Press release](#)

[Opinion](#)

WHAT THEY SAY...

**“the EDPB wants to support responsible AI innovation”**



## Commission publishes second draft GPAI Code of Practice

19 December 2024

### Key details

The European Commission has published an updated version of the draft General-Purpose AI Code of Practice under the EU AI Act, aimed at providers of general-purpose AI models and those with systemic risk for the purposes of compliance with Chapter V of the Act.

The new draft contains more detailed provisions and concrete examples, and includes first drafts of the specific KPIs being established for GPAI model providers under Art. 56 of the Act. It includes a more comprehensive Safety and Security Framework, including commitments to map specific risk tiers; additional measures for post-deployment monitoring and external risk assessments; an expanded taxonomy of systemic risks; and newly developed sections on serious incident reporting, whistleblowing protections, and public transparency.

The next draft, due in February 2025, is expected to include more granularity on KPIs, together with a template for reporting summaries of training data content (which will apply to all in-scope model providers). The Code must be finalised by 2 May 2025. The provisions on GPAI models in Chapter V will apply to models released after 2 August 2025, although the fining powers of the Commission in Art. 101 do not take effect until one year later. Pre-existing models must come into compliance by 2 August 2027.

### Links to further information

[Press release](#)

### WHAT THEY SAY...

**“ensuring that all parts of the Code fit together seamlessly and are easy to understand”**



Marketing, adtech &  
cookies

## ICO opens consultation on cookies and tracking technologies

20 December 2024

### Key details

The UK Information Commissioner's Office has opened a consultation on new draft guidance covering cookies and tracking technologies.

It is based on existing guidance, but with new detailed content on compliance, consent management and online advertising. It identifies a wide range of tracking technologies which are subject to the consent rules in the Privacy and Electronic Communications Regulations 2003 (PECRs), including cookies, tracking pixels, link decoration (enriching URLs with user information), navigational tracking, web storage, fingerprinting techniques, and scripts and tags, with the underlying principle that the purpose of the technology will determine whether it is covered by the regulations rather than any technical specification.

It includes illustrations of compliant and non-compliant cookie banners, and confirms that websites must not rely solely on browser settings to indicate consent, nor rely on terms and conditions or bundled consents. The ICO recommends refreshing consents for existing uses every 6 months, though this is just a guideline.

The new guidance on online advertising confirms that the “take it or leave it” approach (only offering services in return for non-essential personal data) will not comply with UK law. The draft does not include guidance on “consent or pay” which will be the subject of separate guidance in 2025. It also advises that ad measurement purposes do require consent, but this need not be separate from consent to general advertising purposes.

The consultation closes on 14 March 2024.

### Links to further information

[Consultation](#)[Draft guidance](#)

### WHAT THEY SAY...

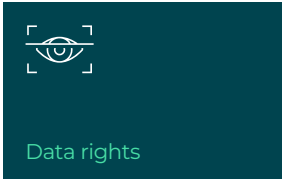
**“a significant update to the detailed cookies guidance”**



## Enforcement & legal action

# Enforcement & legal action

Jurisdiction: **EU (Italy)**



## Garante orders bank to notify data subjects after breach

2 November 2024

### Key details

The Italian data protection authority, the Garante, has ordered a bank to notify over 3,500 affected data subjects of a data breach under Art. 34 of the GDPR. The breach involved an employee accessing the financial data of over 3,500 customers out of “curiosity”, including details of high-profile individuals.

Under Art. 33, the bank reported to the Garante details of the breach relating to nine data subjects whose account information was directly affected. It also notified the data subjects under Art. 34. However, it did not report the wider unauthorised access and did not notify the other affected data subjects, arguing the breach was not “likely to result in a high risk” to their rights.

The authority disagreed, citing the sensitive nature of financial data and confidentiality standards in the banking sector, underlined in EDPB Guidelines. It noted that the bank could contact customers without disproportionate effort.

The bank was ordered to comply with Art. 34 within 20 days.

SHOOSMITHS SAYS...

**Useful steers on notification obligations in the financial sector.**

### Links to further information

[Order](#)



## DPC fines council for unauthorised CCTV

13 November 2024

### Key details

The Irish Data Protection Commission (DPC) has fined a County Council over the use of CCTV cameras and ANPR systems in various council- controlled locations including a harbour, bottle banks and housing estates. It found violations of provisions of the GDPR and of the Law Enforcement Directive (LED) as transposed into national law. The decision contains useful analysis of the contrasting roles of a public authority acting as controller under the GDPR and as competent authority under the LED.

Breaches included:

- failure to conduct a DPIA or have a CCTV policy
- lack of joint controller agreement with the local police force
- failure to identify a lawful basis for processing
- failure to secure monitoring screens against unauthorised screenshotting by staff
- excessive surveillance without justification
- excessive retention
- lack of logging and processing records
- lack of signage or explanation for the surveillance.

A fine of €29,500 was imposed, and the council was ordered to ensure compliance with data protection laws.

A few weeks later, the Swedish data protection authority (the IMY) fined a landlord SEK 200,000 (€17,000) for excessive surveillance in the common areas of an apartment building. It determined that the landlord's legitimate interests were outweighed by those of data subjects and found breaches of Arts 6(1) and 13 of the GDPR. It ordered the landlord to cease all surveillance within four weeks, except in the garage area, where it could be justified.

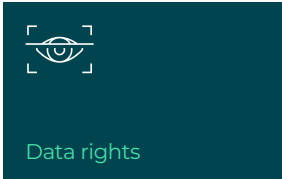
### Links to further information

[DPC decision](#)

[IMY press release](#)

SHOOSMITHS SAYS...

A reminder of the heavy responsibility which comes with the use of surveillance techniques, even if well-intentioned.



## FCC proposes \$735,000 fine of Hong Kong video doorbell company

21 November 2024

### Key details

The US Federal Communications Commission has issued a Notice of Apparent Liability for Forfeiture (NAL) against a Hong Kong manufacturer of video doorbells for allegedly maintaining false contact information for its US agent and ignoring an FCC inquiry.

The NAL is not yet made final, and the company will have an opportunity to respond. The same false contact address is apparently being used in hundreds of other certifications under the relevant FCC Rules, linked.

It follows allegations earlier in 2024 that third parties can easily take control of the doorbell by downloading the related app and holding down a button on the equipment. There are also concerns that information about IP addresses, unencrypted Wi-Fi details, and camera stills are transmitted on the open internet. The FCC says it is investigating these issues further.

### Links to further information

[Press release](#)

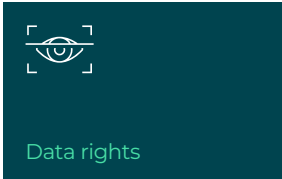
[Notice](#)

[2022 rules](#)

SHOOSMITHS SAYS...

**Not a ringing endorsement.**

Jurisdiction: **EU (Spain)**



## DPA issues €5,000 fine for assumption of consent

24 November 2024

### Key details

The Spanish data protection authority, the AEPD, has fined a law firm €5,000 for unlawfully publishing an employee's name and photograph on its website without valid consent.

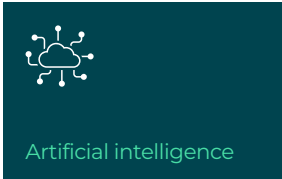
The controller claimed the data subject consented by posing for a photo and providing CV details, in response to a company email inviting employees to have optional photos taken for the website. However, the AEPD found no evidence of explicit consent to company use as required under Art. 4(11) and Recitals 32 and 42 of the GDPR. The assumption of consent without evidence of affirmative action, backed up by information about processing activities, violated Art. 6(1).

### SHOOSMITHS SAYS...

**A warning to controllers that they actually need to obtain consent, not infer it from a course of action.**

### Links to further information

[Resolution](#)



## Tech companies face class action over AI training data

25 November 2024

### Key details

A UK law firm has announced the launch of the first UK class action against Microsoft and Google related to the use of personal data in developing AI systems. The claim is open to anyone with an MS or Google account or who has ever used their products or services.

Although a claim has not yet been issued, the central allegation is that personal data including sensitive information is being used without proper consent, presumably contrary to the UK GDPR and Data Protection Act 2018.

The firm cites actions against the companies in California which hinge on various forms of unlawful conduct including breach of copyright law, rather than purely data protection considerations. In the UK, the copyright issue is in dispute in an action (Getty Images v Stability AI) awaiting trial in the High Court, with judgment expected in 2026.

The UK government has since opened a consultation on future legislation to clarify the copyright issue.

### SHOOSMITHS SAYS...

When it comes to AI training data, it looks as if the copyright issue may be resolved before the data protection one.

### Links to further information

[Claim page](#)

# Enforcement & legal action

Jurisdiction: **US (New York)**



## Insurance companies settle data breach for \$11.3m

25 November 2024

### Key details

The New York Attorney General and NY Department of Financial Services have reached an \$11.3m settlement with two insurance companies following data breaches in 2020-21 which exposed the personal information of state residents as part of a campaign to attack car insurance quoting systems.

Both companies were alleged to be in breach of the Cybersecurity Regulation (23NYCRR Part 500) which applies in the New York financial services sector.

As part of the settlement, the companies must pay the fines and implement stronger data security measures, including risk assessment. The Cybersecurity Regulation has been the subject of phased upgrades which will bring more entities and obligations into scope, ending in November 2025.

SHOOSMITHS SAYS...

**Insuring good  
cybersecurity.**

### Links to further information

[AG press release](#)

[NYDFS press release](#)





## Commission starts NIS 2 enforcement against 23 member states

28 November 2024

### Key details

The European Commission has initiated infringement procedures against 23 EU member states for failing to meet the 17 October 2024 deadline for fully transposing the Network and Information Systems (NIS 2) Directive.

Letters of formal notice were sent to all EU countries except Italy, Lithuania, Belgium and Croatia. Notably, the action includes Hungary and Latvia which both passed legislation purporting to transpose the Directive into national law before the deadline, reflecting concerns that the transposition was not sufficiently tailored to permit practical operation.

The Commission has taken equivalent action against 24 states in relation to the parallel Critical Entities Resilience Directive (CERD) which covers wider resiliency issues including non-cyber physical threats to critical infrastructure, and which carried the same implementation deadline.

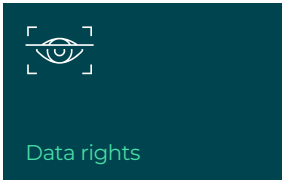
Member states now have two months to comply and notify the Commission, or face potential further action, including reasoned opinions. Failures to transpose can ultimately lead to Commission fines, although many countries have advanced NIS 2 implementation plans and are unlikely to incur penalties.

SHOOSMITHS SAYS...

They were slow to get going with NIS 1 as well.

### Links to further information

[Press release](#)



## CJEU clarifies Art. 14 of the GDPR

28 November 2024

### Key details

The CJEU has delivered its preliminary ruling (NAIH v UC, C 169/23) addressing the obligations under GDPR Art. 14(5)(c) when personal data is collected other than from the data subject.

The case arose after a complaint under Art. 77(1) alleging insufficient data protection in issuing COVID-19 vaccination certificates, and in particular the controller's failure to provide required information about processing such as purpose, legal basis, and data subject rights. The controller relied on the exemption in Art. 14(5)(c) which disappplies some data subject rights where it is subject to member state law and such law contains appropriate protective measures. It also argued that some of the personal data (such as the certificate number) was generated by the controller and not received from a third party and was therefore outside Art. 14.

The CJEU confirmed that Art. 14 applies to all personal data collected other than from the data subject, regardless of whether the data was obtained from third parties or generated by the controller. The court also clarified that in complaints about Art. 14(5)(c), supervisory authorities may check whether member state laws include appropriate measures to protect the data subject's legitimate interests to assess whether the exemption would apply, but this would not extend to evaluating security measures under Art. 32, since these would not be relevant to the exercise (and controllers remain subject to the rest of the GDPR in any event).

### Links to further information

[Judgment](#)

### SHOOSMITHS SAYS...

**Making sure controller-generated personal data is not immune from data protection law.**

Jurisdiction: **EU (Belgium)**



Marketing, adtech & cookies

## Belgian DPA fines loyalty scheme €5,000 for GDPR violations

28 November 2024

### Key details

The Belgian data protection authority has imposed a fine of up to €100,000 on a customer loyalty platform for breaches of the GDPR.

The platform collected and collated customer personal data from electronic ID cards for marketing purposes, sharing information between various brands. The authority found that it:

- failed to obtain valid consent, by withholding information about data sharing and other purposes when ID cards were presented
- did not make withdrawal of consent accessible and intuitive
- breached data minimisation principles by collecting unnecessary information from ID cards, such as the ID number
- retained personal data for 8 years without justification.

The authority also found that the practice of granting commercial advantages in return for non-essential data processing meant that consent could not be validly given.

The company has four months to revise its practices before a €5,000 daily fine is imposed up to a maximum of €100,000.

WHAT THEY SAY...

**“the massive centralisation of data directly from the chip of the eID card poses a high risk to the privacy of millions of consumers”**

### Links to further information

[Press release](#)

[Decision](#) (French only)



## Garante warns news company over data sharing with OpenAI

29 November 2024

### Key details

The Garante, Italy's data protection authority, has issued a formal warning to the GEDI media group regarding its agreement to share editorial content with OpenAI. The Garante raised concerns over potential GDPR violations, particularly regarding the sharing of personal and sensitive data, including criminal conviction data.

The group entered into agreements with OpenAI in September 2024 to ingest editorial content to allow ChatGPT users to search in real time for news content, and for use in AI training. The stated aim of the project was to protect its IP rights and reduce the risk of conveying fake news.

The Garante noted:

- legitimate interests (Art. 6(1)(f) of the GDPR) as a lawful basis for data processing cannot justify the use of special category or criminal convictions data
- a legitimate interest in processing personal data for journalistic purposes would not cover other uses, such as AI training
- late development of a data protection impact assessment (DPIA)
- the impossibility of letting data subjects object to processing if data were transmitted on 30 November as planned.

The authority warned that such data-sharing practices probably breach Arts 9, 10, and 12 to 23 of the GDPR and said it will conduct further investigation.

### Links to further information

[Press release](#)

[Formal warning](#)

SHOOSMITHS SAYS...

A new hope for return of the GEDI data.



## NOYB announces “QE” status for representative actions

2 December 2024

### Key details

None of Your Business, the Austrian-based privacy rights group, has announced approval as a “qualified entity” (QE) under the EU Representative Actions Directive (2020/1828) which will enable it to bring “representative” (class) actions across the EU. As a result, NOYB will be able to request injunctions, and redress measures including possible damages claims, on behalf of affected EU consumers where there is breach of consumer law including the GDPR.

NOYB has been approved as a QE in Austria and in Ireland but is able to bring representative claims in any EU country under the cross-border rules in Art. 6. The Directive enables QEs to bring actions for breaches of consumer laws listed in Annex I, which include the GDPR and the ePrivacy Directive. The list does not cover post-2019 consumer legislation, though it will be subject to review by 2028.

As a QE, NOYB is subject to various transparency duties under Art. 13 including the obligation to publish details of actions which they have “decided to bring”. NOYB says that it expects to bring its first actions in 2025.

The Directive does not prevent claims being brought under other provisions, for example the right to elect representative bodies in Art. 80 of the GDPR. This right can be problematic in practice, as seen in the recent refusal by the Belgian DPA (linked) to recognise the mandate of NOYB in relation to claim against Google and a media company over tracking and transfers via Google Analytics.

### Links to further information

[NOYB press release](#)

[Directive](#)

[Art. 80 action](#)

WHAT THEY SAY...

**“has the potential to be a game changer”**



Marketing, adtech & cookies

## Garante issues €842k fine for unlawful telemarketing

3 December 2024

### Key details

The Italian data protection authority, the Garante, has announced a fine of Sky Italia for unlawful telemarketing practices in relation to NOW TV.

After 275 complaints, the Garante's investigation found that the media company violated Arts 5(1)(a) and 6(1)(a) of the GDPR by:

- relying on outdated pre-GDPR consents
- not checking the RPO (the national Do Not Call registry)
- documenting consent in insecure files
- relying on consent apparently obtained as part of signing up to services without offering users the chance to opt out.

It confirmed that an invitation to activate a new subscription to NOW TV ("Reactivate with a click") would not constitute a service message exempt from consent requirements.

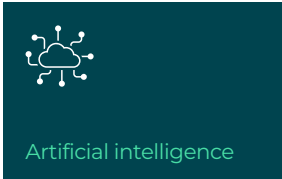
As well as the fine, the Garante ordered the controller to carry out checks on third party marketing lists and prohibited it from processing personal data for promotional purposes without the required consents.

SHOOSMITHS SAYS...

**A reminder of the importance of careful management of marketing consents.**

### Links to further information

[Order](#)



## FTC proposes consent order for false FRT claims

3 December 2024

### Key details

The US Federal Trade Commission (FTC) has proposed a consent order against a technology company for making misleading claims about its facial recognition technology (FRT) in breach of s.5(a) of the FTC Act.

The technology is embedded into home security products on sale in the US which can detect whether callers match pictures and IDs of permitted or banned people provided by the homeowner. They do not provide identification by matching against public databases.

The FTC proposed order is based on apparently false claims that the FRT solution was highly accurate, trained on millions of images, and free of racial or gender bias. However, the FTC investigation found that the technology was trained on only about 100,000 individuals, with further training based on AI derived synthetic images. The system failed to rank among the top 100 algorithms tested by the National Institute of Standards and Technology, and the company lacked evidence to support claims about accuracy and unbiased performance.

The proposed order prohibits the company from misrepresenting the accuracy, efficacy, or performance of its FRT. Once finalised, the FTC will have fining powers for breach of up to about \$50,000 per violation.

UK data protection law does not apply to purely domestic use of cameras which only capture images within the boundary of private property. The ICO provides extensive guidance on the use of CCTV including FRT technologies for commercial purposes.

### Links to further information

[Press release](#)

[Complaint](#)

[Proposed order](#)

### SHOOSMITHS SAYS...

Recognising that bias in AI systems can also mean that consumer products don't work.



## AEPD fines phone company €1.3m for security failings

5 December 2024

### Key details

The Spanish Data Protection Authority (the AEPD) has fined a telecoms company €1.3m for a data breach affecting over 1.4m people. The breach, which started on 9 September 2022, was detected seven days later and reported to the AEPD four days after that. It was achieved following a phishing attack on an employee and enabled access to landline phone numbers and linked technical and configuration data including MAC addresses and Wi-Fi details.

The AEPD found that landline numbers were personal data as they could easily be linked to an account owner through a phone directory. The controller argued that they were non-personal data in the hands of the attacker and pseudonymised data in the hands of the company (although the latter would still have triggered compliance requirements, including notification).

The controller was criticised for failing to detect the first attack and only reporting the attack four days after detecting a massive upswing in activity in the compromised account. The company waited until the employee returned from holiday to confirm that activity was not related to them, at which point the incident was deemed malicious and reported to the regulator.

The regulator criticised the controller's failure to adopt a risk-based approach to data security and noted that basic security measures such as two-factor authentication would have prevented the breach. The company was fined for breaches of Art. 5(1)(f) and Art. 32 of the GDPR.

### Links to further information

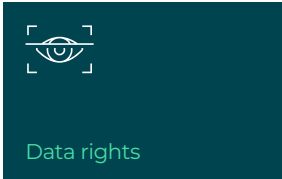
[Resolution](#) (Spanish only)

### SHOOSMITHS SAYS...

A full programme of staff phishing training didn't let the company off the hook.



Jurisdiction: **UK**



## Court of Appeal confirms 2019 fine for data breach

9 December 2024

### Key details

The ICO has welcomed the dismissal of an appeal against a monetary penalty notice issued in December 2019 for careless disposal of sensitive personal information by a controller.

The Court of Appeal found that:

- the burden of proof in an appeal under s.163 of the DPA 2018 lies with the appellant. This means that in (the rare) cases where the court cannot decide which outcome is more probable, it will decide in favour of the regulator
- when it comes to the amount of a penalty, tribunals and courts may take account of the Commissioner's findings in the original notice (in contrast to the underlying breaches, which may require fresh consideration).

The fine had been reduced on appeal from £275,000 to £92,000 after the controller, a pharmaceutical supplier, provided evidence showing that less personal data was involved than originally claimed.

WHAT THEY SAY...

**“provides clarity for future appeals”**

### Links to further information

[ICO statement](#)

[Judgment](#)

Marketing, adtech &  
cookies

## Orange mail attracts €50m fine for inbox advertising and cookies

10 December 2024

### Key details

The French data protection authority, the CNIL, has announced a €50m fine imposed last month on Orange in relation to its email service, Orange Mail, for failing to get proper consent to marketing.

The first breach was a failure to obtain consent to direct marketing emails added to a user's inbox, ("inbox advertising"). Spaces were sold to advertisers by Orange and mimicked other emails in the inbox. The CNIL found that these were different in nature from direct marketing emails sent by third parties. The CNIL applied a CJEU 2021 ruling (StWL Municipal Works, linked) which confirmed that inbox advertising constituted "use of ... electronic mail for the purposes of direct marketing" which required specific consent. The sender was therefore in breach of Art. L. 34-5 of the CPCE (French transposition of Art. 13 of the ePrivacy Directive).

The CNIL dismissed arguments that the marketing was no different to advertising banners on a website, and that it only required additional consent if it involved personal data processing. It also found that Orange was the only party in a position to get consent as it controlled the allocation of spaces.

Second, the CNIL found a failure to delete cookies after withdrawal of user consent, contrary to Art. 82 of the French DPA. The company argued that once user consent was withdrawn, it and partners did not read or act on information transmitted from the cookies, but that it was technically impossible to prevent information being so transmitted. The CNIL rejected these arguments and noted Orange's responsibility for compliance in relation to advertising partners.

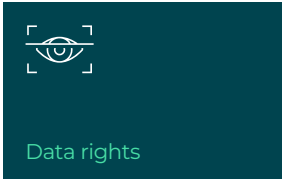
The fine was based on Orange's leading position in the French market (affecting 7.89m accounts), and the seriousness of the breach. The CNIL noted that Orange changed the format of its advertising in November 2023. As well as the fine, the CNIL imposed a daily penalty of €100,000 per day after three months of non-compliance in relation to the breach concerning Art. 82.

### Links to further information

[Press release](#)[StWL Municipal Works](#)[Decision](#)

SHOOSMITHS SAYS...

**Squeezing hard on  
marketing practices.**



## Court of Appeal refuses class MOPI claim

11 December 2024

### Key details

The Court of Appeal has published its judgment on a major class action against Google based on a “misuse of private Information” (MOPI) claim. The court confirmed the strike out and summary judgment made by the High Court in May 2023.

The case, *Prismall v Google*, concerned the use by Google and Deep Mind of patient-identifiable medical data for the development of a tool for the diagnosis of kidney disease, and for further commercial use in training AI systems. An earlier representative claim, *Lloyd v Google*, concerning unlawful tracking under the Data Protection Act 1998, was dismissed by the UK Supreme Court in 2021 on the grounds that damages were not available under the DPA 1998 for mere loss of control of personal data, rather than material damage.

In this case, under the common law tort of MOPI, the Court of Appeal found:

- each claimant would need to show a “reasonable expectation of privacy” which would be undermined by sharing information in the media, as some claimants had done
- some of the claims involved partial medical records with no specific reference to a medical condition
- the least affected claimant in the class might therefore have suffered no loss, so the representative would not have “the same interest” as all the other class members as required by Rule 19.8 of the Civil Procedure Rules.

It appeared to the court that an action on behalf of a reduced class, although possible in theory, was not economic.

### Links to further information

[Judgment](#)

### SHOOSMITHS SAYS...

The judge had no kind words for Google but conceded that UK privacy laws are very difficult for class actions.



Marketing, adtech &  
cookies

## CNIL issues formal notices over cookie banners

12 December 2024

### Key details

The French data protection authority, the CNIL, has issued formal notices to several companies for using misleading cookie consent banners in violation of Art. 82 of the Data Protection Act, which transposes Art. 5(3) of the ePrivacy Directive.

The CNIL's investigation revealed that the banners failed to collect valid user consent by:

- preferencing opt-in options through colour and font
- effectively hiding opt-out options in other text
- presenting options to accept several times but deny options only once.

The CNIL emphasised that refusing cookies must be as simple as accepting them. The companies have one month to update their banners to comply with the law.

SHOOSMITHS SAYS...

**French collection.**

### Links to further information

[Press release](#)

# Enforcement & legal action

Jurisdiction: **SOUTH KOREA**



Marketing, adtech & cookies

## PIPC fines car insurance companies over marketing

12 December 2024

### Key details

The South Korean Personal Information Protection Commission (PIPC) has announced fines of up to KRW 6.198 billion (€4.1m) imposed on four automotive insurance companies for breaching the Personal Information Protection Act (PIPA). The authority's investigation into twelve insurance companies, triggered by over 13,000 customer complaints, found excessive data collection and retention and improper marketing practices, in breach of Arts 21, 31, and 39-3 of the PIPA.

The PIPC found that four of the companies were collecting registration and mobile numbers online using pop-ups which misled customers. The information was used to make over 30m unlawful phone calls and texts selling insurance products. The campaigns had been designed by marketing teams without consulting chief privacy officers (DPOs).

### SHOOSMITHS SAYS...

The takeaway – involve your privacy team in designing marketing campaigns. “CPOs play a role in establishing internal control systems for handling personal information”

### Links to further information

[Press release](#)



## DPC fines Meta €251m for “View As” data breaches

17 December 2024

### Key details

The Irish Data Protection Commissioner has announced fines of €251m imposed on Meta as a result of data breaches arising in 2018 which exposed the Facebook accounts of 3m people in the EU (29m globally) to unauthorised view.

The breaches arose because of design failures in the “View As” function permitting a user to see a third-party view of their Facebook pages, which when combined with other features inadvertently allowed third party users to access private content, including personal data relating to children. The vulnerability was remedied after 14 days.

The DPC imposed fines in respect of:

- design failures (Art. 25(1), €130m)
- processing of more personal data than necessary for specific purposes (Art 25(2), €110m)
- inadequate breach notification information (Art. 33(3), €8m)
- insufficient documentation (Art. 33(5), €3m).

The decision, including several reprimands, will be published in due course. The DPC received no objection to the amount or nature of the fines from the other data protection authorities under the consistency mechanism. It follows a €91m fine of Meta in September for password failures.

### Links to further information

[Press release](#)

SHOOSMITHS SAYS...

**Surprised they can remember that far back.**



## Garante fines estate agency over data kept on paper

17 December 2024

### Key details

The Italian Data Protection Authority, the Garante, has fined a real estate agency €5,000 after a complaint about unwanted calls made to a data subject. The contact details had been obtained from a third-party provider some years earlier, but there was no clear legal basis for its collection. It was apparently being kept on an “unattended paper medium freely accessible to company employees”. It is not clear whether it formed or was intended to form part of a filing system, which is required before processing comes within GDPR scope, or whether this was a single piece of paper.

The DPA concluded that the agency, as franchisee, was an independent data controller. It found that the personal data had been stored indefinitely without appropriate safeguards, violating GDPR provisions related to security and accountability. An access request made by the data subject was also answered late and inadequately, leading to breaches of various provisions of the GDPR including Arts 5, 6, 7, 12, 13 and 24.

SHOOSMITHS SAYS...

[Paper view.](#)

### Links to further information

[Decision](#)



## APD announces €200,000 fine for hospital ransomware

17 December 2024

### Key details

The Belgian data protection authority, the APD, has published details of a Litigation Chamber decision confirming imposition of a €200,000 fine of a hospital following a 2021 ransomware incident. The hospital suffered disruptions to services for three days and the personal data of 300,000 people was exfiltrated, including sensitive health information.

The chamber confirmed the following breaches:

- failure to conduct a DPIA (Art. 35(3))
- lack of information security policy (Arts 5(1)(f) and 32)
- failings in software process and procedure, staff training, logging, audit, and password security (Arts 5(1)(f), 24 and 32).

The hospital queried the need to carry out a DPIA, given that the hacker exploited the staff email account. The chamber's view was that since the email system carried out processing of sensitive data on a large scale, a DPIA was required.

The fine was set at a level to deter future breaches but taking into account the effect of the pandemic, the financial status of the hospital, and the fact that systems were restored relatively quickly after the incident. It was the second attack on the hospital since 2019.

### Links to further information

[Decision](#) (French only)

### WHAT THEY SAY...

**“underlines the need for increased diligence in securing personal data in hospitals”**



# Enforcement & legal action

Jurisdiction: **EU (Germany)**

## Bavarian DPA orders corrective measures on Worldcoin

19 December 2024

SHOOSMITHS SAYS...

**A whole world of pain.**

### Key details

The Bavarian state data protection authority has announced the first results of its investigation into Worldcoin, which include the imposition of various corrective measures. Worldcoin is a cryptocurrency based on one-time only identification using iris scans, a type of biometric data. Scans are carried out using an “Orb” which it says allows holders to “verify their humanness and uniqueness”.

The authority has ordered the company to:

- provide unrestricted rights of erasure within one month
- allow for explicit consent for “certain processing steps in the future”
- delete some existing records.

The company, founded by Sam Altman, and recently rebranded as “World”, has been the subject of enforcement action in various global jurisdictions, and temporarily suspended EU and UK operations on a voluntary basis in mid-2024 following regulator interventions in Spain and Portugal. It will appeal the findings, and it is not clear when the company will resume operations in Europe.

### Links to further information

[DPA announcement](#)

[World press release on orbs](#)



## Garante announces €15m fine for ChatGPT

20 December 2024

### Key details

Following an investigation and temporary ban in 2023, the Italian Data Protection Authority, the Garante, has announced sanctioning measures and a fine of €15m imposed on OpenAI for violations of the GDPR and national privacy laws in relation to the use of ChatGPT in Italy.

The Garante found:

- failure to report a data breach in March 2023 involving the chat history of previous users being publicly available to subsequent users
- processing of personal data without identifying an appropriate legal basis under the GDPR and before a DPIA or LIA had been carried out
- violations of transparency obligations
- failure to provide appropriate age-verification.

It has also ordered the company to undertake a publicity campaign on national media to promote public awareness of how the technology works, the use of training data, and the exercise of data subject rights.

The fine and measures relate to the period before establishment of an OpenAI headquarters in Ireland. The Garante has forwarded its findings to the Irish DPC which is now lead supervisory authority under Art. 56 of the GDPR.

The order includes details of the sources and training methods reported by OpenAI. The order does not include any discussion of the use of special category personal data in model training.

### Links to further information

[Press release](#)

[Order](#)

SHOOSMITHS SAYS...

Like the EDPB, avoiding a lot of tricky questions on model training.



Marketing, adtech & cookies

## California settles four actions for failure to register by data brokers

23 December 2024

### Key details

The California Privacy Protection Agency (CPPA) has announced a total of four settlements with data brokers for alleged failure to register and pay an annual fee as required by Senate Bill 362 (the “Delete Act”).

It follows an “investigative sweep” started in October 2024. Settlements of around \$50,000 have been agreed to avoid possible fines of up to \$200 per day for failure to register.

The agency also reminds in-scope data brokers that those active in 2024 must register and pay the annual fee of \$6,600 by 31 January 2025. From 1 July 2025 they must also collect and report specified information annually about responses to deletion requests from consumers.

The increased enforcement activity is in preparation for mandatory participation in a centralised “deletion mechanism” by all registered data brokers in the state from mid-2026.

SHOOSMITHS SAYS...

Going for broke.

### Links to further information

[Press release](#)

# Enforcement & legal action

Jurisdiction: **US (California)**Accountability &  
governance

## Apple settles Siri “spying” class action

31 December 2024

### Key details

Apple has provisionally agreed to a proposed settlement of a class action, Lopez et al. v. Apple Inc, based on allegations that Apple’s virtual voice assistant, Siri, “spies” on users by listening to conversations intended to be private.

Under the proposed settlement, any US user who attests that they have been the subject of unintended spying between 2014 and 2024 on up to five Siri-enabled devices (iPhone, iPad, Apple Watch, MacBook, iMac, HomePod, iPod touch, or Apple TV) is entitled to claim up to \$20 per device. Apple’s total liability will be up to \$95m.

The allegation is that the technology over-responded to the voice command “hey Siri”, designed to alert the assistant to an upcoming request. The claim is that devices would therefore analyse and record voice conversations intended by the users to be private, and send information to third parties. The claim was based on violations of various state and federal laws including the California Invasion of Privacy Act and the Wiretap Act.

The settlement does not include any admission of liability by Apple. The company denies that data has ever been sold to advertisers. It changed settings following issuance of the claim in 2019 so that users had to opt into allowing recordings to be sent for third party analysis to improve the service. A similar class action against Google is ongoing.

SHOOSMITHS SAYS...

So are they listening in? We still don’t know.



## Industry & sector news



## TikTok announces controls on beauty filters for under 18s

26 November 2024

### Key details

TikTok has announced that it is rolling out changes to its filters. It will restrict the use of certain visual effects to under 18s, give users more information about them, and update guidance for content creators on unintended consequences of certain appearance filters.

It has also announced:

- over 175m monthly users in Europe
- €2bn investment globally to improve safety and security, including in-app mental health support
- removal of 6m accounts monthly that fail to meet the 13+ age requirement
- the launch of Project Clover to migrate European user data to dedicated servers in Norway, Ireland, and the US.

### SHOOSMITHS SAYS...

Some rapid self-regulation in the face of rising calls to ban social media for children.

### Links to further information

[Press release](#)



## VW Group suffers vehicle geolocation data breach

26 November 2024

### Key details

A Volkswagen Group subsidiary has confirmed a data breach affecting around 800,000 electric vehicles in various European countries. The breach was reportedly caused by misconfiguration of an Amazon cloud database by a subsidiary company, and led to vehicle data including geolocation data being exposed between September and November 2024. Affected vehicles were mostly in Germany, but also included models sold in Norway, Sweden, France, the UK, Belgium, the Netherlands and Denmark.

The leak was exposed by an “ethical hacking” group which was able to link data to individuals by combining various data sets. The leak was then reported in a German national newspaper, which managed to further expose information relating to high-profile politicians. The company remedied the breach on the day it was reported to them and there is no indication that information has been accessed by any malicious third party.

SHOOSMITHS SAYS...

**More problems with  
connected products.**

Jurisdiction: **US**



## Doughnut franchise files SEC report after cyber attack

29 November 2024

SHOOSMITHS SAYS...

**Could be sticky.**

### Key details

US food supplier Krispy Kreme has filed a form 8-K to the Securities and Exchange Commission following a cybersecurity attack which impacted its ability to process online orders in the US.

It detected the attack on 29 November, and has not yet revealed whether ransomware was involved, any loss of data including personal data, or who was responsible. The company anticipates short-term financial losses due to reduced digital sales and the cost of cybersecurity experts but does not expect long-term effects. The company's share price fell 2% following the public disclosure of the breach. It says that investigation and remediation efforts are ongoing.

### Links to further information

[SEC filing](#)





## TikTok asks for emergency injunction to stop ban

9 December 2024

### Key details

TikTok has requested an emergency injunction to delay the effect of the de facto ban of the site in the US, due to take effect on 19 January 2025. It follows enactment of the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACAA) in April 2024, legislation highly targeted at TikTok which would force the owners to sell to a US owned company.

On 6 December, the DC Court of Appeals refused to overturn the ban on the grounds of unconstitutionality. TikTok is asking for a delay and Supreme Court review of the constitutional position and says it will suffer irreparable harm if the ban is not lifted.

The President elect has indicated that he would overturn the PAFACAA, but it is not clear if he would support a Supreme Court veto on media controls on the grounds of national security.

SHOOSMITHS SAYS...

**TikTok making every second count.**

### Links to further information

[Emergency motion](#)

Marketing, adtech &  
cookies

## ICO responds to Google plans on fingerprinting

19 December 2024

### Key details

The UK Information Commissioner's Office has issued a statement criticising Google's plans to allow advertisers to use device fingerprinting techniques to replace third party cookies from 16 February 2025.

Fingerprinting involves identifying and tracking individual devices across various platforms. The ICO is concerned that the technology is hard for browsers to block, difficult to reverse and challenging to bring into compliance with data protection law. The ICO points out that in 2019 Google said, "we think [fingerprinting] subverts user choice and is wrong".

Google policy currently prohibits most use of fingerprinting with Google platform products. The company says that the change is in response to greater use of connected products such as smart TVs and advances in privacy enhancing technologies.

The statement coincides with the ICO's new draft guidance on tracking technologies, which notes that fingerprinting techniques involving attribution of an "anonymous" identifier will still come under ePrivacy laws requiring consent, even if email addresses or other personal data cannot be inferred from it.

### WHAT THEY SAY...

**"fingerprinting is not a fair means of tracking users online"**

### Links to further information

[ICO statement](#)[Google announcement](#)

Jurisdiction: **US**



## US Treasury confirms hack by Chinese state actors

30 December 2024

### Key details

The US Treasury has confirmed a “major cybersecurity incident” in early December attributed to Chinese “government hackers”. The attack was apparently enabled through a key used by a tech support company to provide remote access.

It follows a number of attacks on major US phone and digital companies over 2024 attributed to Chinese interference in US elections.

An update from the US Cybersecurity and Infrastructure Security Agency (CISA) confirmed that no other US government departments were affected. The Treasury has made no official statement, although it subsequently announced sanctions against a Chinese tech company for involvement with Flax Typhoon, a major cyber group behind a number of attacks on US critical infrastructure.

SHOOSMITHS SAYS...

**US/China relations looking increasingly stormy.**

### Links to further information

[CISA announcement](#)

[Treasury announcement](#)



**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: January 2025

©Shoosmiths LLP 2025

**SHOOSMITHS**

[www.shoosmiths.com](http://www.shoosmiths.com)

**FOR  
WHAT  
MATTERS**