

SHOOSMITHS

PRIVACY & DATA | GLOBAL EDITION

Data protection

June 2023 roundup

www.shoosmiths.com

FOR
WHAT
MATTERS



Legislation



Guidance & Consultations



Enforcement & Legal Action

THE BIG STORY



UK and US announce
“data bridge” as part of
Atlantic Declaration on
economic cooperation
8 JUNE 2023



Industry & Sector News



INDEX

Index


















	JURISDICTION
Legislation	
08 ↔ China's SCCs come into force and guidance is issued.....	CHINA
09 ⚙️ ICO publishes opinion on Data Protection and Digital Information (No. 2) Bill	UK
10 ⚙️ Comprehensive privacy laws now in ten US states	US (Various)
11 ↔ UK and US announce “data bridge” as part of Atlantic Declaration on economic cooperation	US/UK
12 🤖 European Parliament publishes EDPB/S draft amendments to the proposed AI Act.....	EU
13 ⚙️ Data Protection and Digital Information (No.2) Bill: Research briefing and new version published.....	UK
14 ⚙️ Data Privacy and Security Act signed by governor	US (Texas)
15 🏛️ Senators introduce bill protecting US data from foreign surveillance.....	US
16 ⚙️ AI and data sharing announced in 2023 workplan.....	CHINA
17 🏛️ Parliament agrees to European Production Orders and European Preservation Orders.....	EU
18 ⚙️ Nigerian Data Protection Bill becomes law.....	NIGERIA
19 ⚙️ Oregon passes Consumer Data Privacy Bill.....	US (Oregon)
20 🛡️ Banks testing new powers to share financial information under Economic Crime and Corporate Transparency Bill.	UK
21 ⚙️ Retained EU Law (Revocation and Reform) Bill finalised.....	UK

Key:









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

Index

Guidance & consultations
















23	 ICO updates UK Children’s Code guidance on edtech	UK
24	 DHSC consults on creating Secure Data Environments to access NHS data for research purposes	UK
25	 Advocate General considers medical exemptions for special category data in Art. 9(2)(h)	EU
26	 Ofcom updates guidance under NIS Regulations	UK
27	 Digital Markets Act: European Commission consultation on compliance report template	EU
28	 EDPB adopts final version of Guidelines on the calculation of administrative fines	EU
29	 EDPB adopts final version of Guidelines on the application of Article 65(1)(a)	EU
30	 ICO releases Children’s Code evaluation report	UK
31	 ICO issues new PETS guidance	UK
32	 ICO publishes research on synthetic data	UK
33	 ICO warns of tougher enforcement for businesses using generative AI	UK
34	 CDEI publishes reports on demographic information in AI systems, and assurance techniques	UK
35	 ENISA publishes report on cybersecurity practices in the supply chain	EU
36	 ODI releases report on use of commercially available information (CAI) by US intelligence agencies	US
37	 Digital Services Act: European Commission consults on online database of content moderation decisions	EU
38	 EDPB adopts Recommendations 1/2022 on application and approval process for EU controller BCRs	EU
39	 EDPB adopts template form to facilitate cross-border complaints	EU

Key:

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

Index

Enforcement & legal action











41	 FTC and DOJ order \$30.8m in collective fines against Alexa and Ring.....	US
42	 Berlin DPA fines bank €300,000 for lack of transparency with automated decision-making.....	EU (Berlin)
43	 ICO reprimands Thames Valley Police for releasing witness details to suspected criminals.....	UK
44	 ICO fines two firms for making unlawful marketing calls.....	UK
45	 Swedish DPA announces Spotify fine of €4.98m for transparency failures.....	EU (Sweden)
46	 Garante fines TIM SpA €7.6m for unlawful telemarketing activities.....	EU (Italy)
47	 CJEU publishes opinion on liability for Europol data breach.....	EU
48	 Commission sends Statement of Objection to Google alleging abusive practices in adtech.....	EU
49	 CNIL fines KG COM €150,000 for unlawful processing of personal data.....	EU (France)
50	 Director guilty of s. 55 DPA offences subject to confiscation order under Proceeds of Crime Act.....	UK
51	 CNIL confirms reduced €40m fine of Criteo for GDPR failings in personalised advertising.....	EU (France)
52	 CJEU holds that data subjects have the right to access date and reason for the consultation of personal data..	EU
53	 AG issues opinion on data subject access rights under Law Enforcement Directive.....	EU
54	 Garante announces €40k fine of VW Leasing GmbH for inadequate response to DSAR.....	EU (Italy)
55	 NOYB gets permission for judicial review of Data Protection Commission (DPC).....	EU (Ireland)

Key:









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

Index

Industry & sector news

- 57  Microsoft reveals expected \$425m fine for LinkedIn ad practices..... **EU (Ireland)**
- 58  Toyota announces long-term data leak in its Connected services..... **JAPAN**
- 59  NHS Trusts accused of sharing patient details with Facebook without consent..... **UK**
- 60  Kuwait to collect biometric data of everyone in the country..... **KUWAIT**
- 61  Zoom to offer data localisation for paying customers in EEA..... **EU**
- 62  Ticketmaster to bring website into compliance with DAA Self-Regulatory Principles..... **US**
- 63  OAIC announces that it has been victim of cyber attack..... **AUSTRALIA**
- 64  Senators launch investigation into use of health data by Amazon Clinic..... **US**
- 65  Irish Council for Civil Liberties urges Irish Parliament to prevent ‘criminalising’ DPC reporting **EU (Ireland)**
- 66  Datatilsynet authorizes further use of facial recognition systems by football club..... **EU (Denmark)**

Key:

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



Legislation



Transfers

China's SCCs come into force and guidance is issued

1 June 2023

Key details

The Standard Contract Measures for the transfer of personal data from China have come into effect following their adoption on 23 February 2023. The Cyberspace Administration of China (CAC) has also issued guidance on their use.

Processors using standard contracts to transfer personal information outside China must meet all these conditions:

- Not be an operator of critical information infrastructure
- Handle the personal information of fewer than one million people in total
- Have made cumulative outbound transfers of personal information of fewer than 100,000 people since January 1 of the previous year
- Have made cumulative outbound transfers of sensitive personal information of fewer than 10,000 people since January 1 of the previous year.

The measures require processors to conduct a Personal Information Protection Impact Assessment ("PIPIA") before transfer and processors must file this plus contract information with the CAC within 10 working days from the effective date of the contract (filing does not affect the validity of the SCCs).

Links to further information

[Original announcement](#)

[EC analysis](#)

SHOOSMITHS SAYS...

CAC seems to have the same dilemma as the EDPB:

“it is still unclear whether offshore PI handlers subject to the extraterritorial effect of the PIPL are eligible for the China SCC approach, though the CAC currently considers offshore collection of PI to constitute a cross border data transfer”



ICO publishes opinion on Data Protection and Digital Information (No. 2) Bill

31 May 2023

Key details

The ICO response suggests where changes to the bill are needed to improve clarity or to better reflect policy intent.

ICO recommends amendments to:

- Definition of personal data in Clause 1 and the test for third party identification, which as drafted carries “a theoretical privacy risk”
- Conditions for consent to processing for the purposes of scientific research in Clause 3
- The explanatory note about controllers’ need to satisfy a legal basis for further processing under Art. 8A
- Vexatious or excessive requests by data subjects
- Information provision obligations where organizations have collected data directly from data subjects
- Automated decision-making in Clause 11
- ‘High risk processing’ regarding record-keeping requirements in Clause 15
- Distinguishing between the tests for adequacy, and appropriate safeguards in Clause 21
- Direct marketing for the purposes of democratic engagement, particularly regarding a data subject’s right to object to direct marketing.

WHAT THEY SAY...

“I welcome the DPDI bill as a positive package of reforms that allow us to continue to operate as a trusted, fair and independent regulator”

Links to further information

[ICO response](#)

[Bill](#)

Jurisdiction: **US (Various)**



Comprehensive privacy laws now in ten US states

June 2023

Key details

From next month there will be comprehensive state privacy legislation in force in California, Colorado, Connecticut and Virginia, and enacted in Indiana, Iowa, Montana, Tennessee, Texas and Utah.

WHAT THEY SAY...

“State-level momentum for comprehensive privacy bills is at an all-time high”



Transfers

UK and US announce “data bridge” as part of Atlantic Declaration on economic cooperation

8 June 2023

Key details

The Atlantic Declaration looks to establish a new approach in US/UK relations in various areas including nuclear partnership, energy security, critical minerals supply, export controls and future technologies such as AI and Privacy Enhancing Technologies.

Announcements include a commitment in principle to establish the “UK Extension to the Data Privacy Framework” for secure personal data flows. Key points:

- US companies approved to join the framework will be able to receive UK personal data under the new bespoke, opt-in certification scheme
- The scheme will be enforced in the US by the Federal Trade Commission and Department of Transportation, and administered by the Department of Commerce
- The UK government will formally consult the ICO under DPA 2018. The Secretary of State must take into account, but is not bound by, the ICO’s views (see MOU, below)

- The government estimates £92.4m in direct savings per year in reduced “red tape” for 55,000 businesses.

The scheme is an extension to the European Commission scheme forming part of the draft adequacy decision in the US/EU Data Protection Framework. It is unlikely to be finalised until that decision has been approved by the Commission.

Other data-related things of note:

- The declaration underlines support for the Global Cross-Border Privacy Rules (CBPR) Forum and the OECD’s Declaration on Government Access to Personal Data Held by Private Sector Entities
- The US supports the UK’s plan to launch the first Global Summit on AI Safety this year (see below).

Links to further information

[UK press release](#)
[UK MOU](#)
[UK statement](#)
[US statement](#)

SHOOSMITHS SAYS...

Easy to see why the UK is trying so hard to establish frictionless data flow to the US:

“In 2021, about 30% of the UK’s total data enabled services exports [were] to the US”
– a cool £79bn.



European Parliament publishes EDPB/S draft amendments to the proposed AI Act

7 June 2023

Key details

The European Data Protection Board and Supervisor amendments are part of the report stage to agree the European Parliament's draft before it goes into final negotiation with the Commission and Council. The Parliament's final position will be debated this week with a vote on Wednesday.

The amendments:

- Propose a new recital explicitly basing the Act on current EU data protection law (GDPR, Law Enforcement Directive, EUGDPR, PECRs)
- Recite that the Act does not seek to affect data protection and privacy law, powers and rights
- Clarify the meaning of “machine learning”
- Create new definitions of “biometrics-based” data, biometric identification and biometric categorisation
- Distinguish remote biometric identification
- Propose new exceptions for open-source software
- Classify some AI systems using special category data as high risk
- Narrow use of AI systems for the purposes of law enforcement
- Define some new high-risk systems, such as those monitoring behaviour to determine a person's education level, and systems able to influence the outcome of elections or referenda
- Provide that deployers of AI systems should be registered and provide certain contact information.

Links to further information

[Draft amendments](#)

SHOOSMITHS SAYS...

Grinding out agreement on AI.

“As a pre-requisite, artificial intelligence should be a human-centric technology. It should not substitute human autonomy or assume the loss of individual freedom and should primarily serve the needs of the society and the common good”



Data Protection and Digital Information (No.2) Bill: Research briefing and new version published

9 June 2023

Key details

The government has completed the Public Committee stage of the Bill, which makes substantial amendments to UK GDPR, the Data Protection Act 2018, and PECRs.

It has also published a new research briefing outlining the limited amendments made. A Keeling Schedule for the updated version is not yet available.

SHOOSMITHS SAYS...

The House of Commons has not accepted substantive amendments to the Bill. Let's hope the Lords have a sharp pencil at the ready.

Links to further information

[Latest version](#)

[Commons briefing](#)



Data Privacy and Security Act signed by governor

18 June 2023

Key details

The law applies to persons who:

- Conduct business in Texas or produce a product or service for Texas residents
- Process or engage in the sale of personal data
- Are not a small business (max 1,500 employees and \$41.5m revenue)

Does not apply to non-profits, educational establishments, or businesses already subject to HIPAA or GLBA.

Drafted along GDPR lines. Introduces data protection assessments and data subject rights. Only enforceable through the Attorney General – no private right of action. Fines up to \$7,500 per violation.

The bill enters into effect on 1 July 2024, with some opt-out provisions in effect 1 January 2025.

SHOOSMITHS SAYS...

Of limited scope: 99.7% of businesses in the US qualify as “small”.

“All hat an’ no cattle”, as they say in Texas

Links to further information

[Bill](#)



Senators introduce bill protecting US data from foreign surveillance

14 June 2023

Key details

The bipartisan bill, the ‘Protecting Americans’ Data from Foreign Surveillance Act’ 2023 is sponsored by ten senators and representatives. It applies criminal and civil penalties to prevent the transfer of data relating to US citizens to countries if it is likely to be exploited by an adversary or may harm national security.

The bill directs the US Department of Commerce to identify high risk data and to categorise countries into three tiers. Export to a top tier country would be banned, and to a middle-ranked country only permitted under licence.

SHOOSMITHS SAYS...

China crisis.

“We don’t export advanced technologies or weapon systems to our adversaries for good reason. We shouldn’t allow data brokers to export Americans’ personal data either”

Coincidence of the week: the thresholds for exemption closely mirror those found in the recently adopted China SCCs.

Links to further information

[Bill](#)

[Press release](#)



AI and data sharing announced in 2023 workplan

6 June 2023

Key details

The State Council of the People's Republic of China has announced its 2023 Legislative Work Plan. The work plan includes development of a draft Artificial Intelligence Law, protection of minors online, developing data sharing regulations on government affairs, and network data security management regulations.

SHOOSMITHS SAYS...

Their vision for 2023: to 'actively participate in the reform and construction of the global governance system'.

Links to further information

[Notice](#)



Parliament agrees to European Production Orders and European Preservation Orders

13 June 2023

Key details

The European Parliament has voted in favour of a framework for the exchange of electronic evidence by criminal law enforcement authorities in the EU. Includes a Directive on appointment of legal representatives to manage orders (2018/0107), and a Regulation on evidence orders (2018/225).

Once in effect, the law will require relevant service providers based or operating in the EU to

- Appoint a legal representative in at least one EU Member State as a contact point in charge of receiving and enforcing orders
- Provide relevant evidence direct to authorities in other member states or preserve it for up to 60 days.

Orders can be served on providers of electronic communication services, social networks, online marketplaces, other hosting service providers and providers of internet infrastructure.

It will replace the current patchwork of bilateral mutual assistance agreements. The agreed text needs to be formally adopted by the Council. The directive will come into effect 6 months after publication. Legal representative requirements must be enforceable under member state law 30 months after that.

Links to further information

[Texts](#)

[Press release](#)

WHAT THEY SAY...

“offering a common, EU-wide solution for addressing legal orders to service providers by way of a legal representative”



Nigerian Data Protection Bill becomes law

14 June 2023

Key details

The law establishes the Nigerian Data Protection Commission and provides a legal framework for processing personal data, data controller obligations and the appointment of a DPO. It also imposes restrictions on international transfers. The legislation is not yet available.

SHOOSMITHS SAYS...

Africa's largest economy.

“a clear signal that Nigeria is committed to safeguarding fundamental rights and freedoms”

Links to further information

[PLAC Summary](#)



Oregon passes Consumer Data Privacy Bill

22 June 2023

Key details

Oregon has become the eleventh state to pass privacy legislation.

Applies to businesses in the state or providing products or services to residents, which:

- Control or process personal data on at least 100,000 residents
- Derive 25% of revenue from selling the data of more than 25,000 residents.

(Same consumer threshold standard as several other states.)

It has fewer exemptions than many other state laws and a wider definition of personal data, it contains a unique biometric definition, a right to be given a list of specific (not generic) third party data recipients, and does not exclude pseudonymous data from protections.

Enforcement is through the Attorney General, there is no private right of action. Maximum penalty of \$7,500 per violation.

Takes effect 1 July 2024, or 1 January 2025 for non-profit organisations.

WHAT THEY SAY...

“one of the strongest passed to date”

Links to further information

[Bill](#)



Banks testing new powers to share financial information under Economic Crime and Corporate Transparency Bill

22 June 2023

Key details

The bill addresses some of the current concerns about operation of the company registration system, and aims to deter economic crime through increased transparency. It includes new provisions designed to facilitate information sharing about customers with government authorities and other banks.

Reuters has reported that six banks are working with the National Crime Agency to test the data sharing proposals, and eight are working on setting up a new database of suspected economic crime. No official announcements have been made.

The bill is at final report stage and expected to become law in Autumn 2023. Relevant provisions are at cl. 182 onwards.

SHOOSMITHS SAYS...

First steps towards more open data sharing in the financial sector.

Links to further information

[Bill](#)



Retained EU Law (Revocation and Reform) Bill finalised

27 June 2023

Key details

The REUL Bill has passed through both houses and is set to get Royal Assent. We do not yet have a final version including the agreed amendments.

As drafted, the bill will have a more limited impact on data protection law than as originally conceived. However, it does include changes to the Investigatory Powers Act and may affect the status of past European Court of Justice decisions in UK courts such as Schrems 2.

SHOOSMITHS SAYS...

The REUL of law.

Links to further information

[Bill](#)

Guidance & consultations





Sensitive data &
vulnerable individuals

ICO updates UK Children's Code guidance on edtech

31 May 2023

Key details

The ICO has updated its guidance on education technologies to clarify when they may be in the scope of the Children's Code. The code applies to relevant "information society services" (as defined in the DPA 2018) that are likely to be accessed by children in a direct-to-consumer basis, such as online or in an app store.

Schools as public authorities are not in scope of the code but edtech providers may be, if they process personal information "beyond the instructions of a school" and determine why and how personal information is processed, thereby exercising control over the means and purposes of processing.

Guidance includes reminders that:

- Data protection law will apply regardless of whether the code does
- The 'public task' lawful basis under Art. 6(1)(e) UK GDPR is unlikely to be an appropriate lawful basis for edtech providers.

Links to further information

[Guidance](#)

[Announcement](#)

SHOOSMITHS SAYS...

Lessons in safety for a vast and expanding sector.

Latest edtech trends:

- Immersive learning
- Accessibility tools
- Remote learning
- AI enabled learning
- Gamification
- The G-suite (Google everywhere)
- Massive global investment

Jurisdiction: **UK**

DHSC consults on creating Secure Data Environments to access NHS data for research purposes

26 May 2023

Key details

The Department of Health and Social Care (DHSC) has begun a public consultation on the creation of Secure Data Environments (SDEs) for the purpose of accessing NHS data for research purposes. The aim is that SDEs will become the default route for accessing NHS data, for research and external uses.

Builds on 12 guidelines published in September 2022. The policy update confirms:

- NHS organisations will maintain oversight of data held in SDEs
- SDEs will need to adhere to high standards of data integrity, security and transparency
- An accreditation model for SDEs will be developed for this purpose
- From a future date, commercial and/or academic controlled SDEs will not continue to host NHS data or make it available for research.

Closes 23 June 2023.

Links to further information

[Consultation](#)

[Draft policy update](#)

[Guidelines](#)

SHOOSMITHS SAYS...

Learning the painful lessons of over-ambitious deployment of public health data:

“we will move only as fast as the public and stakeholders accept”

Jurisdiction: **EU**

Advocate General considers medical exemptions for special category data in Art. 9(2)(h)

25 May 2023

Key details

The opinion comes in advance of a preliminary ruling on referral from the German Federal Labour Court. The case concerns whether the medical service of a health insurance fund should be prohibited from preparing a medical report for an insurer on its own employee. The AG's view is that the exception in Art. 9(2)(h) EU GDPR permitting processing of special categories of data for certain medical purposes is available to the medical service even though it happens also to be the claimant's employer.

Findings of more general importance:

- If using this exception, you also need a lawful basis for processing under Art. 6 (so you can't rely on Art. 9(3) alone)
- The degree of fault on the part of the controller or processor does not affect liability or quantum of damages in Art. 82(1)
- The involvement of the data subject in the event giving rise to compensation may exempt the controller or processor from liability under Art. 82(3).

ZQ v MDK (Case C-667/21) EU:C:2023:433

Links to further information

[AG's opinion](#)

SHOOSMITHS SAYS...

GDPR decision-making in
excellent health.

Jurisdiction: **UK**

Ofcom updates guidance under NIS Regulations

31 May 2023

Key details

Ofcom has issued updated guidance both for communications providers, and for operators of essential services (OESs), under the Network and Information Security Regulations (NIS).

The Guidance for communications providers is issued under s. 105Y Communications Act 2003. Section 7 details Ofcom's information sharing duties and powers. It sets out the situations in which Ofcom expects to pass information to third parties (NCSC, or another "relevant body") without the consent of the provider in question.

The other guidance is for OESs, which are likely to be domain name registries and service providers, and IXP (internet exchange point) operators. It includes updates on designation, compliance requirements, investigations, and enforcement.

Links to further information

[S. 105 guidance](#)[OES guidance](#)

WHAT THEY SAY...

NIS to see you.**What happens to all the information which providers are reporting under NIS?****Answer: Ofcom “may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions. Such a disclosure does not breach any obligation of confidence owed by Ofcom or any other restriction on the disclosure of information (however imposed)”**

Jurisdiction: **EU**



Digital Markets Act: European Commission consultation on compliance report template

6 June 2023

Key details

The Commission is consulting on the template for the annual report that designated gatekeepers will have to submit under Art. 11 of the Digital Markets Act ('DMA').

In particular, the Commission wants feedback on the following:

- Precise indicators that the Commission could use to assess whether measures implemented by gatekeepers are effective
- Content and presentation of the non-confidential summary of the compliance report that the gatekeepers must provide under Art. 11(2).

Comments must be submitted by 5 July 2023.

SHOOSMITHS SAYS...

Tightening the DMA thumbscrews.

“Gatekeepers will be required to provide the Commission with their first compliance report within six months of their designation as gatekeepers”

Links to further information

[Consultation](#)



EDPB adopts final version of Guidelines on the calculation of administrative fines

7 June 2023

Key details

The European Data Protection Board has adopted the final version of Guidelines 04/2022 on the calculation of administrative fines under the EU General Data Protection Regulation ((EU) 2016/679).

The guidelines take a five-step approach:

1. Identify the processing operations involved, check no double counting under Art. 83(3)
2. Classify the breach, its seriousness and the turnover of the undertaking
3. Evaluate aggravating and mitigating circumstances
4. Identify relevant legal maximums for the different processing operations
5. Check that the final amount meets the requirements of effectiveness, dissuasiveness and proportionality.

The Guidance contains new summary tables and examples, following public consultation.

WHAT THEY SAY...

The fine print.

Includes guidance on how groups of undertakings are dealt with – see 6.2.1. and 6.2.2

Links to further information

[Guidelines](#)

[Press release](#)

Jurisdiction: **EU**



EDPB adopts final version of Guidelines on the application of Article 65(1)(a)

7 June 2023

Key details

The EDPB has adopted the final version of Guidelines 03/2021 on Art. 65(1)(a) GDPR, which allows the EDPB to adopt binding decisions where data protection authorities disagree on the interpretation of GDPR.

The guidelines have been updated to include an executive summary and to introduce clarification and reflect recent developments from other new guidelines.

SHOOSMITHS SAYS...

One of the guidelines may be of particular interest to the DPC and Meta:

“An action for annulment before the Court of Justice does not suspend the effects of the decision of the EDPB”

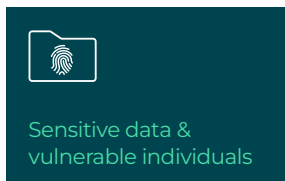
(para 123)

Links to further information

[Guidelines](#)

[Press release](#)

Jurisdiction: **UK**



ICO releases Children’s Code evaluation report

14 June 2023

Key details

The ICO has released its review and assessment of the Children’s Code following the public consultation which ran between March and May 2023.

Their key messages are:

- The Code has driven global law-making
- ISS providers have made positive changes but there is still more to do
- Parents and schools are pivotal
- The ICO is under fire for not enforcing hard enough
- Only a third of businesses expect to incur Code compliance costs
- Two thirds expect to be Code compliant by end 2023
- Two in five children lie about their age, particularly vulnerable groups
- Half of parents help them do this.

SHOOSMITHS SAYS...

ICO deserves a pat on the back, but senses mission creep.

“Delays to the [Online Safety] Bill have meant the code has been increasingly expected to provide regulatory certainty in areas where it wasn’t specifically designed to do so”

Links to further information

[Evaluation report](#)

[Press release](#)

[Key message report](#)

Jurisdiction: **UK**



ICO issues new PETs guidance

19 June 2023

Key details

The new guidance on privacy enhancing technologies, or PETs, is aimed at Data Protection Officers and others using large personal data sets in finance, healthcare, research, and central and local government.

The central part of the guidance is an analysis and explanation of eight commonly used PETs with links to industry standards and the underlying data protection principles. There is also high-level guidance for DPOs on understanding and assessing the use of PETs for processing in their organisation.

SHOOSMITHS SAYS...

Conclusion of another PET project.

The Commissioner is in Japan this week talking with the G7 about PETs and global transfer rules.

Links to further information

[Guidance](#)

[Press release](#)

[G7 Data Protection Roundtable](#)

Jurisdiction: **UK**



ICO publishes research on synthetic data

13 June 2023

Key details

The research by the ICO, Financial Conduct Authority and Alan Turing Institute explores generating anonymous synthetic data in the financial services sector.

‘Synthetic data’ is fake data generated by algorithm, used to train AI where datasets are not accessible or too risky to use. But results always need testing against real data to check for bias or inaccuracy, which either involves using real data again, or complex maths which is not transparent.

The conclusion is that validation is still a critical barrier to adoption, but common standards and guidance would be a good first step.

SHOOSMITHS SAYS...

Make it so you can fake it.

“To drive adoption, the industry could shift to a risk-based model for privacy validation that accepts some level of inherent risk in generating and sharing synthetic data”

Links to further information

[Research paper](#)

[Announcement](#)

Jurisdiction: **UK**



ICO warns of tougher enforcement for businesses using generative AI

15 June 2023

Key details

The ICO is calling for businesses to address privacy risks prior to the use of generative AI, and warns that it will conduct tougher checks on compliance with data protection laws.

Follows ICO guidance in April about how to address generative AI risks.

SHOOSMITHS SAYS...

A warning shot before the AI stampede.

“could become a £1 trillion market within a decade”

Links to further information

[Press release](#)

[April guidance](#)



CDEI publishes reports on demographic information in AI systems, and assurance techniques

14 June 2023

Key details

The Centre for Data Ethics and Innovation, part of DSIT, has published a report on the challenges of using demographic information for bias monitoring in various data driven systems, including AI.

The central problem (which overlaps with the synthetic data issues on page 33) is that access to good demographic data is important for maintaining fairness, but difficult because of the sensitive nature of the data. The two approaches suggested are 'data intermediaries' (an independent data guardian) and 'proxies' (a type of verification which still involves personal data, although at a reduced level).

SHOOSMITHS SAYS...

Great ideas in need of some regulatory architecture.

...Unlike in the EU, where the Data Governance Act gives us impressive architecture (which may remain empty for some time)

Links to further information

[Report](#)

Jurisdiction: **EU**



ENISA publishes report on cybersecurity practices in the supply chain

13 June 2023

Key details

The ENISA (EU Cybersecurity Agency) report is an overview of the current supply chain cybersecurity practices followed by ‘essential and important’ entities in the EU, as defined in the updated Network and Information Systems Directive (NIS 2).

Arts 21(2)(d) and 21(3) of NIS 2 impose specific duties relating to supply chain security on those entities.

The report sets out a five-step approach to the supply chain challenge with recommended security practices for each step. These practices are appropriate for implementation of the NIS2 requirements.

SHOOSMITHS SAYS...

The threat from below.

“58% of surveyed CEOs feel their partners and suppliers are less resilient than their own organisation”

Links to further information

[Press release and report](#)

Jurisdiction: **US**



ODI releases report on use of commercially available information (CAI) by US intelligence agencies

5 June 2023

Key details

The Office of the Director of National Intelligence published a declassified report into commercially available information which is bought and used for intelligence purposes in the US. CAI has traditionally been treated as publicly available, and therefore little regulated in the US, but the report recognises that the availability of commercial smartphone data means that intelligence services can bypass traditional controls on information gathering.

The report recommends:

- Establishing a list of what is used
- Proper policies and procedures
- ‘More refined policies to govern its acquisition and treatment’.

SHOOSMITHS SAYS...

The intelligence community sensing it has too much of a good thing.

“Unfettered access to CAI increases its power in ways that may exceed our constitutional traditions or other societal expectations”

Links to further information

[Report](#)



Digital Services Act: European Commission consults on online database of content moderation decisions

21 June 2023

Key details

The European Commission has launched a survey on the publicly accessible database it is required to establish under Art. 24(5) of the DSA.

The 'DSA Transparency Database' will store decisions and statements from 'online platforms' concerning their reasons for removal of information and other content moderation decisions. These statements are made under Art. 17(1), which requires providers of hosting services to supply a statement of reasons to affected service recipients if restrictions are imposed.

The survey asks:

- What methods should be used for submitting statements
- How quickly statements should be submitted (options range from immediately to less than once a week)
- Whether the database should allow tools to facilitate research and public scrutiny
- What safeguards should be put in place
- Whether changes should be made to the proposed content and structure of the database.

The survey closes on 17 July 2023.

Links to further information

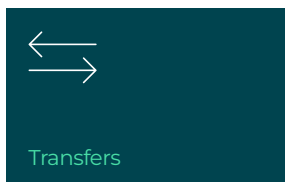
[Survey](#)

[Digital Services Act](#)

SHOOSMITHS SAYS...

Content moderation gets down to brass tacks.

“All online intermediaries, except micro and small enterprises, will have to comply with wide-ranging new transparency obligations to increase accountability and oversight”



EDPB adopts Recommendations 1/2022 on application and approval process for EU controller BCRs

21 June 2023

Key details

Once published by the European Data Protection Board, the final version of 'Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules (BCR-C)' will provide:

- An updated application form for approval
- Clarification the content of BCR-2
- Updated guidance on the requirements, taking account of Schrems 2.

Rules will be in effect from the publication date (to be announced). BCR-C holders will need to bring their BCRs in line with the recommendations, either during the application process or as part of their 2024 annual update.

BCR-P for processors are in development.

SHOOSMITHS SAYS...

The new BCRs are “subject to the necessary legal, linguistic and formatting checks and will be made available on the EDPB website once these have been completed”

Links to further information

[Press release](#)



EDPB adopts template form to facilitate cross-border complaints

20 June 2023

Key details

The voluntary template issued by the European Data Protection Board is a standard form which data subjects can fill in to register a complaint to a member state data protection authority (DPA) about possible infringements in connection with the processing of their personal data under Art. 77 EU GDPR.

It enables the complainant to give consent to transfer of information to other DPAs and the data controller, to make investigations easier.

It can be used by individuals, legal representatives or other entities. There is also a new template EDPB acknowledgement including information about next steps and rights of redress.

WHAT THEY SAY...

“will help DPAs save time and resolve cross-border cases more efficiently”

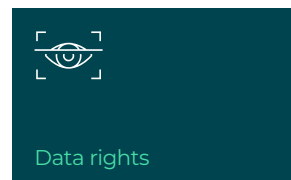
Links to further information

[Templates](#)

[EDPB press release](#)



Enforcement & legal action

Jurisdiction: **US**

FTC and DOJ order \$30.8m in collective fines against Alexa and Ring

31 May 2023

Key details

The US Federal Trade Commission (FTC) and the Department of Justice (DoJ) have announced a \$25m fine and various corrective measures against Amazon's Alexa. They allege Children's Online Privacy Protection Act violations stemming from data deletion and retention practices for children's voice and geolocation data.

In addition to the data deletion requirement in the proposed Alexa order, it:

- Stops Amazon using data which is subject to consumer deletion requests for the creation or improvement of any data product
- Requires deletion of children's inactive Alexa accounts
- Requires notification of the FTC-DoJ action against the company
- Requires notification of retention and deletion practices
- Mandates clear privacy policies
- Orders a privacy program for geolocation information.

The FTC has also announced a \$5.8 million fine and corrective measures against Amazon's Ring, pending federal court approval. The Commission alleges that Ring customers did not consent to video recordings being accessed by Amazon employees or to recordings being used to train algorithms.

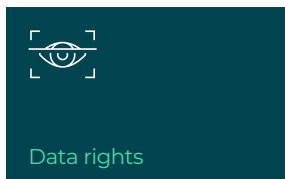
Links to further information

[Alexa announcement](#)[Ring announcement](#)[Alexa draft order](#)[Ring draft order](#)

SHOOSMITHS SAYS...

Alexa, is that the FTC at the door?

At least in Europe, Ring says it's not using recordings to train algorithms nor giving access to employees.

Jurisdiction: **EU (Berlin)**

Berlin DPA fines bank €300,000 for lack of transparency with automated decision-making

31 May 2023

Key details

The Berlin data protection authority (BBDI) has announced a fine of €300,000 on an undisclosed bank for breach of Arts 5(1)(a), 15(1)(h), and 22(3) of EU GDPR.

The complaint came after the bank used an algorithm which rejected the complainant's request for a credit card seemingly without justification. The bank did not provide any further information, just generic information on the scoring process. The complainant could not meaningfully challenge the decision.

The BBDI found that the bank failed to provide transparent and comprehensible information about the automated decision when requested and therefore this warranted the fine. The Commissioner held that where automated decisions are made it is a requirement that customers are informed of the reason behind the decision.

SHOOSMITHS SAYS...

Computer sagt nein.

The fine “took into account in particular the bank’s high turnover as well as the deliberate design of the application process and the information”

Links to further information

[EDPB summary](#)[Press release](#)

Jurisdiction: **UK**



ICO reprimands Thames Valley Police for releasing witness details to suspected criminals

2 June 2023

Key details

The ICO has issued a reprimand to TVP after they released information which led to suspected criminals finding out a witness's address. The witness has now had to move house and the risk to the individual remains high.

The TVP did not have training in place to ensure that officers were trained on the guidance on disclosure and redaction.

The ICO has recommended:

- Providing training to all staff responsible for redactions and disclosures
- Sharing updates to policies or processes as soon as they are available
- Continuously reviewing policies and guidance on the handling of personal data.

SHOOSMITHS SAYS...

“Our enforcement action in this case should act as a warning to other organisations”

We agree it should: so perhaps a case for imposing a fine?

Links to further information

[Reprimand](#)

[ICO press release](#)

Jurisdiction: **UK**Marketing, adtech &
cookies

ICO fines two firms for making unlawful marketing calls

14 July 2023

Key details

The ICO has issued a £130,000 fine to Crown Glazing Ltd for making more than 500,000 direct marketing calls to TPS registered people, resulting in 37 complaints.

It has also fined Maxen Power Supply Ltd £120,000 after more than 100 complaints about unsolicited marketing calls to businesses and individuals. The company used overseas operators that purported to be from National Grid or an existing energy supplier, but claimed these international call centres were “independent contractors” and “third party intermediaries”.

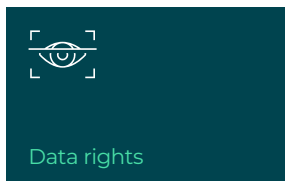
WHAT THEY SAY...

“In case organisations remain unclear on their obligations, the ICO operates a telephone helpline”

Links to further information

[Crown enforcement notice](#)[Maxen enforcement notice](#)[ICO press release](#)

Jurisdiction: **EU (Sweden)**



Swedish DPA announces Spotify fine of €4.98m for transparency failures

13 June 2023

Key details

IMY, the Swedish data protection authority, has issued the fine for Data Subject Access Request failures under Arts 12(1), 15(1) and 15(2) EU GDPR.

It notes that Spotify does have comprehensive privacy notices and DSAR responses, but:

- Information is not clear enough, and
- Too much technical information is supplied in English.

The decision has been made in co-operation with other authorities, and the violations are said to be of “low severity overall”.

SHOOSMITHS SAYS...

Makes the case for an elegant Scandi makeover.

“data subjects must receive meaningful information”

Links to further information

[Press release](#)

[Ruling \(Swedish only\)](#)

Jurisdiction: **EU (Italy)**



Marketing, adtech & cookies

Garante fines TIM SpA €7.6m for unlawful telemarketing activities

13 June 2023

Key details

A follow-up to sanctions in January 2022. The company is the former Telecom Italia SpA, and the fines relate to various infringements of EU GDPR, including:

- Marketing calls to opted-out customers
- DSAR failures and delays
- No online privacy policy for mobile subscribers
- A data breach.

SHOOSMITHS SAYS...

TIM's up.

Links to further information

[Ruling](#)

Jurisdiction: **EU**

CJEU publishes opinion on liability for Europol data breach

15 June 2023

Key details

The CJEU has issued the opinion of an Attorney General stating that Europol and a Member State can be jointly and severally liable for damage resulting from unlawful data processing in breach of Arts 49 and 50 of Regulation (EU) 2016/794 ('the Europol Directive').

The case has followed the murder of a Slovak journalist and his fiancée in 2018. Europol received data from a suspect's phone, which was unlawfully released to the public. The suspect raised a compensation claim which was dismissed. The claim has now been appealed to the CJEU.

The opinion recommends rejecting all grounds of appeal except one which relates to liability as between member states and Europol.

Case C-755/21 P Kočner v Europol

SHOOSMITHS SAYS...

You're appealing? You're appalling? Europol-ling!

Links to further information

[AG's opinion](#)

Jurisdiction: **EU**Marketing, adtech &
cookies

Commission sends Statement of Objection to Google alleging abusive practices in adtech

14 June 2023

Key details

The statement is part of formal proceedings opened in 2021 into whether Google has broken competition law rules by favouring its own online display advertising technology services, and restricting access by third parties to user data for advertising purposes on websites and apps.

The Commission It has sent Google a preliminary view that it is abusing its dominant position in breach of Art. 102 TFEU, by favouring its own ad exchange AdX:

- In the ad selection auction run by DFP (Google's publisher ad server)
- In the way it places bids on ad exchanges using Google Ads and DV360 (Google ad buying tools).

It is asking for mandatory divestment of parts of Google's business.

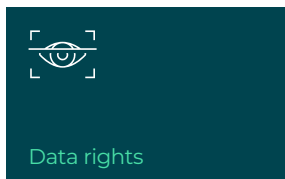
Google will now respond and there will be a formal hearing before possible remedies are imposed, including a fine of up to 10% annual worldwide turnover.

SHOOSMITHS SAYS...

The Commission's Ad
enough.

Links to further information

[Commission Press release](#)

Jurisdiction: **EU (France)**

CNIL fines KG COM €150,000 for unlawful processing of personal data

15 June 2023

Key details

CNIL has published details of its €150,000 fine of Société KG COM S.A. for breaches of EU GDPR and cookies violations under French law.

KG COM provides online clairvoyance readings, and the investigation followed a 2020 data breach.

CNIL has found:

- Systematic phone recording contrary to Art. 5(1)(c)
- Retention of bank account details without lawful basis (Art. 6)
- Failure obtain consent to collect special category data (Art. 9)
- Lack of transparency regarding processing (Arts 12 and 13)
- Security failings (Art. 32)
- Failure to notify breach (Art. 33)
- Non-compliant cookie use (Art. 82 French DPA).

The fine reflects a reduced company size following earlier regulatory problems.

Links to further information

[Decision](#)

[Press release](#)

SHOOSMITHS SAYS...

Didn't see that coming.

Jurisdiction: **UK**

Director guilty of s. 55 DPA offences subject to confiscation order under Proceeds of Crime Act

21 June 2023

Key details

A former director of Datasearch Services Limited (DSS) was found guilty in February 2022 of six offences under the Data Protection Act following a 2016 complaint to the ICO by Royal Bank of Scotland (RBS).

DSS was a tracing agent company used by the bank to find RBS creditors. The director recorded personal financial information and built profiles of consumers using impersonation techniques outside the bank's instructions.

He was prosecuted and pleaded guilty to six offences under s. 55 DPA in February 2022. He has now been ordered to pay back £38,000 under a POCA confiscation order, fined £10,560 and ordered to pay £15,000 court costs.

SHOOSMITHS SAYS...

High stakes POCA.

Links to further information

[ICO press release](#)

Jurisdiction: **EU (France)**

Marketing, adtech & cookies

CNIL confirms reduced €40m fine of Criteo for GDPR failings in personalised advertising

15 June 2023

Key details

Following complaints lodged by Privacy International and NOYB, Criteo S.A., an online advertising company, was issued with a notice of intent to fine €60m in June 2022 by the French DPA for GDPR failings including lack of consent, DSAR and transparency breaches. Criteo responded and CNIL has now issued a final decision revising the fine to €40m but finding substantial failings.

Criteo specialises in behavioural retargeting, tracking the behaviour of internet users via cookies in order to display personalised advertisements. CNIL found that although the company does not handle data subject names, the depth of data meant that re-identification was possible in some cases.

CNIL found the following breaches:

- Failure to demonstrate that personal data was obtained by partners with consent (Art. 7.1)
- Privacy policy was too broad in its terms (Art. 12 and 13)
- Information given in response access requests was incomprehensible (Art. 15(1))

- Requests to delete and withdraw consent only stopped personalised ads but did not erase identifiers or delete navigation history (Art. 7(3), 17(1))
- Failure to provide a compliant agreement between joint controllers (Art. 26).

Fine based on:

- Nearly 2% of company worldwide turnover (below the applicable limit of 4%)
- Large number of identifiers involved (370m)
- The company business model which relied on large personal data processing operations, and
- The ability to process without evidence of consent which drove increased income.

CNIL acknowledges that the company has now made changes to its practices.

The decision has been approved by all 29 supervisory authorities, and the company can appeal to the Council of State up to two months from the date of publication.

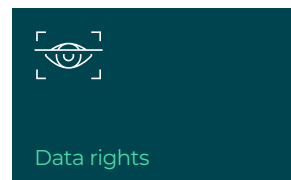
SHOOSMITHS SAYS...

Aggregating large amounts of data can also aggregate partner failings down the chain.

“contracts concluded with partners did not contain any clause obliging them to provide proof of users’ consent [...and] the company did not undertake any audit campaign of partners”

Links to further information

[Decision](#)
[Press release](#)

Jurisdiction: **EU**

CJEU holds that data subjects have the right to access date and reason for the consultation of personal data

22 June 2023

Key details

The CJEU has issued its judgment in a case referred by the Administrative Court of Eastern Finland.

The case was brought by a former employee of the bank whose personal data was accessed by the bank's internal audit team while the employee was still employed and a customer of the bank. The employee made a DSAR asking the bank to identify the individual who had consulted their data, the dates on which it was accessed and the purposes for which it was processed. The bank refused to identify the staff member(s) involved but provided some further details of the consultation.

The Court of Justice has confirmed the Attorney General's opinion (December 2022) that:

- The principles of GDPR apply to DSARs made since 25 May 2018, even if they relate to processing which took place before that date
- A controller must let the data subject know the dates and purposes of consultation operations by staff
- The controller does not have to disclose the identity of staff consulting the data, unless this is essential for the exercise of GDPR rights, bearing in mind the rights and freedoms of staff
- Rights of access were not affected by the fact that the controller was acting within the framework of a regulated activity, or the fact that the data subject happened to be an employee as well as a customer.

C-579/21 Pankki S

Links to further information

[Ruling](#)[Press release](#)

SHOOSMITHS SAYS...

Balancing the privacy rights of different classes of employees.

“Wherever possible, means of communicating personal data that do not infringe the rights or freedoms of others should be chosen”

Jurisdiction: **EU**

AG issues opinion on data subject access rights under Law Enforcement Directive

15 June 2023

Key details

The case concerns an individual who was refused a security clearance certificate by the Belgian National Security Authority, and requested the identity of the controllers responsible and access to the information concerning them. The Belgian Supervisory Body for Police Information (OCIP) confirmed that checks had been carried out but gave no further details. The individual brought a claim against the OCIP in the Belgian court, which has been referred to the European Court of Justice (CJEU).

The Attorney General's opinion is that:

- Belgian law is incompatible with the LED in creating a blanket exemption to the direct right of access
- Where an individual has to exercise rights indirectly through a supervisory body, that body may have to provide additional information depending on the circumstances 'in light of proportionality'.

Case C-333/22 Ligue des droits humains ASBL, BA v. L'organe de contrôle de l'information policière

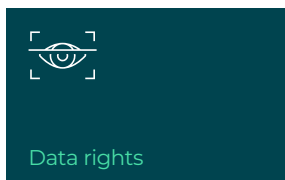
SHOOSMITHS SAYS...

CJEU flexes its muscles with Brussels.

We'll need the future CJEU ruling to understand quite what's going on here.

Links to further information

[Press release](#)

Jurisdiction: **EU (Italy)**

Garante announces €40k fine of VW Leasing GmbH for inadequate response to DSAR about creditworthiness

22 June 2023

Key details

A person who was refused credit by VW Leasing (VWL) when trying to buy a car made a data subject access request asking for information about the credit decision. VWL responded by reproducing information submitted by the applicant, saying it relied on a credit information system provided by a supplier to assess the risk, and inviting the data subject to contact the supplier directly to find out more.

The Garante has found that this was not an adequate response, and that VWL should have provided the information itself directly to the data subject.

The relatively low fine reflects:

- The single complainant, and first-time violation by the company
- Good faith in its suggested approach
- Co-operation with the regulator
- Provision of the required information to the data subject during the investigation.

SHOOSMITHS SAYS...

A useful reminder that a DSAR response is a controller responsibility.

Links to further information

[Ruling](#)

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

NOYB gets permission for judicial review of Data Protection Commission (DPC)

19 June 2023

Key details

According to reports in the Irish Times, None of Your Business (the data rights organisation run by Max Schrems) has succeeded in getting permission for a judicial review of the DPC's handling of complaints brought by NOYB against Meta and WhatsApp concerning processing of personal data for behavioural advertising, and reliance on 'performance of a contract' as a legal basis. It is asking for a declaration that the DPC failed to carry out its investigations within a reasonable time, contrary to EU GDPR and the Irish Data Protection Act. The case has now been adjourned for later hearing.

SHOOSMITHS SAYS...

NOYB tries yet another angle of attack.

Links to further information

[Court listing](#)



Industry & sector news

Jurisdiction: **EU (Ireland)**



Marketing, adtech & cookies

Microsoft reveals expected \$425m fine for LinkedIn ad practices

1 June 2023

Key details

Following investigations ongoing since 2018, the Irish Data Protection Commission has sent the company a draft decision on alleged GDPR violations through targeted ad practices by LinkedIn. It proposes a fine of approximately \$425m. Following a low-profile announcement on its investor relations site, the company has now made a statement. Nothing public from the DPC yet.

WHAT THEY SAY...

A (micro)soft target: yesterday they were fined \$20m under COPPA and the FTC Act for non-compliant Xbox data collection.

Microsoft “intends to defend itself vigorously in this matter”.

Links to further information

[MS statement](#)

Jurisdiction: **JAPAN**



Toyota announces long-term data leak in its Connected services

31 May 2023

Key details

Toyota has advised that information on customers both inside and outside Japan collected by its “Toyota Connect” system may have been externally accessible from October 2016 to May 2023, due to a “misconfiguration” of its cloud service.

Toyota has confirmed that a further 260,000 customers have been affected in Japan, but has not yet provided detailed information on overseas customers. It may affect cars bought since 2007.

This follows the announcement in May that the vehicle data of 2.15m Japanese users who had signed up to cloud services since 2012 has been externally available for 10 years.

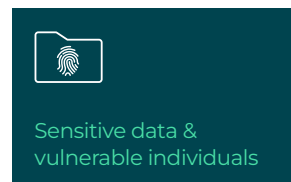
WHAT THEY SAY...

“we will work closely again with TC to explain and thoroughly enforce the rules for data handling”

Links to further information

[Toyota statement](#)

Jurisdiction: **UK**



NHS Trusts accused of sharing patient details with Facebook without consent

27 May 2023

Key details

An Observer/Guardian report alleges that the NHS has exposed information about patients' medical conditions, appointments and treatments with Facebook without consent, via the "Meta Pixel" tracking tool in 20 NHS Trust websites, which collects browsing information.

Collected information includes data on people visiting webpages about various sensitive health conditions, and data collected when users click on buttons to book appointments and order prescriptions.

17 of the 20 NHS Trusts that had Meta Pixel on their webpage have now confirmed they have removed it. Problems appear to be based on Trusts installing the tool for various recruitment and marketing campaigns without checking settings.

SHOOSMITHS SAYS...

No official ICO announcement, but it says it has "noted the findings" and is considering the matter.

Jurisdiction: **KUWAIT**



Kuwait to collect biometric data of everyone in the country

28 May 2023

Key details

The Kuwaiti government has announced it will start collecting fingerprint scans for everyone who lives in, and enters the country, over 18. The aim is to fingerprint all citizens and residents within a year.

To do this, the Ministry of Interior has installed 49 devices across the country, including at border crossings. These devices will not just collect fingerprint scans, but also face and eye scans if the fingerprinting does not work.

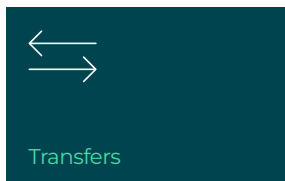
SHOOSMITHS SAYS...

According to legal commentators:

“There is no general data protection regulation. There is no general data protection authority.”

Countries including Japan and the US have been collecting biometric data of travellers for many years – but not for the population as a whole.

Jurisdiction: **EU**



Zoom to offer data localisation for paying customers in EEA

6 June 2023

Key details

Zoom will support localised data storage for premium customers who can choose specific data from its webinars, meetings, and team chat tools to store in Frankfurt. Data may still be shared with its U.S. operations in very specific or “exceptional” circumstances.

SHOOSMITHS SAYS...

[The dawn of localisation as a service?](#)

Jurisdiction: **US**Marketing, adtech &
cookies

Ticketmaster to bring website into compliance with DAA Self-Regulatory Principles

13 June 2023

Key details

The Digital Advertising Alliance (DAA) is a US ad-industry body representing 650 media companies which offers a self-regulation framework and responds to consumer complaints about online advertising. It has asked Ticketmaster Entertainment LLC to bring its website into compliance with the DAA Self-Regulatory Principles.

As a result, Ticketmaster has:

- Included a prominent link directing users to a page providing enhanced notice and opt-out tools
- Provided additional links to third-party opt-out tools and ad disclosure
- Committed to compliant cookies banners.

SHOOSMITHS SAYS...

Some of the big names are signed up to self-regulation: members include Google, Amazon, Facebook, Oracle, Netflix, eBay, Experian, Disney...

Links to further information

[Press release](#)[DAA Program Information](#)

Jurisdiction: **AUSTRALIA**



OAIC announces that it has been victim of cyber attack

15 June 2023

Key details

The Office of the Australian Information Commissioner (OAIC) has had data stolen by the Russian criminal ransomware group known as BlackCat, or ALPHV. The data was stolen from legal firm HWL Ebsworth, who act for the OAIC, on 8 May 2023.

SHOOSMITHS SAYS...

The biter bit.

“consistent with requirements under the Notifiable Data Breaches scheme, OAIC will notify affected individuals where necessary”

Links to further information

[OAIC Statement](#)

Jurisdiction: **US**

Senators launch investigation into use of health data by Amazon Clinic

16 June 2023

Key details

In a letter to the Amazon CEO, the senators are asking for information about Amazon Clinic to be disclosed by 30 June 2023, following reports that the online health platform is ‘harvesting health data’. The service, launched in November 2022, provides health information about common conditions to consumers in 32 states, by connecting them with ‘qualified telehealth providers’ and the ‘Amazon Pharmacy’. The senators allege that patients can only sign up to the services if they consent to ‘HIPAA authorisation’, in violation of the Act.

SHOOSMITHS SAYS...

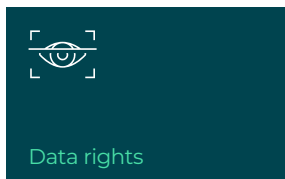
Senators fear they may be trading privacy for healthcare.

“customers deserve to fully understand why Amazon is collecting their health care data and what the company is doing with it”

Links to further information

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

Jurisdiction: **EU (Ireland)**



Irish Council for Civil Liberties urges Irish Parliament to prevent ‘criminalising’ DPC reporting

26 June 2023

Key details

The Irish Council for Civil Liberties (ICCL) has urged MLAs to challenge a proposed amendment to the Irish Courts and Civil Law (Miscellaneous Provisions) Bill 2022 when it comes up for final debate on 28 June 2023.

The last-minute government revision to s. 26A permits the DPC to direct that certain information which it deems to be confidential may not be disclosed, with violations resulting in a €5,000 fine, where ‘disclosure could reasonably be expected to prejudice the effectiveness of the performance by the Commission of a relevant function’.

The ICCL claims that the amendment will prevent critics of the DPC, such as Max Schrems, from discussing complaints and actions of the DPC freely.

WHAT THEY SAY...

“will gag people from speaking about how the DPC handles their complaint and from speaking about how big tech firms or public bodies are misusing their data”

Links to further information

[Amendments including Section 26A](#)

Jurisdiction: **EU (Denmark)**



Datatilsynet authorizes further use of facial recognition systems by football club

22 June 2023

Key details

The Danish data protection authority has announced an extension to its 2019 authorisation of Brøndby IF's use of facial recognition at stadiums for its matches. Under the new rules, they can use mobile systems at away matches, and develop a register of people who violate their rules of conduct.

This is already authorised under national law.

SHOOSMITHS SAYS...

Legal for now – but could face a challenge under the draft EU AI Act.

Links to further information

[Press release](#)



**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: July 2023

©Shoosmiths LLP 2023

SHOOSMITHS

www.shoosmiths.com

**FOR
WHAT
MATTERS**