

SHOOSMITHS

PRIVACY & DATA | GLOBAL EDITION

Data protection

May 2023 roundup

www.shoosmiths.com

FOR
WHAT
MATTERS



Legislation



Guidance & Consultations



Enforcement & Legal Action

THE **BIG** STORY



DPC publishes findings of enquiry into Meta transfers from EEA to US and fines Meta €1.2bn

22 May 2023













Industry & Sector News










INDEX

Index
















| | JURISDICTION |
|---|---------------------|
| Legislation | |
| 08  Digital Markets, Competition and Consumers Bill introduced into Parliament..... | UK |
| 09  Digital Services Act: European Commission designates first Very Large Online Platforms and Search Engines..... | EU |
| 10  Digital Markets Act becomes fully applicable | EU |
| 11  US Senators re-introduce “COPPA 2.0” | US (Federal) |
| 12  MEPs vote against US adequacy decision under EU-US DPF and go to US for discussions | EU/US |
| 13  Government releases Keeling Schedules for DPD1 (No 2) Bill..... | UK |
| 14  Government publishes list of laws to be revoked under REUL Bill | UK |
| 15  Artificial Intelligence (Regulation and Workers’ Rights) Private Members’ Bill introduced in House of Commons. | UK |
| 16  Bill prohibiting use of TikTok in state passed..... | US (Montana) |
| 17  Ruling on judicial proceedings exemption in DPA 2018 | 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

























| | | |
|----|--|--------------------|
| 19 |  ICO asks for views on data protection and content moderation..... | UK |
| 20 |  CMA gives fourth update on Google’s Privacy Sandbox on Chrome third party cookies..... | UK |
| 21 |  CNIL publishes work programme for connected vehicle working party..... | EU (France) |
| 22 |  EDPS proposes new rules to promote better cooperation..... | EU |
| 23 |  EDPB publishes Data Protection Guide for small businesses..... | EU |
| 24 |  EDPS publishes 2022 Annual Report..... | EU |
| 25 |  DRCF publishes annual report and workplan..... | UK |
| 26 |  Ofcom opens consultation on calling line identification (CLI) authentication..... | UK |
| 27 |  ENISA publishes report on AI cybersecurity standards in preparation for EU AI Act..... | EU |
| 28 |  FDPIC launches updated website and data breach portal..... | SWITZERLAND |
| 29 |  Call for evidence on Digital Markets, Competition and Consumers Bill..... | UK |
| 30 |  EDPB adopts guidelines on facial recognition technology in the area of law enforcement..... | EU |
| 31 |  ICO publishes guidance on DSARs for employers..... | UK |
| 32 |  Biometrics and Surveillance Camera Commissioner publishes letter to MP about surveillance cameras..... | UK |
| 33 |  CMA consults on whether to accept Meta binding commitments on use of DDA..... | UK |

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




| | | |
|----|---|--------------------------------|
| 35 |  AG's opinion on liability for third party breaches and non-material damages..... | EU (Bulgaria) |
| 36 |  ICO reprimands University Hospitals Dorset NHS Foundation Trust..... | UK |
| 37 |  Garante fines online marketing company €300k for misleading practices..... | EU (Italy) |
| 38 |  CJEU preliminary ruling on scope of right to a “copy” under Art. 15(3) | EU |
| 39 |  CJEU preliminary ruling on compensation for non-material damage | EU |
| 40 |  AG issues opinion on conditions for imposing a fine for infringement of EU GDPR..... | EU |
| 41 |  AZOP fines B2 Kapital €2.27m for unauthorised processing of personal data..... | EU (Croatia) |
| 42 |  AEPD fines GSMA Ltd €200k for failure to carry out DPIA before using biometric access system..... | US (Spain) |
| 43 |  ICO publishes TikTok enforcement and penalty notices..... | UK |
| 44 |  Findings against Clearview AI in Austria and France..... | EU (France and Austria) |
| 45 |  ICO reprimands two councils for failing to respond to information access requests | UK |
| 46 |  AG issues opinion on controller “fault” under EU GDPR in Covid app case..... | EU |
| 47 |  US FCC announces first use of new blocking powers to stop scam calls..... | US (Federal) |
| 48 |  AEPD publishes €75,000 fine for requiring photo ID as part of flat rental | EU (Spain) |
| 49 |  EDPB publishes binding decision on Meta transfers case..... | EU |
| 50 |  DPC publishes findings of enquiry into Meta transfers from EEA to US and fines Meta €1.2bn..... | EU (Ireland) |
| 51 |  CNIL fines health website over GDPR violations..... | EU (France) |
| 52 |  ICO fines two companies for unsolicited marketing calls..... | UK |
| 53 |  AG announces \$39.9m settlement with Google over location tracking practices..... | US (Washington State) |
| 54 |  CJEU dismisses Meta appeal challenging information requests in competition investigation..... | EU |
| 55 |  AEPD publishes fine imposed on Digi Spain Telecom €70,000 for processing without legal basis... | EU (Spain) |
| 56 |  AG agrees \$550,000 settlement with Practicefirst for data breach..... | US (New York) |
| 57 |  ICO reprimands Ministry of Justice after bags of confidential information left unsecured at prison..... | UK |
| 58 |  High Court strikes out class action for misuse of private information against Google and DeepMind | UK |

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

- 60  Garante authorises ChatGPT in Italy..... **EU (Italy)**
- 61  IABEurope and other trade associations ask Commission to keep level playing field in draft Data Act..... **EU**
- 62  ODA sends questionnaires to DPOs as part of EDPB survey..... **EU (Belgium)**
- 63  Apple and Google announce new specification to prevent unwanted Bluetooth tracking..... **GLOBAL**
- 64  Australian law firm victim of a Russian-linked ransomware attack..... **AUSTRALIA**
- 65  Norway DPA bans collection of grocery shopping data for government statistics..... **EU (Norway)**
- 66  Toyota reveals that driver data of up to 2.15m may have been exposed..... **JAPAN**
- 67  Google announces that Bard AI is available in 180 countries, but not including EU or Canada..... **GLOBAL**
- 68  Cyber Security Breaches Survey 2023 published..... **UK**
- 69  France’s constitutional court backs use of AI surveillance cameras for Paris Olympics..... **FRANCE**

Key:

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



Legislation



Digital Markets, Competition and Consumers Bill introduced into Parliament

25 April 2023

Key details

The bill contains provisions to strengthen consumer protections in digital markets.

The principal relevant provisions are:

- **Part 1:** Conduct requirements and merger control for platforms with “Strategic Market Status” (SMS) in respect of digital activity (aimed at e-commerce and social media sites), with a link to the UK, and turnover of £1bn in the UK or £25bn globally.
- **Part 2:** Changes to the Competition Act and Enterprise Act to update powers to intervene in anti-competitive activities.
- **Part 3:** Enforcement by CMA of “infringing commercial practices” directly or through the court, or via “online interface orders” to remove or change content, restrict access, display warnings, and delete domain names.
- **Part 4:** Consumer protections including bans on fake consumer reviews and a regime for renewal of subscription contracts.

Fines are tiered, and may rise up to 10% of global turnover. Enforcement and regulation will be by the Competition and Markets Authority (CMA).

The bill is expected to come into effect as soon as possible following parliamentary approval, subject to secondary legislation and the publication of guidance.

Links to further information

[Bill](#)

[Press release](#)

SHOOSMITHS SAYS...

Losing patience with sharp practice online.

“Smartphones and online shopping have profoundly changed the landscape. From abuse of power by tech giants, to fake reviews, scams and rip-offs like being caught in a subscription trap – consumers deserve better”



Digital Services Act: European Commission designates first Very Large Online Platforms and Search Engines

25 April 2023

Key details

Under the DSA, the European Commission has designated 17 Very Large Online Platforms (VLOPs) and two Very Large Online Search Engines (VLOSEs) that reach at least 45 million average monthly active users in the EU. These include platforms such as TikTok, Facebook, Instagram, Wikipedia, Snapchat and Google Search.

These companies will be subject to more obligations than other intermediary services.

By 25 August 2023, the designated companies must comply with full DSA obligations including:

- Submitting their first annual risk assessment to the Commission for independent audit
- Identifying, analysing and mitigating a wide array of risks
- Ad labelling and listing
- Passing data to researchers
- Publishing compliant terms and conditions in clear summary
- Designing systems to protect children
- Flagging and acting on illegal content.

Links to further information

[Press release](#)

SHOOSMITHS SAYS...

Holding the household names accountable for the safety of online users.

And an official pun:

“Today is the D(SA)-Day for digital regulation”



Digital Markets Act becomes fully applicable

2 May 2023

Key details

The provisions of the DMA (Regulation 2022/1925) now apply in full.

The DMA sets out new obligations for platforms that act as “gatekeepers” in the digital sector, and grants the Commission authority to carry out market investigations and exercise enforcement powers.

Presumed gatekeepers have at least €7.5bn annual turnover or €75bn market capitalisation, a “core platform service” in 3 member states, 45m active EU end users, plus an “entrenched and durable position”.

The DMA contains various obligations on gatekeepers relating to end user functionality, third party interoperability, and advertiser access to performance measuring tools. Business users must be allowed to promote offers and conclude contracts outside the gatekeeper platform.

It grants a potential right of action in EU national courts for those harmed by gatekeeper conduct.

Potential gatekeepers have until 3 July 2023 to notify their core platform services to the Commission. The Commission then has until 6 September 2023 to decide whether the company meets the threshold. Confirmed gatekeepers must comply with DMA requirements by 6 March 2024.

Links to further information

[DMA text](#)

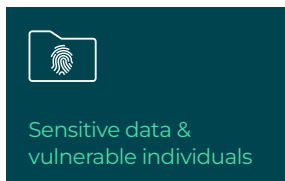
[Press release](#)

[Revised Q&A](#)

SHOOSMITHS SAYS...

Playing fair in the digital playground.

“one of the first regulatory tools to comprehensively regulate the gatekeeper power of the largest digital companies”



US Senators re-introduce “COPPA 2.0”

5 May 2023

Key details

Two senators have reintroduced their updated version of the Children Online Privacy Protection Act (COPPA) 1998.

Key reforms would:

- Require consent to collect personal information from 13 to 16 year olds
- Ban targeted advertising to minors
- Revise the current “actual knowledge” tests to “reasonably likely”
- Require an “eraser button” where technologically feasible
- Establish a digital marketing Bill of Rights for teenagers and a youth marketing division at the FTC.

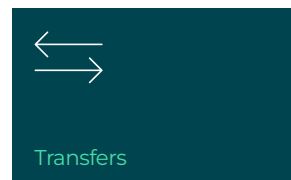
This is a bipartisan bill, with major support.

WHAT THEY SAY...

“today’s online guardrails were written before the invention of the iPhone... We won’t address the threats to young people if we don’t stop the data practices at the root of the problem”

Links to further information

[Press release](#)



MEPs vote against US adequacy decision under EU-US DPF and go to US for discussions

11 May 2023

Key details

Members of the European Parliament have voted 306-27 with 231 abstentions to reject the adequacy decision forming part of the proposed EU-US Data Privacy Framework.

Key objections are on bulk collection, the new DPRC court (based on secrecy and presidential interference), lack of maturity of US intelligence practices, and the likelihood of the DPF being overturned by the Court of Justice (CJEU).

In response to this rejection, MEPs are meeting with US lawmakers, regulators and government officials in Washington DC on 15-18 May to discuss the DPF together with a wide range of other current policy issues.

The Commission must take account of the MEPs but their decision is not binding. The Commission will take this, plus the EDPB opinion, into consideration. It must also get approval from a committee of member state representatives.

WHAT THEY SAY...

“contains significant improvements, but unfortunately, we are not there yet... the mechanism must genuinely protect the data of EU citizens and businesses”

Links to further information

[Press release](#)

[Announcement](#)



Government releases Keeling Schedules for DPDI (No 2) Bill

10 May 2023

Key details

The Government has published Keeling Schedules (redline versions) of the proposed changes to be introduced by the Data Protection and Digital Information (No 2) Bill to UK GDPR, Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (PECRs).

The bill:

- Clarifies the definition of scientific research to include commercial activity
- Recognises some legitimate interests (some of which will not require the balancing test) such as direct marketing, crime and national security, transfer of data within organisations for administrative purposes, and ensuring network security
- Widens powers to process for new purposes
- Clarifies anonymisation and identifiability tests for personal data
- Changes record keeping requirements
- Reforms the ICO to devolve power from the Commissioner onto a board
- Replaces independent Data Protection Officers with Senior Responsible Individuals
- Creates a new “data protection test” for international transfer
- Upholds existing safeguards for international transfers.

It grants wider government powers to change rules by secondary legislation.

Links to further information

[Press release](#)

[GDPR schedule](#)

[PECRs schedule](#)

[DPA schedule](#)

SHOOSMITHS SAYS...

Dippidy-doooh-dah.

The Information Commissioner has told the Public Bills Committee that DPDI2 won't affect UK adequacy, as it “retains all the rights” of EU GDPR.

...we shall see.



Government publishes list of laws to be revoked under REUL Bill

10 May 2023

Key details

Amendments to the proposed Retained EU Law (Revocation and Reform) Bill include new Schedule 1, which lists the pieces of legislation to be revoked under the new “opt-in” system for identifying laws to be repealed on 31 December 2023.

UK GDPR, NIS and the PECRs are not included, so will not be affected by the bill as currently conceived.

The bill revokes the Data Retention and Acquisition (DRA) Regulations 2018 (SI 2018/1123) which modify Parts 3 and 4 of the Investigatory Powers Act 2016, and regulate the powers of public authorities to acquire communications data from telecoms companies under the “Communications Code”. The DRA Regulations were introduced as a result of a CJEU ruling on non-compliance of the UK regime with European Fundamental Rights, and provide (among other things) for independent authorisation of acquisition requests by the Investigatory Powers Commissioner.

The bill may also still affect the status of past CJEU decisions, such as Schrems II.

Lords is debating amendments which (1) affect the role of retained EU case law and (2) require parliamentary scrutiny of individual pieces of legislation before it can sunset.

Links to further information

[REUL list](#)

[DRA Regulations](#)

SHOOSMITHS SAYS...

Another juggle in the Brexit Freedom balancing act.



Artificial Intelligence (Regulation and Workers' Rights) Private Members' Bill introduced in House of Commons

17 May 2023

Key details

Introduced by Labour MPs to protect the rights of individuals working alongside AI in shops, offices, factories and services.

The Bill:

- Calls for regulation and sector-specific guidance on “high-risk” AI
- Creates a statutory duty for employers to consult with trade unions and employees before using AI in the workplace
- Amends the DPA 2018 and Employments Rights Act 1996 to strengthen equalities
- Creates a right to human review of AI “high-risk” decisions
- Establishes a right for workers to disconnect from work.

It is based on a TUC report. The bill is not expected to be taken forward in this Parliament, but is designed to draw attention to the need to protect workers’ rights in the face of AI development. It may form part of a future Labour manifesto.

WHAT THEY SAY...

“recognising the importance of people in a world increasingly run by machines”

Links to further information

[Motion for leave](#)

[TUC reports](#)



Bill prohibiting use of TikTok in state passed

18 May 2023

Key details

The Montana Governor has approved the act which attempts to stop the company's operations within the state.

The prohibition is violated by

- The operation of TikTok by the company or users
- The option to download the TikTok mobile app being provided by a mobile app store

within Montana.

An entity may be fined \$10,000 for each violation plus \$10,000 a day for every day the violation subsists. There are no fines for individual users. There are exemptions for government, law enforcement and research uses. It will be enforced by Dept of Justice.

Subject to surviving legal challenge, the law will be in effect from 1 January 2024.

SHOOSMITHS SAYS...

[Stopping the TikTok clock.](#)

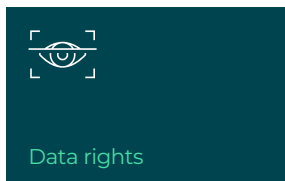
“to protect Montanans’ personal and private data from being harvested by the Chinese Communist party”

[...tip...just use a VPN.](#)

Links to further information

[Bill](#)

[Bill history](#)



Ruling on judicial proceedings exemption in DPA 2018

26 May 2023

Key details

The High Court has considered the “judicial proceedings” exemption in para 14, Part 2, Schedule 2 of the Data Protection Act 2018 which suspends certain provisions of the UK GDPR for personal data processed by an individual or court “acting in a judicial capacity” or where judicial independence might be prejudiced.

Proceedings were brought by an individual against a provider of court transcription services and a costs judge for failing to respond to a DSAR in the context of longstanding litigation against a government department.

Findings:

- The exemption covers all judicial functions including a transcription service
- A litigant cannot use DSARs to obtain litigation documents or conduct investigations – they need to go through appeals process
- It does not matter if a party is not present at hearing.

The court refused to grant discretionary relief for late response to a DSAR which was – at most – two days late.

Obiter, the judge cast some doubt on the ICO way of calculating a calendar month for a DSAR response, i.e. the corresponding calendar date of the next month following receipt, saying: “I would not necessarily endorse the entirety of that guidance”.

Links to further information

[Judgement](#)

SHOOSMITHS SAYS...

First detailed consideration of the scope of the judicial exemption to the right to access.

Guidance & consultations



Jurisdiction: **UK**



ICO asks for views on data protection and content moderation

2 May 2023

Key details

The Information Commissioner has called for views on data protection issues arising when doing content moderation, in preparation for the Online Safety Bill. It wants to hear about what personal data is processed when content moderation is being carried out, whether clarification of applicable law is needed, and the challenges of compliant moderation. Follows the joint statement with Ofcom made in November 2022.

SHOOSMITHS SAYS...

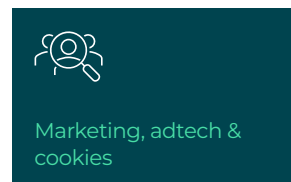
Facing the data protection paradox: editing data means processing data.

“We have a role to ensure that personal data is processed in compliance with data protection law during content moderation”

Links to further information

[Call for views](#)

Jurisdiction: **UK**



CMA gives fourth update on Google's Privacy Sandbox on Chrome third party cookies

27 April 2023

Key details

The Competition and Markets Authority has reported on the implementation of Google's legally binding commitments given in February 2022 to replace third party cookies in Chrome with alternative "Privacy Sandbox" tools.

They say Google is on track, but would like feedback from advertisers, ad techs and civil society groups (in and out of the UK) and are encouraging representatives of these groups to get in touch.

The CMA says it needs to "build a deeper understanding of Google's internal data control systems in order to robustly test Google's proposals on Chrome browsing history, Google Analytics data, and ad inventory on websites not owned and operated by Google".

SHOOSMITHS SAYS...

A Chrome cracker.

"Google intends to remove third party cookies from Chrome in the second half of 2024"

Links to further information

[Report](#)

Jurisdiction: **EU (France)**



CNIL publishes work programme for connected vehicle working party

25 April 2023

Key details

CNIL (the French DPA)'s "Compliance Club", (made up of manufacturers, rental companies and service operators) is prioritising discussions on the use of geolocation data, both as used in commercial vehicle fleets and as part of vehicle ownership.

It will publish summaries and draft guidance based on a series of workshops in 2023. Other topics will follow.

SHOOSMITHS SAYS...

"The regulatory method used by the CNIL for several years is intended to be predictable and based on exchanges with all stakeholders"

... they like fining, too.

Links to further information

[Press release](#)



EDPS proposes new rules to promote better cooperation

25 April 2023

Key details

The European Data Protection Supervisor has proposed additions to the Commission's proposal for a regulation on new procedural rules relating to GDPR enforcement, introduced in February 2023.

It is trying to address ambiguities in Chapter VII of GDPR which "curtail efficient and effective cooperation". For example, the EDPS cannot compel a national DPA to enforce findings about the "EUGDPR", the data protection law for EU institutions. If institutions have disputes with non-EU processors (say, an EU agency using a US cloud service provider), then this is arguably outside national DPA competence.

The EDPS has drafted a new Article to address these problems with an explicit duty of cooperation.

SHOOSMITHS SAYS...

Getting a better grip for the ongoing tussle with the Irish DPC.

“practical experience has confirmed that certain obstacles persist and the EDPS now considers that legislative intervention is warranted”

Links to further information

[EDPS report](#)

[Commission proposals](#)

Jurisdiction: **EU**



EDPB publishes Data Protection Guide for small businesses

27 April 2023

Key details

The European Data Protection Board has produced an interactive guide with short videos and checklists to help small businesses understand data protection compliance. Areas the guide covers include:

- Data subject rights
- Data breaches
- Data security and general compliance
- Links to materials for SMEs from national Data Protection Authorities.

SHOOSMITHS SAYS...

There's nothing small about GDPR or the EU.

The guide is “currently available in English and will be made available in other EU languages over time”

Links to further information

[Guide](#)

[Press release](#)

Jurisdiction: **EU**



EDPS publishes 2022 Annual Report

20 April 2023

Key details

Current preoccupations of the European Data Protection Supervisor are:

- Complexity brought by the DGA, DMA, DSA, AI Act and Data Act – EDPB will “strive to ensure that data protection is not undermined”
- Digital Euro project, and proposals to enable data sharing and third-party access for a wide range of financial sectors and products
- Supervision of large-scale IT systems under the new interoperability framework, especially the difficulty of upholding data subject rights through complex data flows
- Algorithmic profiling
- Ukraine – using the Eurojust database for hub for preserving evidence of war crimes.

Plus, reflections on Covid, the Schengen area, using non-EU processors, DPOs, Europol, data breach by EU institutions, and more.

WHAT THEY SAY...

“With this role comes a sense of responsibility to contribute to reflections on the function of the state in a democratic society”

Links to further information

[Annual report](#)

[Press release](#)

[Executive summary](#)

[Speech before LIBE Committee](#)

Jurisdiction: **UK**

DRCF publishes annual report and workplan

27 April 2023

Key details

The Digital Regulation Cooperation Forum was founded in 2020 to support regulatory co-ordination in digital markets, and co-operation on areas of mutual importance. It consists of the ICO, FCA, CMA and Ofcom. It is voluntary and does not override individual regulators.

The annual 2022/2023 report sets out the progress made in key areas such as:

- Coherence between regimes – initially, the Online Safety Act (ICO/Ofcom)
- Sharing and promoting best practice in areas of common interest, including horizon scanning.

Future areas of interest include illegal online financial promotions, regulation of digital assets and online advertising.

SHOOSMITHS SAYS...

Baby steps from a possible digital “super-regulator”.

Links to further information

[Annual report](#)[Workplan](#)

Jurisdiction: **UK**



Marketing, adtech & cookies

Ofcom opens consultation on calling line identification (CLI) authentication

28 April 2023

Key details

The telecoms regulator is carrying out a consultation on the introduction of CLI authentication. This would require network providers to confirm the authenticity of each caller's number before passing it to the call recipient, in an effort to stop spam calls.

This would require extensive investment by the regulator and telecoms providers including integration of CLI authentication into networks; crypto key and certificate management; establishment of an administrator; a common database; plus some rules about dealing with attestation, exceptions and failures.

Ofcom is also publishing reports, including one on US/Canada experiences under their "STIR/SHAKEN" programmes. Their key takeaway is that all network providers must take part and buy in to any CLI authentication system.

Closes 23 June 2023.

SHOOSMITHS SAYS...

Dialling down nuisance calls.

"UK Voice Service Providers have already agreed to take an important first step towards these goals by planning to convert their networks to all Internet Protocol by 2025"

Links to further information

[Consultation](#)

Jurisdiction: **EU**



ENISA publishes report on AI cybersecurity standards in preparation for EU AI Act

27 April 2023

Key details

The ENISA (EU Cybersecurity Organisation) report provides an overview of existing and planned AI cybersecurity standards, highlighting where new standards may be needed, in preparation for the draft EU AI Act.

The report's recommendations include:

- Taking a broad definition of “cybersecurity” to include general trustworthiness of systems
- Understanding gaps and getting standardised AI terminology
- Technical guidance on how existing standards should be applied to AI
- Focus on machine learning (as this is where major developments are happening now).

SHOOSMITHS SAYS...

Speaking the same language for those large language models.

“AI systems will, once in a while, make wrong predictions... it is still difficult to understand when the AI system will fail, but it will eventually”

Links to further information

[Press release](#)

[Report](#)

Jurisdiction: **SWITZERLAND**

FDPIC launches updated website and data breach portal

11 May 2023

Key details

The Swiss Federal Data Protection and Information Commissioner ('FDPIC') has launched its updated website in preparation for the revised Federal Act on Data Protection, which will come into effect on 1 September 2023 (and largely reflects GDPR). They have also introduced the 'DataBreach Portal'.

The updated website has dedicated sections outlining new principles, rights, and obligations as well as key topics covered, such as the duty to provide information.

The 'DataBreach Portal' enables data controllers to promptly report any data breaches in electronic form. From 1 September 2023 all reports must be made through the portal.

Links to further information

[Press release](#)[Reporting portal](#)

SHOOSMITHS SAYS...

Will all go like clockwork.

Switzerland:

- is not in the EU/EEA
- has adequacy decisions with the EU and UK
- has invalidated Privacy Shield like the EU
- recognises EU SCCs, with adaptations



Call for evidence on Digital Markets, Competition and Consumers Bill

18 May 2023

Key details

The DMCC institutes a competition regime for the largest and most powerful digital platforms including a mandatory code of conduct and merger control. It includes revocation and replacement of the Consumer Protection for Unfair Trading Regulations (CPUT regs). The House of Commons Public Bill Committee has published a call for evidence on the Bill.

The Committee will sit from 13 June and report by 18 July. Anyone looking to submit written evidence is advised to do this as soon as possible.

SHOOSMITHS SAYS...

[A chance to run DMCC.](#)

Links to further information

[Call for evidence](#)



EDPB adopts guidelines on facial recognition technology in the area of law enforcement

17 May 2023

Key details

The final version of the Guidelines has been adopted following public consultation. They provide guidance to EU and national lawmakers and law enforcement authorities on using FRT systems, based on interpretation of the Law Enforcement Directive.

The European Data Protection Board repeats its call for a ban on the use of FRT in the following cases:

- For remote identification in public spaces
- For categorisation of individuals into clusters using various discriminatory grounds
- To infer the emotions of a natural person
- Using a database populated by mass-scale scraping techniques (Clearview-style).

Bans would be implemented via the new EU AI Act.

SHOOSMITHS SAYS...

[Setting the FRT boundaries.](#)

Links to further information

[Guidelines](#)

[Press release](#)



ICO publishes guidance on DSARs for employers

24 May 2023

Key details

The ICO has published a blog and Q&A for employers on dealing with DSARs.

Covers:

- Request format and clarification
- Withholding information
- Third party information
- Witness statements
- Whistleblowing reports
- Confidential references
- Exemptions for legal professional privilege and crime/taxation, management information
- Recording negotiations with requester
- Unfounded and excessive requests
- NDAs and grievance processes
- CC-d emails
- Social media searches
- CCTV footage.

15,848 complaints were reported to the ICO between April 2022 and March 2023.

Links to further information

[ICO blog](#)

[ICO guidance](#)

SHOOSMITHS SAYS...

“many employers are misunderstanding the nature of subject access requests”

ICO says it will not advise on responses but will contact an organisation if there is a complaint.

Jurisdiction: **UK**

Biometrics and Surveillance Camera Commissioner publishes letter to MP about surveillance cameras

12 May 2023

Key details

The Commissioner's letter addresses an MP's concerns about the use of surveillance cameras around the homes of MPs.

The letter makes the following points:

- UK privacy rights are only derived from the Convention on human rights
- The only specific regulation of cameras is by ICO through data protection legislation
- The only UK code for camera installation was issued in 2012, and revised in 2022; it only covers police and local authorities
- The code will be abolished under the proposed Data Protection and Digital Information (No. 2) Bill, after which "there will be no specific legal instrument directly addressing the use of surveillance camera systems, by the police or at all"
- It took a long time for the government to acknowledge security risks from foreign-made cameras.

Concerned MPs should complain to the ICO, police and Security Minister who chairs the "Defending Democracy Taskforce" and is promoting a "National Security Bill".

SHOOSMITHS SAYS...

Plea for better regulation from the last camera commissioner.

"private citizens now have access to technology that was only recently the preserve of state intelligence agencies"

Links to further information

[Letter](#)



CMA consults on whether to accept Meta binding commitments on use of DDA

26 May 2023

Key details

The Competition and Markets Authority is consulting on whether to accept binding commitments from Meta in relation to competition investigations into its digital display advertising services (DDA) in Facebook Marketplace.

Meta has proposed various modifications to its practice including a “Marketplace Technical Solution” (redaction and firewalling) and an opt-out for advertisers.

The CMA’s preliminary view is that the commitments would address the concerns identified.

Consultation closes 26 June 2023.

SHOOSMITHS SAYS...

Pragmatism and efficiency, or the easy way out?

“this would avoid having to pursue a potentially lengthy investigation and leads to earlier changes that would benefit businesses and consumers”

The EU is signalling a very different approach (see page 54).

Links to further information

[Call for evidence](#)

[CMA press release](#)



Enforcement & legal action

Jurisdiction: **EU (Bulgaria)**

AG's opinion on liability for third party breaches and non-material damages

27 April 2023

Key details

The original claim was brought by an affected person following the 2019 leak of social security information of millions of Bulgarian citizens by the NAP (the national tax authority). The opinion from the Attorney General is for a preliminary ruling on referral from the Bulgarian Court of Appeal. (Natsionalna agentsia za prihodite (Case C-340/21) EU:C:2023:353)

Key findings:

- No automatic assumption of inadequate TOMs where there is a data breach – though the controller will have the burden of proof
- Third party breach will not exempt controller from liability – will depend on the “not in any way responsible” test (Art 82(3))
- Fear of future data misuse can be non-material damage which gives rise to compensation, but only if it is actual and certain emotional damage and not simply trouble or inconvenience.

Not binding on ECJ, but likely to be followed.

Links to further information

[Judgement](#)

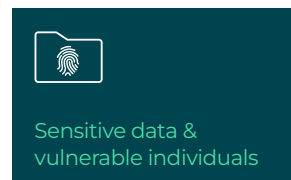
[CJEU press release](#)

SHOOSMITHS SAYS...

Pushing at the data damages door.

And opening the door to forum shopping for emotional damages?

“There is a fine line between mere dissatisfaction and genuine non-pecuniary damage, but the national courts, which are responsible for drawing this dividing line on a case-by-case basis, should carefully assess all the evidence produced by the person concerned. What matters is a disorder of an objective nature, even of low intensity, provided that it is demonstrable”

Jurisdiction: **UK**

ICO reprimands University Hospitals Dorset NHS Foundation Trust

25 April 2023

Key details

The NHS Trust wrote a letter to various recipients which had the full address of all other cc-d recipients at the bottom. This was done to “prevent any errors when manually writing addresses on envelopes”. As a result, the address of one data subject was disclosed to their abusive ex-partner.

The ICO has found infringement of Art. 5(1)(f) UK GDPR.

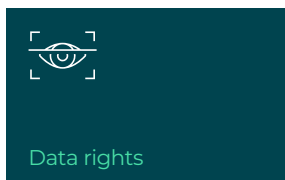
The Trust’s proposed solution (which has been accepted by the ICO) is that they will look at what other organisations are doing, and will try to act where their practice might pose a risk – for example by blind cc-ing, but only where patients have told the doctor in advance.

SHOOSMITHS SAYS...

Data protection in UK public institutions is apparently on life support.

Links to further information

[ICO reprimand](#)

Jurisdiction: **EU (Italy)**

Garante fines online marketing company €300k for misleading practices

23 February 2023

Key details

The fine was imposed in February 2023 following complaints about the practices of Ediscom, which collates and sells data for marketing purposes, including through recipe and quiz websites. It holds information on 21m people, and holds the largest proprietary digital marketing database in Italy. The Garante found that it:

- Used dark patterns to obtain consent
- Collected excessive personal data
- Gave insufficient warnings about third party use
- Failed to manage consent properly
- Failed to check consents on third party data.

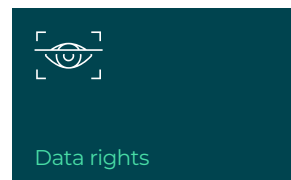
It also imposed various prohibition and compliance orders.

SHOOSMITHS SAYS...

First ruling on dark patterns by the Italian regulator.

Links to further information

[Ruling](#)

Jurisdiction: **EU**

CJEU preliminary ruling on scope of right to a “copy” under Art. 15(3)

4 May 2023

Key details

The CJEU has given its preliminary ruling on the scope of the EU GDPR right to a “copy” of personal data being processed under Art. 15. Art. 15(1) contains rights to a confirmation of processing from the controller, access to personal data and additional information; Art. 15(3) is the right to a “copy of the personal data undergoing processing”.

The original complaint was against CRIF, an agency which provides credit information to lenders. The data subject asked for emails and database extracts “in a standard technical format”, and they provided a list and summary statement of his personal data.

Key points:

- The right to obtain a “copy” of personal data under Art. 15(3) EU GDPR means “a faithful and intelligible reproduction of all their personal data undergoing processing”

- This entails the right to obtain copies of extracts from documents, or even entire documents or extracts from databases if the provision of such a copy is essential in order to enable the data subject to exercise GDPR rights, although account must be taken of the rights and freedoms of others
- “Copy” in Art. 15(3) means a copy of personal data, not of a document
- “Information” in Art. 15(3) does not refer back to Art. 15(1)
- Art. 15(3) is about the “practical arrangements” for Art. 15(1); it does not establish a separate right from the Art. 15(1) right.

It confirms the AG’s opinion, published 15 December 2022.

SHOOSMITHS SAYS...

Copyright on the copy right.

Links to further information

[Summary](#)

[AG’s opinion](#)

Jurisdiction: **EU**

CJEU preliminary ruling on compensation for non-material damage

4 May 2023

Key details

The Österreichische Post (OP) Supreme Court case. The Austrian postal service sells information about political affinities for targeted advertising. OP generated and retained (but did not communicate) personal data about presumed political affinities based on statistical guesswork. This offended the data subject who asked for compensation under Art. 82(1): the right to compensation for any person who has “suffered material or non-material damage due to infringement”.

The AG’s opinion, published 7 October 2022, concluded that mere upset is not “non-material damage” leading to compensation rights.

The ECJ has ruled that:

- mere infringement of the GDPR is not sufficient to confer a right to compensation: there must also be damage and a causal link
- the right to compensation is not limited to non-material damage that reaches a certain “threshold of seriousness as this would be too narrow, and “liable to fluctuate”
- national courts must apply the domestic rules of each member state relating to the extent of financial compensation (subject to equivalence and effectiveness principles).

Links to further information

[ECJ preliminary ruling](#)

[AG’s opinion](#)

SHOOSMITHS SAYS...

[**Squaring the compensation circle.**](#)



AG issues opinion on conditions for imposing a fine for infringement of EU GDPR

3 May 2023

Key details

The Advocate General has issued an opinion prior to a preliminary ruling on the conditions under which an administrative fine may be imposed on a legal person for infringement of the GDPR.

It arises from a €14.3m fine on a real estate company for having failed to enable regular deletion of tenant data. The major fine was for deliberate infringement of Art. 25(1) and Art. 5(1) (plus a small fine for infringement of Art. 6(1)). The fines were overturned in the national court, and the public prosecutor has appealed.

The AG's opinion is that:

- A company as controller can be fined even where there is no prior finding of infringement by employee(s)
- GDPR fines require intentional or negligent conduct by a controller.

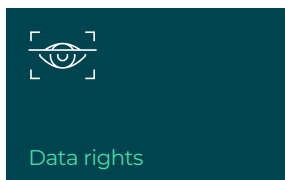
SHOOSMITHS SAYS...

Good and bad news for controllers: no strict liability, but responsibility for the outcome of staff conduct.

Links to further information

[AG's opinion](#)

Jurisdiction: **EU (Croatia)**



AZOP fines B2 Kapital €2.27m for unauthorised processing of personal data

4 May 2023

Key details

The fine was imposed following an anonymous tip-off in December 2022, accompanied by a USB stick which contained personal information of 77,317 debtors.

AZOP found:

- Lack of legal basis for the processing
- Failure to inform data subjects
- Failure to enter a contract with the processor
- Breach of confidentiality and security obligations.

AZOP therefore imposed the fine for violations of Art.s 6(1), 13(1), 28(3), 32(1)(b), and 32(2) of EU GDPR.

SHOOSMITHS SAYS...

Kapital punishment.

“We also point out that in this particular case it is about possible individual criminal liability... which is within the competence of the Ministry of the Interior” - AZOP

Jurisdiction: **EU (Spain)**

AEPD fines GSMA Ltd €200k for failure to carry out DPIA before using biometric access system

10 May 2023

Key details

The complainant – a British resident in Spain – was speaking at the 2021 Mobile World Congress, a mobile communications industry trade show, in Barcelona. Attendees were asked to upload passport details including photographs, in advance, to be processed in a third country. This would enable entry into the “BREEZ” (Biometric Recognition Easy Entry Zone) which allowed contactless ID mechanism. Presenters couldn’t register without doing this.

The fine was for failure to carry out a Data Protection Impact Assessment to assess the risks, proportionality and necessity of the system on the rights and freedoms of the interested parties.

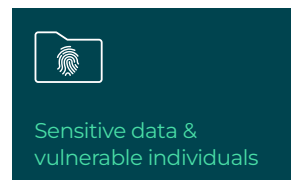
SHOOSMITHS SAYS...

no BREEZ.

Links to further information

[Ruling \(Spanish only\)](#)[GSMA reponse](#)

Jurisdiction: **UK**



ICO publishes TikTok enforcement and penalty notices

15 May 2023

Key details

The notices relate to the £12.7m fine announced in April 2023 for violations of data protection law in relation to children's data.

Includes the following Annexes:

- Annex 2: detailed analysis of how the ICO estimated the number of children under 13 using the service
- Annex 3: details of infringement, including determinations on the use of generic email addresses for DPOs; and on the requirements of Arts 13(1) and 13(2).
- Annex 4: examples of content on TikTok aimed at users under 13.

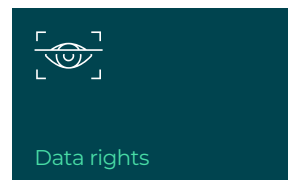
SHOOSMITHS SAYS...

The fine print.

“the steps taken by TikTok as the data controller were not commensurate to its size and resources or to the seriousness of the issues [...] the total penalty amounts to just 2.32% of the combined turnover of TikTok Ltd and TikTok Inc, and only 0.036% of the turnover of ByteDance”

Links to further information

[Notices](#)

Jurisdiction: **EU (France and Austria)**

Findings against Clearview AI in Austria and France

10 May 2023

Key details

The Austrian data protection authority (DSB) has found Clearview AI Inc. in violation of Arts 5(1)(a), (b), and (c), 6(1), and 9(1) of the GDPR and has ordered them to delete the complainant's personal data and to designate a representative within the EU, following a complaint submitted by an individual. No fine has been imposed.

The French data protection authority (CNIL) has imposed a further penalty payment of €5.2 million on Clearview AI Inc., due to non-compliance with the injunction it issued on 17 October 2022. Adds €100k per day to the existing €20m fine, for the period up to February 2023. The French government is apparently asking the Federal Trade Commission for advice on enforcement in the US.

SHOOSMITHS SAYS...

On top of (unpaid) fines from UK, Greece, Italy.

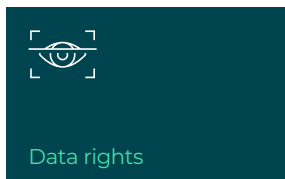
They won't ever pay up, but fines mean that the business is effectively closed in Europe, as organisations using Clearview may also be fined. Also makes strict regulation under the AI Act more likely.

And see effect on Google Bard, below.

Links to further information

[CNIL press release](#)[NOYB press release](#)[CNIL Ruling](#)[DSB decision](#)

Jurisdiction: **UK**



ICO reprimands two councils for failing to respond to information access requests

28 April and 5 May 2023

Key details

The ICO has reprimanded Norfolk County Council and Plymouth City Council after they failed to respond to DSARs from the public, in breach of Arts 12(3), 15(1) and 15(3) UK GDPR.

Between April 2021 and April 2022, Norfolk only responded to 51% of DSARs on time (251 residents).

Plymouth City Council had 18 requests taking up to two years to complete and a further 18 requests taking between three months and one year. There were also 20 outstanding requests up to a year old, and eight requests still outstanding up to two years later.

The Councils must provide details of actions taken to address recommendations within six months.

SHOOSMITHS SAYS...

We're so SAR-ry.

“Other organisations should take note that we will act if they fail to meet their legal obligations when responding to SARs”

Expensive, though – Plymouth has had to take on 3 more full time staff to get back on track.

Links to further information

[Norfolk reprimand](#)

[Plymouth reprimand](#)

Jurisdiction: **EU**

AG issues opinion on controller “fault” under EU GDPR in Covid app case

4 May 2023

Key details

The Advocate General’s opinion is the basis for a preliminary ruling by the CJEU on a matter brought from Lithuanian court. Arises from concerns about the development of an app for contact tracing during Covid-19, called “Karantinas”. NVSC (the Lithuanian Public Health Authority) commissioned the app from a developer (ITSS), but then withdrew before a contract was concluded. The app was developed and made available on app stores, and included links and references to NVSC.

The app was found to be infringing of EU GDPR (Arts 5, 13, 24, 32, 35).

Issue: was NVSC a joint controller as commissioning body, even though it withdrew from the project and had limited influence on processing activity?

Key findings:

- A controller needs actual influence over the purposes and means of the processing, not just formal involvement
- Joint controllership can exist without agreement or co-ordination, as long as influence over the “purposes and means” of processing is exercised jointly
- “Processing” includes the use of personal data during the test phase of an app, unless anonymised
- Fines can only be imposed for intentional/ negligent breach
- A controller can be fined for the actions of a processor acting on its behalf.

Will go back to national court for application to the facts. (Nacionalinis visuomenės sveikatos centras Case C-683/21).

SHOOSMITHS SAYS...

Public health authority washes its hands of “rogue” track and trace app.

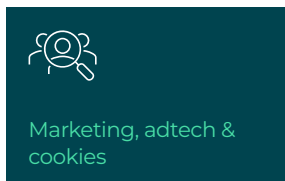
Findings about commissioner and controller responsibility are likely to be influential.

Links to further information

[AG’s opinion](#)

Enforcement & legal action

Jurisdiction: **US (Federal)**



US FCC announces first use of new blocking powers to stop scam calls

11 May 2023

Key details

The Federal Communications Commission (FCC) has used new powers to prevent phone calls which are routed through a “gateway provider” in the US from being communicated onwards by phone companies, since the provider regularly carries messages generated by scammers outside the US.

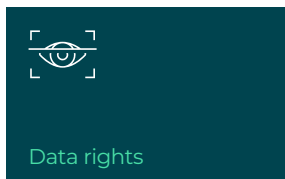
Ofcom is currently consulting on equivalent powers in the UK (see update from last week).

WHAT THEY SAY...

“a fair, transparent, but tough process by which we can essentially shut down access to U.S. communications networks”

Links to further information

[Press release](#)

Jurisdiction: **EU (Spain)**

AEPD publishes €75,000 fine for requiring photo ID as part of flat rental

10 May 2023

Key details

The Spanish data protection authority has imposed a fine of €75,000 on Marketing Accommodation Solutions FZ, L.L.C., for violation of Arts 5(1)(c) and 13 of the GDPR.

An individual complained that when staying at the property they were required to provide the e-mail addresses, phone numbers, and addresses, as well as photographs of each guest and both sides of their ID. There was no option to refuse this at check-in.

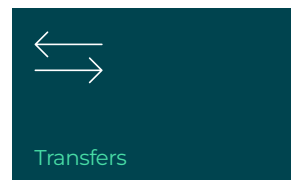
The AEPD found that the photo and ID data was not necessary for the purposes carried out (breach of minimisation principle) and adequate information about data collection was not sent to the individual making the reservation, so imposed the fine.

SHOOSMITHS SAYS...

[Check-in out.](#)

Links to further information

[AEPD decision](#)



EDPB publishes binding decision on Meta transfers case

22 May 2023

Key details

The decision arises from the various challenges since 2013 on whether Facebook (now Meta) can export the personal data of EEA data subjects to its US parent company in reliance on SCCs and associated risk assessments. As relevant supervisory authority, the DPC has had to take in to account the view of various other European supervisory authorities, and they have not reached consensus on various matters. The DPC referred these questions to the EDPB under the Art. 65 dispute resolution procedure, which has now published its binding decision.

The EDPB decision:

- Instructs the Irish Data Protection Commissioner (DPC) to impose a fine on Meta
- Outlines the factors which should affect the size of fine (gravity of infringement, scale of processing, number of data subjects, duration of infringement, scale of profits)
- Determines that the fine should be based on the consolidated turnover of the Meta group, and that the starting point should be 20-100% of the maximum
- Instructs the DPC to include an order to stop infringing processing (see below).

The EDPB decision was passed to the DPC last month, but it has only now been published, at the same time as the resulting DPC decision, also noted in this update. Meta can apply for annulment of the EDPB decision within 2 months (Recital 143, EU GDPR).

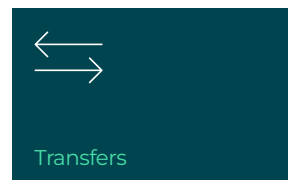
Links to further information

[Decision](#)

[Press release](#)

SHOOSMITHS SAYS...

[Full Meta Jacket.](#)

Jurisdiction: **EU (Ireland)**

DPC publishes findings of enquiry into Meta transfers from EEA to US and fines Meta €1.2bn

22 May 2023

Key details

Based on its own findings and the binding decision of the EDPB, The Irish DPC has issued a record fine and various orders to Meta Ireland in relation to transfers to the US.

Key points:

- This is largest fine imposed under EU GDPR to date (beats €746m Amazon fine in 2021)
- Use of SCCs plus risk assessment “did not address the risks to the fundamental rights and freedoms” of EU users
- Meta must cease the unlawful processing, including storage, in the US of personal data of EU/EEA users transferred in violation of the GDPR (i.e. delete or return data), within 6 months of the date of decision notification
- The “Suspension Order”: Meta must suspend any future transfer of personal data to the US by 6 months from the appeal/annulment expiry date, by reference to a timetabled implementation plan.

Other interesting findings (refs are to paras of ruling):

- 7.42 on the precedence of the EU Charter over the European Convention and Court of Human Rights
- 7.94 on the fundamental incompatibility of prevention purposes and human rights
- 7.141 nothing in recent US developments undermines CJEU analysis of US legal position in Schrems II
- 7.195 encryption may provide adequate safeguards (though it doesn't in this case)
- 9.51 this ruling would be trumped by a future adequacy decision
- 9.86 EDPB finds “the highest degree of negligence”
- 10.11 on applicability: “any internet platform falling within the definition of an electronic communications service provider subject to the FISA 702 PRISM programme may equally fall foul of the requirements of Chapter V GDPR and the EU Charter of Fundamental Rights regarding their transfers of personal data to the USA”.

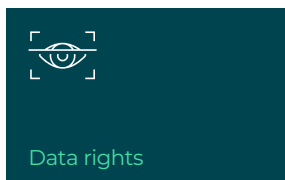
WHAT THEY SAY...

“the pertinent point is that Meta Ireland is not in a position to demonstrate that [...] no interference with EU rights occurs. Such interference does occur, and Meta Ireland does not have a remedy for it.”

Links to further information

[Decision](#)

[Press release](#)

Jurisdiction: **EU (France)**

CNIL fines health website over GDPR violations

11 May 2023

Key details

The French DPA has fined the company behind a health website €380,000. The website offers articles, tests, quizzes and discussion forums related to health and well-being for the general public. Follows a 2020 complaint by Privacy International (a UK privacy rights charity).

CNIL found the following infringements:

- Art. 5.1(e): storing data longer than necessary (two years, and in some case over three years after necessary processing)
- Art. 9: failure to obtain consent to the collection of sensitive health data
- Art. 26: failure to have legal agreement with joint controllers in relation to selling advertising space
- Art. 32: defective security measures (e.g. password protocol)
- Art. 82 French DPA: cookie violations (€100k of the fine).

The action involved the one-stop shop procedure as the website has visitors from all the member states. The company has since remedied all defaults.

Links to further information

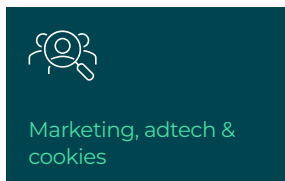
[Decision](#)[Press release](#)[Complaint](#)

SHOOSMITHS SAYS...

Recognising that a company has rights, too: the decision will no longer identify the company after 2 years.

Content is now hidden behind a cookie wall – more challenges ahead?

Jurisdiction: **UK**



ICO fines two companies for unsolicited marketing calls

16 May 2023

Key details

The ICO has issued fines to UK Direct Business Solutions Ltd (£100k, 410,369 calls) and Ice Telecommunications Ltd (£80k, 72,682 calls) for violation of Regulation 21 of the PECRs 2003. They both made unsolicited calls to companies which were signed up to the Corporate Telephone Preference Service.

Both fines follow significant numbers of complaints from targeted businesses, and findings that callers were on occasion “rude and aggressive”.

SHOOSMITHS SAYS...

Why the difference in fine?
Hard to say, though Ice is still infringing despite putting in place measures (hence the enforcement notice) where UKBS has apparently stopped.

Links to further information

[Press release](#)

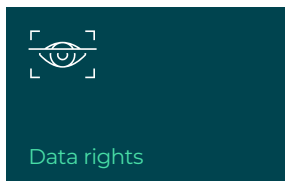
[UKBS penalty notice](#)

[Ice penalty notice](#)

[Ice enforcement notice](#)

Enforcement & legal action

Jurisdiction: **US (Washington State)**



AG announces \$39.9m settlement with Google over location tracking practices

18 May 2023

Key details

Google LLC has agreed to the fine in respect of alleged misleading location tracking practices contrary to the Consumer Protection Act.

Follows a 2020 lawsuit for deceptive and unfair practices in obtaining consent in relation to tracking users.

Practices included:

- Collecting location data and tracking users even when location tracking and location history was disabled
- Misleading descriptions
- Repeatedly asking users to consent to tracking, and
- Claiming certain products would not function unless location was enabled.

Google must also review their practices in areas such as consent, limits on data use and retention, disclosure and compliance requirements.

SHOOSMITHS SAYS...

Going it alone has paid off – other states mounted a collective action and got around half the payout per consumer.

Links to further information

[Press release](#)

[Consent decree](#)



CJEU dismisses Meta appeal challenging information requests in competition investigation

24 May 2023

Key details

Part of competition investigations into Facebook's data related practices in 2019, including Facebook Marketplace. The Commission has made various large-scale requests for information based on wide-ranging search terms under the competition enforcement regulation (1/2003), which Meta Ireland has challenged on various grounds with the Court of Justice (CJEU).

This is the first CJEU ruling on search term requests, and using data rooms for sensitive material.

Key findings:

- Commission requests are sufficiently clear and consistent: just because the investigation is wide-ranging does not mean the requests are too vague
- The use of very wide search terms in Commission requests which would reveal a lot of irrelevant material (e.g. "big question", "shut down") is justified
- Just because the material captures information about new Meta services and products does not mean the requests are unnecessary or too wide
- The potential infringement of Charter rights in the disclosure of sensitive personal information of Meta employees and third parties is overcome by use of a "Protected Documents" protocol which minimises data use
- Meta suggested some of the search terms itself so cannot now challenge their appropriateness.

Meta's refusal to comply with previous orders means they cannot now be permitted to derive benefit from their non-compliance.

Links to further information

Judgements [here](#) and [here](#)

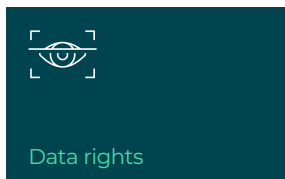
[Commission press release](#)

SHOOSMITHS SAYS...

Reaping the whirlwind.

As in the transfers ruling, Meta cannot put forward arguments based on the scale and architecture of its own service to counter legal challenges to the nature of the service.

...at least in the EU.

Jurisdiction: **EU (Spain)**

AEPD publishes fine imposed on Digi Spain Telecom €70,000 for processing without legal basis

23 May 2023

Key details

Digi Spain Telecom provides mobile, internet, broadband, TV and landlines, and has 3.8m mobile customers in Spain. It has been fined by the Spanish DPA for processing without a lawful basis contrary to Art. 6(1) GDPR.

Digi had provided a duplicate SIM card to a third party without consent, which allowed the third party to access the complainant's bank account and transfer money. The third party committed the fraud on the basis of name, telephone number, ID number and the last four digits of the subscriber's bank account, which complied with Digi's security requirements.

The AEPD found that Digi had not correctly ascertained the identity of the third party and therefore had no lawful basis for processing (as it was not necessary for the performance of a contract under Art. 6(1)(b)).

SHOOSMITHS SAYS...

Interesting use of Art. 6(1)
(lawful basis) to challenge
security failings.

Links to further information

[Decision](#)

Enforcement & legal action

Jurisdiction: **US (New York)**

AG agrees \$550,000 settlement with Practicefirst for data breach

23 May 2023

Key details

The New York AG has settled with three Practicefirst medical management companies in relation to violation of the Health Insurance Portability and Accountability Act 1996 (HIPAA).

An investigation found that Practicefirst's failures to install software patches and to encrypt led to a hack in December 2020, with 79k files being accessed and social security numbers, medical and financial information for over 1.2 million patients made available.

As well as paying the fine, Practicefirst must

- Maintain a comprehensive information security program
- Designate a Chief Information Security Officer
- Encrypt personal health information
- Process personal information only to the minimum extent necessary to accomplish the intended legitimate business purpose.

Links to further information

[Press release](#)

[Assurance of Discontinuance](#)

SHOOSMITHS SAYS...

Largely HIPAA-thetical: various class actions by affected claimants have been dismissed as this was a ransomware attack and there has been no actual harm yet.

But still expensive – Practicefirst paid the (undisclosed) ransom in 2021.



Sensitive data &
vulnerable individuals

ICO reprimands Ministry of Justice after bags of confidential information left unsecured at prison

27 April 2023

Key details

The ICO has issued the MOJ with a formal reprimand after it was discovered that due to a late pick up, confidential documents had been left for 18 days in an unsecured prison holding area, where both prisoners and staff had access to 14 bags of un-shredded documents containing NHS medical records and security vetting details. Information was taken by up to 44 people, including prisoners.

The ICO investigation revealed a lack of policies including:

- No pre-agreed areas for staff to leave confidential waste
- Staff being unaware of the need to shred information
- Inaccurate staff training records
- A general lack of staff understanding of the risks to personal data and the need to report data breaches.

The reprimand requires the MOJ to review all policies, procedures and guidance and create a data breach reporting policy as well as providing the ICO with a progress report by the end of October. Also recommends having an agreement between the prison and NHS Trust “to outline any established controllership responsibilities surrounding the handling and eventual destruction of Trust data”.

Links to further information

[Press release](#)

[Reprimand](#)

SHOOSMITHS SAYS...

Perhaps a case for more punitive sanctions?

“the risks to individuals in the prison would be significant and include potential identification within the prison or outside in the wider community. There would also be a significant risk of intimidation by other prisoners”



High Court strikes out class action for misuse of private information against Google and DeepMind

19 May 2023

Key details

The action (*Prismall v Google UK*) arises out of the transfer without disclosure or consent of identifiable information about 1.6m kidney patients to Google and DeepMind in order to create a “Streams” patient database for patient care.

The ICO investigated in 2017 and found breaches of the Data Protection Act 1998.

The claim is an action for misuse of private information; a similar action based on UK GDPR was discontinued following *Lloyd v Google*.

The class of 1.6 million claimants had to be judged on the basis of a “lowest common denominator” and since there were people in it who were affected only marginally by the transfer, the claim as a whole was bound to fail, and has been struck out. Will not prevent individual actions (or a more tailored class action) by affected patients.

SHOOSMITHS SAYS...

Failing to break through the class ceiling.

The English courts continue to mistrust class actions.

Links to further information

[Case report](#)



Industry & sector news

Jurisdiction: **EU (Italy)**



Garante authorises ChatGPT in Italy

28 April 2023

Key details

The Italian DPA has accepted the preliminary steps taken by OpenAI to comply with EU data protection law, and the service has been made available in Italy again.

Measures taken include more information, an opt-out to processing for algorithmic training which is open to anyone in Europe, and age-verification and blocking. ChatGPT says it can comply with deletion requests, but not rectification at present. Algorithmic training is done on the basis of legitimate interest.

WHAT THEY SAY...

The Garante “hopes that the company will continue along this path of adaptation to European data protection legislation”

Links to further information

[Press release](#)

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

IABEurope and other trade associations ask Commission to keep level playing field in draft Data Act

27 April 2023

Key details

The advertising industry body, together with other interested trade groups, has written an open letter to the European Commission and MEPs asking them to remove the ban in Art. 6(2)(b) of the draft EU Data Act. This stops “data recipients” (i.e. third party recipients authorised by users) from processing personal data generated by connected devices, which would effectively stop profiling based on this data. They say that if this processing activity is compliant with EU GDPR, it should be permitted, on the grounds of clarity, fairness and competition.

SHOOSMITHS SAYS...

Fearing another nail in the
profiling coffin.

**“will outlaw
longstanding and widely
accepted processing
activities in all industry
sectors”**

Links to further information

[Letter](#)[Data Act text \(draft\)](#)

Jurisdiction: **EU (Belgium)**



ODA sends questionnaires to DPOs as part of EDPB survey

24 April 2023

Key details

As part of the EDPB “coordinated action on DPOs”, questionnaires have been sent by the supervisory authority to all Belgian-registered Data Protection Officers on an anonymous basis, to encourage participation.

The questions include what tasks DPOs perform, how these are communicated, the work regime and reporting to management. Aggregated results will be published.

WHAT THEY SAY...

“The questionnaire will explore what tasks are entrusted to the DPO in his organisation”.

(We wonder if the survey is also doing any equality monitoring...)

Links to further information

[Press release](#)

Jurisdiction: **GLOBAL**



Apple and Google announce new specification to prevent unwanted Bluetooth tracking

2 May 2023

Key details

The new specification has been jointly developed to address problems raised by unauthorised tracking of mobile devices.

It will allow Bluetooth location-tracking devices to be compatible with unauthorized tracking detection and alerts across iOS and Android platforms. It will be a voluntary capability open to manufacturers to put into new products.

WHAT THEY SAY...

[Find My...](#)

“requires industrywide action to solve”

Links to further information

[Press release](#)

Jurisdiction: **AUSTRALIA**



Australian law firm victim of a Russian-linked ransomware attack

2 May 2023

Key details

Australian law firm HWL Ebsworth has apparently been attacked by a Russian-linked ransomware group called ALPHV/Blackcat. The group alleges that it hacked 4 terabytes of the firm's data, including employee CVs, IDs, financial reports, accounting data, client documentation, credit card information, and a complete network map.

The group operates "ransomware as a service" and has targeted 14 professional services firms in Australia since 2020. The attack was timed for 4.30pm on a Friday afternoon (28 April).

SHOOSMITHS SAYS...

"We're not your typical law firm". Perhaps not, but it's a typical attack.

Jurisdiction: [EEA \(Norway\)](#)



Norway DPA bans collection of grocery shopping data for government statistics

26 April 2023

Key details

Datatilsynet has banned the collection of anonymous statistics on banking and retail purchases by the Norwegian national statistics office which was otherwise authorised under national law.

Their reasoning was that:

- Citizens have no real way of objecting, other than paying by cash
- The practice risks undermining trust in government.

The ban follows several complaints about the practice from members of the public.

SHOOSMITHS SAYS...

[Norse Code.](#)

“there is a limit to what data public authorities can process about individuals, even where the purpose is good”

Links to further information

[Press release](#)

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

Jurisdiction: **JAPAN**

Toyota reveals that driver data of up to 2.15m may have been exposed

5 May 2023

Key details

Toyota has issued an apology to 2.15m “Connected services” customers in Japan whose information has been available openly on the cloud for a decade because settings were inadvertently made public rather than private. The T-connect, G-Link and G-Book services (which customers sign up to) draw information about vehicle location, vehicle ID and driving history from the car to enable entertainment, recovery and maintenance services. Reports say that the issue affects “almost the entire customer base [in Japan] who signed up for its main cloud service platforms since 2012”. Information includes email addresses, vehicle-unique chassis and navigation terminal numbers, timed location data, and videos from the “drive recorder”.

Toyota says it has corrected the settings and has set up a contact service for affected customers in Japan, but it is not known if any data has been exfiltrated for malicious purposes or if the company has contacted the PIPC (Japanese DPA) formally.

SHOOSMITHS SAYS...

Japan’s top car: Toyota sold 1.4m vehicles in Japan in 2021.

Japan’s top industry: automotive employs 5.5m countrywide.

Links to further information

[Press release](#)

Jurisdiction: **GLOBAL**



Google announces that Bard AI is available in 180 countries, but not including EU or Canada

10 May 2023

Key details

Google Bard is now available in 180 countries including the UK, but these do not include Canada or most EU countries. They have not explained why, but reports suggest this is concern about active GDPR enforcement along the lines of ChatGPT in Italy, and uncertainty about the new AI Act, which will be voted on by the European Parliament in June.

SHOOSMITHS SAYS...

All above Bard.

Question: Why is the UK deemed Bard-safe, when it is currently subject to equivalent data protection laws as Italy?

“part of Google’s plan to bake generative AI into everything”.

Links to further information

[Country list](#)

Jurisdiction: **UK**



Cyber Security Breaches Survey 2023 published

19 April 2023

Key details

The Departments for Science, Innovation and Technology and for Culture, Media and Sport have published the findings of their annual cyber breach survey.

Key findings over the last year:

- 32% of businesses recall breaches or attacks, of which about one third are classed as cybercrime
- Reviews of supply chain risks are up
- Fewer breaches and attacks were reported for smaller organisations – probably indicating lower vigilance in the face of other economic threats (e.g. inflation).

But:

- 32% of large businesses still don't have a formal cyber security strategy
- Most medium and small businesses don't have formal incident response plans.

Reporting of risks is still uncommon among all organisations.

SHOOSMITHS SAYS...

The difficulty of getting cyber vigilance to the top of the agenda...until it's too late.

Links to further information

[Surveys](#)

Jurisdiction: **FRANCE**

France's constitutional court backs use of AI surveillance cameras for Paris Olympics

17 May 2023

Key details

France's court has approved the use of AI-powered surveillance for the 2024 Olympics being held in Paris. It has also given guidelines for the implementation of the technology, which involves the use of large-scale, real-time camera systems supported by algorithms to spot suspicious behaviour.

Systems must:

- Not involve FRT
- Only deploy during events at high risk of becoming terror targets
- Ensure no biometric surveillance
- Not link data to other databases
- Make clear who is responsible, which events, why and for how long
- Ensure that individual decisions to use systems can be challenged in court.

The court held that these measures would not infringe on privacy rights as humans will permanently control “the development, implementation and possible evolution of algorithmic processing.”

The plan was passed in the French parliament by a large majority in April.

The technology is set to be in place until March 2025.

Links to further information

[Ruling](#)

SHOOSMITHS SAYS...

French rights put to the guillotine.

“an end to all forms of violence and incivility committed during sporting events”



**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: June 2023

©Shoosmiths LLP 2023

SHOOSMITHS

www.shoosmiths.com

**FOR
WHAT
MATTERS**