

Data Protection Top 10

May 2024

B

Bristows



Mark Watts
Partner

Is everything about to change?

With a UK general election at some point this year, a US election in November and European elections in June, a lot could change over the coming months. Obviously, in each case, it depends on who wins, but changes in the makeup of any government can significantly impact data protection. Will the EU-U.S. Data Privacy Framework be in safe hands if Trump wins? Or just orange hands? Also, over the last few years in Europe, we've had the Data Act, the Data Governance Act, the AI Act, a European Health Data Space and NIS2—an alphabet soup of new data-related laws (yet still no ePrivacy Act). Will this prolific legislative output continue? Or even increase, perhaps? And what of a prospective Labour Government? What are its plans? Is Sir Keir a 'believer' (in data protection)? A lot could change, and we may need to add a few more pages to next year's publication.

But for now, back to this year. Plenty has been going on. The European Data Protection Board continues to wage its war against Adtech and cookies, and the CJEU has got busy examining many of GDPR's finer—yet still important—points. New technology keeps throwing up new challenges, whether biometrics, automated decision-making or generative AI. We're never short of content for this publication, and as with previous years, we could easily have produced a top fifteen or even a top twenty.

As ever, there wasn't a lot of science applied to the order of the Top Ten, and we could have our arms twisted to reorder several of the articles. So, please read it with that in mind.

We hope you enjoy it.

The Bristows Data Protection Team

Contents...

- 1** **Who is making the (automated) decisions?**
Page 4
- 2** **The ICO refereeing biometric data**
Page 6
- 3** **“Your password is incorrect” – Network and Information Security, and Cyber Resilience, take 2 (NIS2 & CRA)**
Page 8
- 4** **Déjà Vu: Will the EU-US Data Privacy Framework suffer the same fate as Privacy Shield?**
Page 10
- 5** **A nudge in the dark**
Page 12
- 6** **A world beyond cookies...**
Page 14
- 7** **A busy CJEU**
Page 16
- 8** **Generative AI: DPAs ‘supervising’ Gen AI learning**
Page 18
- 9** **Online safety: Pushing the boundaries of the Data Protection Top Ten**
Page 20
- 10** **No such thing as a free lunch (or online service)**
Page 22

Image created using Adobe Stock Generative AI



Emma Macalister Hall
Senior Associate

Who is making the (automated) decisions?

In December last year, the CJEU handed down a landmark judgment in the case of Schufa (Case C634/21) regarding the interpretation of “automated individual decision-making” under Article 22 GDPR.

Specifically, the CJEU held that Schufa, a German credit reference agency, engages in ADM under Article 22 when it generates credit scores which a third-party lender then “draws strongly” on when deciding whether to lend to individuals. The CJEU also held that Article 22(1) should be interpreted as a prohibition in principle on using ADM, i.e. it does not have to be invoked by an individual.

The decision attracted significant attention because the CJEU’s interpretation of “decision-making” extended the scope of Article 22 to service providers generating a score or probability value. In Schufa, the lender (not the credit reference agency) decided whether to offer the individual a loan and on what terms. The CJEU held, however, that Schufa was subject to Article 22 because

the lender’s decision drew strongly on the credit score it generated. The Court held that the term “decision” could encompass “a number of acts which may affect the data subject in many ways”, including calculating a credit score.

In principle, the case means that a service provider whose automated processing services are drawn strongly upon by a third party to “establish, implement or terminate a contractual relationship” with an individual could be caught by Article 22. In Schufa, the CJEU held that the credit score played a “determining role” in the decision, noting that a low credit score would “in almost all cases” result in the bank rejecting a loan application (as happened to the individual who brought the case). Therefore, if a third



party relies heavily on other factors when making a decision about an individual, then the service provider's processing may not reach the threshold for ADM. It is hoped that data protection authorities will provide further guidance on what "draws strongly" means in practice in the context of Article 22.

Automated decision-making, particularly based on AI, is prevalent, most notably in sectors such as insurance, finance, recruitment, and healthcare, where automated scoring or evaluation metrics may be used. The Schufa decision will have significant implications for organisations using such technology. It underlines the importance of developing an AI governance framework to ensure compliance with the GDPR and the proposed AI Act – and illustrates that both service providers and their customers need to be aware of their legal obligations concerning ADM.

In the UK, the Data Protection and Digital Information Bill (currently being debated in Parliament) proposes to remove the general prohibition on ADM from Article 22 of the UK GDPR, such that the prohibition would only apply where special category personal data is processed. The Bill still requires controllers to implement safeguards for other uses of ADM. If the Bill is passed in its current form, Schufa may have even less impact in the UK. Although CJEU judgments handed down post-Brexit do not bind UK courts, the ICO has continued to refer to EU enforcement action and case law where relevant to its investigations or decisions.



Will Hewitt
Associate

The ICO refereeing biometric data

When you hear ‘biometric data’, you probably think of the facial recognition technology you use to unlock your smartphone.

But it’s much broader than that, covering many other technologies, many of which are already in widespread use. For example, your Saturday trip to watch the North London derby will involve biometric data at almost every stage: before buying the tickets, your banking app might verify your identity using your voice; when walking through Kings Cross on the way to the stadium facial recognition cameras will monitor public safety; once you reach the stadium, police surveillance vans will be scanning the crowd for known criminals; and during the match itself, sports scientists will be analysing players’ gaits to track performance and fatigue.

With so much interest in biometric technology, it’s no surprise that this has caught the eye of the ICO, which is seeking to referee this emerging league of technology.

The ICO lays down the rules of the game

The ICO published new guidance on processing biometric data in February of this year, which has, amongst other things, reinforced the distinction between biometric data and special category biometric data. This distinction, based on whether biometric data is used to uniquely identify an individual, may give some comfort to those processing biometric data for purposes other than identification since the requirement to have an Article 9 GDPR condition only applies when processing special category biometric data. Avoiding having to jump over the Article 9 hurdles makes running the compliance program much more straightforward.



Serco Leisure – The ICO flexes its muscles

Serco Leisure ended up in hotter water than the local swimming pool after an ICO employee's trip to a leisure centre ended up in an enforcement notice being issued against them. The ICO ordered it to stop using facial recognition and fingerprint scanning technologies to monitor employee attendance.

While no monetary penalty was issued, the ICO was critical of Serco Leisure's inability to justify why less intrusive alternatives, such as ID cards and fobs, would have been ineffective. Given that lawful bases other than consent require the controller to justify why the processing is *necessary*, it's crucial to consider whether any less intrusive alternatives might do the job just as well.

The ICO also showed Serco Leisure a red card for failing to offer data subjects an opt-out or providing an alternative for employees who raised privacy concerns – something deployment of biometric technologies often requires, particularly in an employment context, where there is generally a power imbalance.

This isn't a cameo regulatory intervention by the ICO either, having already fined Clearview AI more than £7.5m in 2022 for unlawful processing of biometric data for facial recognition purposes (although the fine has since been overturned, subject to a further appeal by the ICO).

With the development and uptake of biometric technologies likely to continue, we expect that this is an area that the ICO will be keeping a particularly close eye on over the next twelve months.



Marc Dautlich
Partner


“Your password is incorrect” – Network and Information Security, and Cyber Resilience, take 2 (NIS2 & CRA)

Remember the sketch where Steve Carrell explains to a colleague, “for my password, I’ve chosen the word ‘Incorrect’? That way, when I forget my password, it’s really great, my computer actually reminds me, ‘your password is...”

If only information security were so simple, especially when scaled up to a pan-European level. In 2024, businesses operating in the European Union face a new cyber legal framework shaped by two pivotal pieces of legislation: the NIS2 Directive and the Cyber Resilience Act (CRA). These regulations together represent a significant capacity-building exercise across the EU. They entail a significant collective investment in the EU’s response to escalating cyber threats and our increasing reliance on digital technologies. The UK plans a much more limited upgrade to NIS1, with an uncertain timetable for next steps given a looming general election.

NIS2 Directive: A new paradigm in cybersecurity

The NIS2 Directive will repeal and modernise the existing NIS Directive, expanding the scope of cybersecurity obligations across various sectors within the EU. It aims to establish a higher level of cybersecurity and resilience within organisations, and it will have a more profound impact on how businesses manage their digital infrastructure than NIS1.



One of the critical features of NIS2 is its broadened scope, meaning that it will encompass more industry sectors and a broader range of technology providers. Specifically, the Directive distinguishes between “essential” entities (examples include energy, banking and digital infrastructure) and “important” entities (examples include manufacturing and digital providers) that provide services in the EU. Both categories of entity are subject to obligations to ensure certain cybersecurity standards and meet reporting requirements, but the (extensive) supervisory measures and GDPR-level penalties that can be applied differ depending on which category an operator falls into. Large and medium-sized enterprises fall directly under NIS2’s scope, although small and micro-organisations are still not exempt if they fulfil specific criteria.

The Directive requires the establishment by competent EU authorities of a list of regulated entities by a deadline of April 17 2025. This registration process involves entities providing extensive information, including the sector under which the entity falls, contact details, and a list of their assigned IP addresses. The aim is to ensure EU member states can effectively identify and supervise the entities that fall within the scope of NIS2.

The reporting requirements for cybersecurity incidents under NIS2 have been extended. In addition to more granular reporting deadlines and more detailed reporting, regulated entities must now notify recipients of their services where the incident in question is likely to adversely affect the provision of those services.

An important feature of NIS2 is the focus on supply chain security. Organisations will now be legally required to address cybersecurity risks in their supply chains. This means that parties not subject to NIS2 because they do not meet the threshold requirements may now find themselves indirectly caught because they are suppliers in the supply chain of a regulated entity.

NIS2 also places greater emphasis on the accountability of management. This will require a more proactive approach from the leadership of an organisation, starting with conducting risk assessments and implementing risk mitigation plans, accompanied by mandatory training for management and employees. Personal liability also arises where the steps taken by an entity to implement enforcement measures ordered by a competent authority are deemed ineffective. In certain circumstances, CEOs and senior legal representatives may temporarily be suspended from managerial functions.

Cyber Resilience Act: Securing the digital product lifecycle

Complementing the NIS2 Directive, the CRA focuses on the security of digital products, including hardware and software, placed on the EU market. The CRA aims to ensure that such products meet specific cybersecurity standards before being marketed, thereby better-protecting consumers and businesses from cyber threats.

The CRA applies to all products connected to a network, directly or indirectly. It introduces EU-wide cybersecurity requirements for these products’ design, development, production, and market availability. Manufacturers must conduct mandatory security assessments, implement vulnerability-handling procedures, and provide necessary information to users. Products designated as critical are subject to more stringent obligations.

Image created using Adobe Stock Generative AI



Anna Ni Uiginn
Associate

Déjà Vu: Will the EU-US Data Privacy Framework suffer the same fate as privacy shield?

Those following developments in transatlantic data transfers breathed a huge sigh of relief on 10 July 2023 when, despite criticisms from some stakeholders, the European Commission adopted an ‘adequacy decision’ in favour of the EU-U.S. Data Privacy Framework. So, what is the DPF, and how does it address the ‘Schrems II’ challenges?

The DPF is a US Executive Order that enhances safeguards around United States signals intelligence activities. This order introduces binding safeguards limiting U.S. intelligence agencies’ access to data to help ensure their access is *necessary and proportionate* to national security needs.

The DPF also establishes an independent two-layer redress mechanism to resolve European complaints regarding the processing of their data for national security purposes and imposes clear obligations on U.S. companies participating in the framework to adhere to privacy principles.



Its commitment to “essential equivalence” rather than identical data protection measures provides what many consider to be a flexible approach. Also, it reflects the reality that the EU and the US have different approaches to data privacy, with the US relying more heavily on self-regulation as a compliance tool.

Despite many positives, a question mark remains over the resilience and longevity of the DPF. It was subject to criticism from stakeholders, such as the EDPB and the European Parliament, before its adoption, and these criticisms may resurface as its safeguards are tested in practice. The DPF’s ability to withstand scrutiny and challenge largely depends on its effectiveness in practice, particularly regarding (1) the limitations and safeguards against U.S. intelligence agencies’ access to data and (2) the efficacy of the new redress mechanism for Europeans.

Concerning the limitations and safeguards introduced to address the *Schrems II* finding that US intelligence agencies’ access must be “necessary and proportionate”, it’s possible to argue that proportionality is not being applied in a way equivalent to that under EU law. The DPF doesn’t attempt to define these terms, and some have contended that they have only been included to give the *impression* that the concerns of the CJEU in *Schrems II* have been fully addressed.

What has Max Schrems had to say about it? Only that he is likely to challenge the DPF. However, with the legal challenge process so protracted, even if the *Schrems III* wheels are already in motion, it will likely be some time before the CJEU hears any such challenge. As of April 2024, the DPF has 2,778 participants who can continue to rely on the DPF for their transfers to the US for now, and this number will likely continue to grow.

Image created using Adobe Stock Generative AI



Jamie Drucker
Of Counsel

A nudge in the dark

A screenshot of a web browser window with a dark blue background. The browser's address bar is empty. A white dialog box is centered on the screen, containing the text "Do you want to:" followed by two options. The first option is "Read this fantastic article" with a green checkmark icon. The second option is "Continue to ignore an important compliance topic?" with an empty checkbox icon.

Do you want to:

☒ Read this fantastic article

☐ Continue to ignore an important compliance topic?



The manipulation of online user choices through so-called ‘dark patterns’ has become a growing feature of online services and technology products. These design tricks (which are usually significantly more subtle than the choice opposite) are often embedded in websites and apps to influence users to make choices that benefit the service provider. For example, they may encourage a user (perhaps unwittingly) to sign up for additional product features and provide more information about themselves. Often, they are designed so users take the path of least resistance to access the service they want, such as the one requiring the fewest clicks, at the expense of reading legal terms or applying more privacy-friendly settings.

These “dark patterns”, or “nudge techniques”, as they’re also referred to, can have significant privacy implications. For example, they might be used to make it more difficult for a user to opt out of data collection, obscure privacy-friendly options, or encourage users to share more data than they might have intended. The concern is that this can undermine user choice, make processing less transparent, and make privacy-positive options less easy to recognise or understand.

In August 2023, the ICO and CMA issued a joint position paper highlighting their concerns and outlining the practices they consider potentially harmful. These dark arts include such weird and wonderful

concepts as “harmful nudges and sludge,” “confirm shaming,” “biased framing,” “bundled consent,” and “default settings.”

The paper aims to guide firms and designers in creating online interfaces that respect user choice and privacy through using design to empower user choice and control, testing and trialling design choices, and complying with data protection, consumer, and competition laws.

Perhaps the most high-profile element of this renewed regulatory scrutiny is the focus of the ICO over the last year on the use of “reject all” options in cookie pop-ups and banners. For many years, it had been standard practice for websites and apps to offer users the chance to “accept all” through one click in the pop-up but to have to go through a second or third layer of options if they wanted to reject all cookies. In many ways, this is a classic example of a nudge technique designed to improve the user consent conversion rate.

Unsurprisingly, the ICO has started taking action by writing to the UK’s top websites and requiring them to give equal prominence to “accept all” and “reject all” options, warning that enforcement action will follow if these changes are not implemented. Therefore, whilst allowing users to reject all may impact how much targeted advertising websites do, it is already becoming market standard in the UK to present these user choices on an equal footing.



Hannah Crowther
Partner

A world beyond cookies...

2024 might finally be the year we forget about cookies. Or rather, look beyond cookies to all other technologies that perform similar functions but under a less catchy moniker.

With the ePrivacy Regulation still missing in action, cookies and other tracking technologies continue to be regulated primarily by Article 5(3) of the ePrivacy Directive. Article 5(3) concerns storing information on a user's device and accessing any information already stored. In November last year, the EDPB released draft guidance on the technical scope of Article 5(3), causing shockwaves throughout the online ecosystem.

It has long been accepted that Article 5(3) applies much more broadly than just to cookies, encompassing similar technologies that perform reading or writing operations on a user's device. The EDPB, however, has decided it includes pretty much any operation on a device concerned with connectivity. Activities within the sights of the EDPB include ephemeral storage such as caching and RAM, sending an IP address, and even the 'storage' that takes place when a user completes a form prior to submission. Unless these activities are "strictly necessary" to provide the service "explicitly requested" by the user, they need GDPR-standard consent.

The draft guidance prompted a very significant furore, with 58 formal responses to the consultation. People have argued that the EDPB's interpretation will break the internet, disincentivise Privacy Enhancing Technologies, and make even contextual advertising subject to consent. There is also a parallel debate on whether the EDPB is overreaching by releasing guidance on ePrivacy at all and should stick to the GDPR.

As a general rule, EDPB guidance doesn't tend to change much as a result of the consultation phase. Given the strength of feeling on this one, however, hopefully, it will prove the exception, and the EDPB will have a bit of a rethink.

Meanwhile, on a similar theme, the ad tech industry continues to prepare for a world beyond third-party cookies as more browsers end support for them. Safari and Firefox now block third-party cookies by default. In January, Chrome began phasing out third-party cookies, starting at 1% (although in April, Google announced a delay until



Q1 2025, and it is still subject to addressing competition concerns). Not one to be left out, Microsoft Edge announced in March this year that it would begin experimenting with deprecating third-party cookies, continuing throughout 2024 (but with no firm timeline given).

All of this has prompted the ads ecosystem to think very hard about alternatives. Chrome has its Privacy Sandbox, and Microsoft has announced the Ad Selection API. More broadly,

though, we're seeing a greater emphasis on first-party identifiers, such as encouraging account sign-ins, federated identity solutions and online and offline data matching. Recent privacy-enhancing technologies such as 'trusted execution environments' have also created opportunities for parties to match and share information about users without necessarily disclosing personal data. Even if third-party cookies become a thing of the past, behavioural advertising seems here to stay.



Mac Macmillan
Of Counsel

A busy CJEU

It's been a busy year for the CJEU, with the court handing down a flurry of data protection decisions. Here's a whistlestop round-up...

In *RW v Österreichische Post AG* (C-154/21), the CJEU held that, as part of the right of access, individuals have the right to know not just the categories but also the specific identities of the recipients of their personal data. The decision means that individuals who submit an access request may ask for a list of the specific entities their personal data has been shared with – controllers must provide that information unless it is impossible to identify the recipients or the request is manifestly unfounded or excessive.

In *J.M. vs. Apulaistietosuoja- ja valtuutettu, Pankki S* (Case C-579/21), the question was whether the employees of the controller should be considered “recipients” of personal data for Article 15, such that the data subject had the right to know which employees had accessed his personal data. The Court held that employees acting on their employer’s authority (i.e., the controller) cannot be considered “recipients”. The Court did note, however, that ‘log data’ showing who had consulted the individual’s data may constitute the data subject’s personal data. However, whether to disclose such information would depend on balancing the rights of the requestor and the employees.

In *UZ v Bundesrepublik Deutschland* (Case C 60/22), the CJEU held that not all breaches of the GDPR will render the related processing unlawful (which would give rise to a right of erasure). In particular, failing to meet the obligation to enter into a joint controller agreement or maintain records does not mean that the related processing would be unlawful under GDPR. The Court also held that national courts do not require consent to process personal data. Instead, the appropriate lawful basis is Article 6(1)(e) GDPR: processing necessary for performing a task in the public interest or in exercising official authority vested in the controller.

In an unsurprising decision (*Gesamtverband Autoteile-Handel eV v Scania CV AB* C 319/22), the CJEU confirmed that a Vehicle Identification Number could be personal data where an operator “may reasonably have at their disposal the means enabling them to link a VIN to an identified or identifiable natural person”.

With its detailed discussion of the application of Article 6 to personalised advertising, the decision in *Meta Platforms Inc. v Bundeskartellamt* (C-252/21) is too extensive to summarise fully here. Its key impacts are the CJEU's restrictive interpretation of contractual necessity (processing "must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject") and its confirmation of the right of a national competition authority to make a finding about data protection compliance when looking at potential abuse of a dominant position, subject to cooperation with the appropriate DPAs.

In Case C-487/21, *F.F. v Österreichische Datenschutzbehörde*, the CJEU clarified that the right to "a copy" under GDPR Article 15(3) means an exact and complete reproduction of the subject's personal data, not just a summary or an overview. It may also be necessary to provide extracts from documents where the contextualisation of the personal data processed is necessary to ensure the data are intelligible.

In Case C 307/22, *FT v DW*, the CJEU overruled a national law provision allowing treatment providers to be reimbursed the costs of providing a copy of medical records to a patient as it undermined the effectiveness of the protection given by the GDPR's right of access. The Court emphasised the importance of ensuring the data provided was intelligible when dealing with medical records, which meant providing copies of extracts or even entire documents might be necessary. It also reiterated the principle that requests for access to data can't be rejected based on motive.

In Case C-683/21, the CJEU held that a party which commissions the development of a mobile IT application may be a controller even if it does not itself process data using the app or agree to the app being made publicly available, since it may still have participated in the determination of the means and purposes of processing to be carried out through the app.

In Case C-453/21, *X-FAB Dresden GmbH & Co. KG v FC*, the CJEU examined the scope of protection offered to Data Protection Officers. It held that a DPO could not be given tasks or duties which would result in him determining the objectives and methods of processing personal data, as this would undermine the DPO's independence when monitoring the controller's compliance with GDPR. This is consistent with previous guidance by the Article 29 Working Party.

Case C-300/21, *UI v Österreichische Post AG*, clarified that an individual must be able to demonstrate material or non-material damage caused by an infringement of GDPR to claim compensation for that infringement. Damage should be broadly interpreted so it does not have to meet a certain threshold of seriousness.

In Case C 807/21, *Deutsche Wohnen SE v Staatsanwaltschaft Berlin*, the CJEU held that under GDPR, it is not necessary to show that an infringement can be attributed to a natural person to impose an administrative fine on a legal person, notwithstanding any such requirement in national law. It further confirmed that to impose an administrative fine, it must be established that the controller's infringement was intentional or negligent.

In Case C 340/21, *VB v Natsionalna agentsia za prihodite*, the CJEU established that fear of misuse of personal data can constitute non-material damage under the GDPR. However, the national court should confirm that the fear can be regarded as well-founded. The Court also confirmed that an unauthorised disclosure to a third party does not necessarily mean the security measures adopted by the controller were inappropriate, and that this was a matter for national courts to assess.

Image created using Adobe Stock Generative AI



Elisa Lindemann
Associate

Generative AI: DPAs ‘supervising’ Gen AI learning

For anyone living under a rock for the past year, the use of generative AI tools has continued to spread like wildfire and shows no signs of slowing down.

As ever, new technologies raise new data privacy questions, but perhaps even more so when it comes to ‘large-language models’, such as ChatGPT, given the ‘internet-scale’ datasets used to train them. Data privacy regulators and legislators worldwide are scrambling to find answers, using different approaches and with different results.

The European Commission has established an “EU AI Office”, the European Data Protection Board launched a dedicated ChatGPT taskforce, and you may remember that the Italian *Garante*’s initial reaction to ChatGPT was to ban it, albeit temporarily. Closer to home, the UK government is trying to position itself as a leader in all things AI by taking a pro-innovation approach to AI regulation to “unleash the significant social and economic benefits of AI”.



Also, the Information Commissioner has taken a somewhat ‘techno-optimist’ approach in the UK, supporting the government’s vision. However, it’s also warning developers and deployers of AI tools to comply with data protection laws, updating its guidance, and acknowledging that more clarity is needed on specific issues. Earlier this year, it launched a consultation series on what it sees as the key generative AI questions: (1) determining the lawful basis for processing publicly available data to train models; (2) how to comply with the purpose limitation principle throughout the generative AI lifecycle; (3) the application of the accuracy principle to training data and outputs; and (4) data subject rights.

To date, the ICO has only shared its thoughts on the first three topics, and there are a few surprises, with the ICO mainly agreeing with the approach we’ve seen many developers of generative AI take. For example, it confirms that ‘legitimate interests’ is the most appropriate lawful basis for processing publicly available information to train models, as long as sufficient risk mitigations are in place. The ICO also acknowledges that the principle of data accuracy is not absolute and that the need for accurate outputs will depend on the purpose for which the model will be used.

One criticism of the draft guidance is the ICO’s oversimplification of how generative AI models are trained (do the diagrams remind anyone else of pizzas?). Another is that when conducting a legitimate interests assessment, the ICO expects developers of ‘base’ models to consult their crystal balls and anticipate every potential downstream third-party use, which will be very difficult, if not impossible, in some cases. Limiting the ‘legitimate interests’ basis to downstream uses of a model that the original developer can foresee risks stifling innovation and thwarting some of generative AI’s potential.

The eagerly anticipated fourth consultation will focus on data subject rights. Compliance with data subjects requests relating to training datasets can prove particularly challenging for developers, as training datasets are usually vast and unstructured, with identifiers often removed, making it extremely difficult to isolate the personal data of a particular data subject. Even if this were possible, re-training a model each time a developer has to comply with a data subject’s opt-out request would lead to disproportionate and prohibitive efforts and costs. It will be interesting to see how the ICO addresses this problem. But with so much regulatory scrutiny worldwide, perhaps another regulator will beat them to it.



Faye Harrison
Of Counsel

Online safety: Pushing the boundaries of the Data Protection Top Ten

Last October saw the introduction of the Online Safety Act, a landmark piece of legislation aimed at significantly improving internet safety and the UK's answer to the EU's Digital Services Act.

Last October saw the introduction of the Online Safety Act, a landmark piece of legislation aimed at significantly improving internet safety and the UK's answer to the EU's Digital Services Act.

Despite the UK government's bold claims that the OSA will make the UK 'the safest place in the world to be online', some might question the OSA's place in this year's data protection 'top 10'—it isn't even data protection legislation after all! Yet considering its remit, covering matters such as age assurance and protecting children online, there's clear overlap with data protection laws, including the ICO's Age Appropriate Design Code, and protecting a user's privacy is undoubtedly paramount to ensuring their safety online. Notably, the ICO and Ofcom issued a new joint statement on 1st May, which builds on their earlier joint

statement published in 2022. The statement confirms the regulators' commitment to protecting users online and sets out their plans to collaborate where data protection and online safety intersect, with the aim of ensuring consistency across both regimes.

Who is subject to the OSA?

The OSA places obligations on two key categories of online service providers: user-to-user services (including social media platforms, online gaming sites and video-sharing services) and search services (i.e. services incorporating a search engine). In recent years, many big players in these categories have borne the brunt of data protection regulators' investigation and enforcement activities. They may be less than delighted at the prospect of another regulatory regime alongside the EU's Digital Services Act.



Though it's UK legislation, the OSA also has an extraterritorial scope, covering services that have a significant number of UK users, services that are actively targeting the UK market, and services that are accessible from the UK, which present a 'material risk of significant harm' to UK users.

What are the OSA obligations?

Organisations caught by the OSA will have many new obligations to get to grips with. At its core, the OSA mandates a proactive approach to user online safety, focusing on preventing illegal content and, specifically, shielding children from broader forms of other harmful content. This is a far cry from the current legal regime, which only provides that service providers must promptly remove unlawful content once aware of it.

Service providers must conduct risk assessments, implement measures to counter illegal and harmful content, and employ effective age verification mechanisms to protect children from inappropriate material. However, it should be noted that these obligations will not enter into force until Ofcom, the OSA regulator, has published corresponding guidance and codes of practice. Ofcom is taking a phased approach to this task, with its first draft guidance and consultation relating to illegal harms issued towards the end of last year.

Looking ahead

Ofcom has published a roadmap of guidance, codes of conduct consultations, reports and other actions intended to support the implementation of the OSA, which runs until the end of 2026. Its latest consultation, relating to protecting children from online harms, was published on 8th May. By spring 2025, we can expect to see the first OSA obligations come into force, with Ofcom's OSA enforcement activity anticipated to commence later that year. Answers on a postcard for which organisations might be at the top of its hitlist, but with fining powers even greater than the ICO's, we could see Ofcom delivering some seriously hefty penalties over the next few years.

Until then, Ofcom will have to make do with flexing its muscles against video-sharing platforms only, as existing obligations are in place to protect users against harmful videos under Ofcom's 'VSP Framework'. In force since 2020, the OSA regime will ultimately absorb this framework.

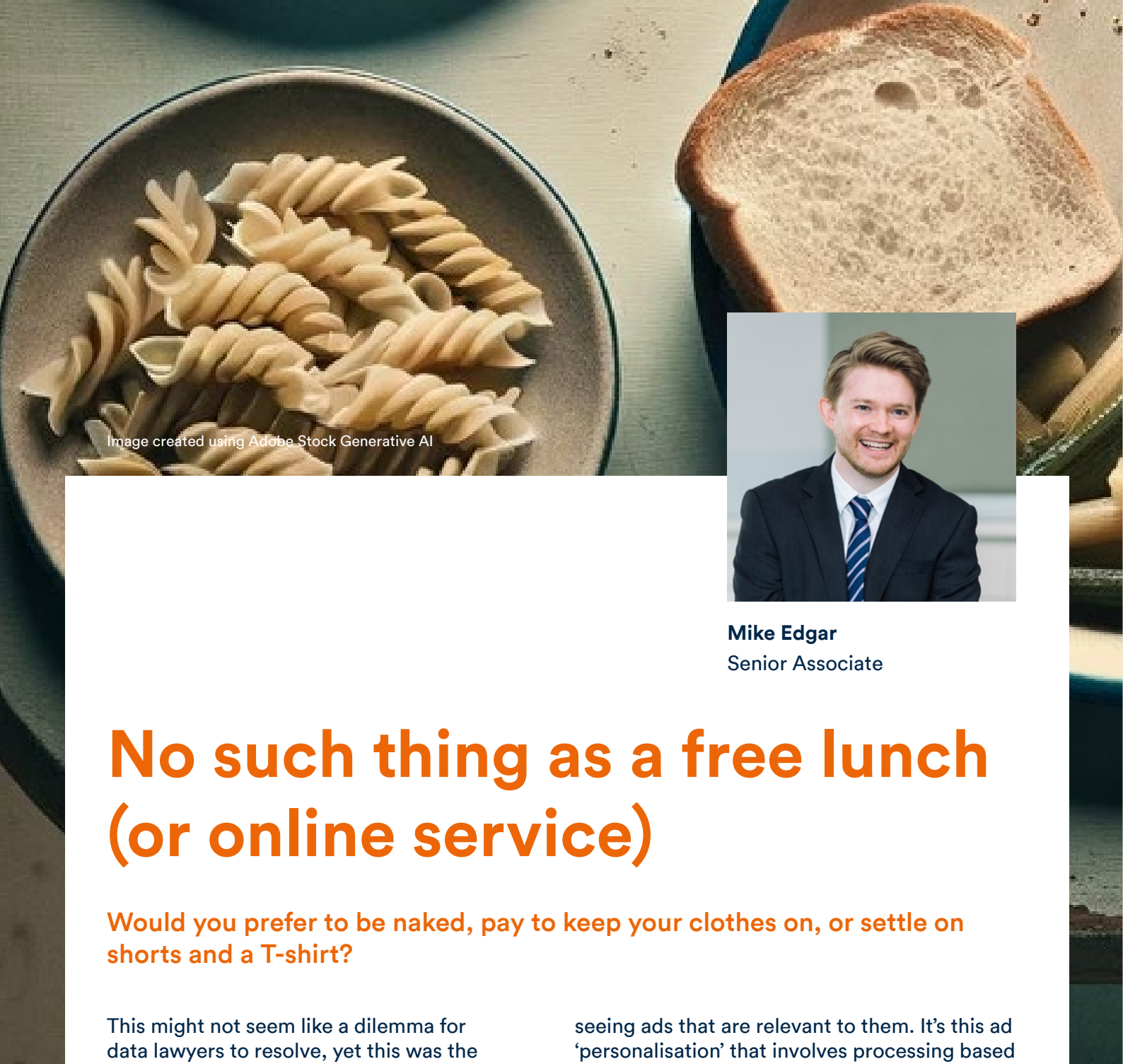
A background image featuring a bowl of fusilli pasta on the left and a slice of bread on the right. The pasta is in a dark bowl, and the bread is a thick slice of a light-colored loaf. The text "Image created using Adobe Stock Generative AI" is overlaid on the pasta.

Image created using Adobe Stock Generative AI



Mike Edgar
Senior Associate

No such thing as a free lunch (or online service)

Would you prefer to be naked, pay to keep your clothes on, or settle on shorts and a T-shirt?

This might not seem like a dilemma for data lawyers to resolve, yet this was the question posed by the chair of the EDPB, Ana Talus, at IAPP's annual Privacy Summit in Washington in April.

Ms Talus was referring to the paid subscription model Meta rolled out to EU users of Facebook and Instagram towards the end of last year. Under the new model, people in the EU, EEA and Switzerland can pay a monthly subscription to use Facebook and Instagram without seeing any ads (the so-called "fully clothed" option). Alternatively, they can continue using these services for free while

seeing ads that are relevant to them. It's this ad 'personalisation' that involves processing based on users' platform activity. We assume that what this activity may reveal is what's behind Ms Talus's reference to a user being "naked".

The move may have surprised some European users who have always been able to use Meta's products for free. However, the new model did not arise out of thin air. Instead, it is the latest in a long-running legal saga in the EU surrounding what GDPR legal basis data controllers can rely on for personalised advertising.



As we covered last year, historically, Meta has relied on the ‘contractual necessity’ basis for personalised advertising, which forms part of its services *“to provide [users] with personalised experiences across the Meta Products in accordance with [its] terms”*. As the Irish Data Protection Commission has previously accepted, this is the fundamental bargain between users and platform providers: free use of services in exchange for the platform earning revenue through serving (personalised) third-party ads. However, the EDPB disagreed and instructed the IDPC to issue hefty GDPR fines to Meta in December 2022 for inappropriate reliance on the contractual necessity legal basis and an order to bring its advertising processing into compliance.

Since then, we saw a rare instance of the Norwegian data protection authority using Article 66 GDPR’s urgent procedure mechanism to bypass the one-stop-shop mechanism and issue a 3-month ban on Meta personalising ads to Norwegian users of Facebook and Instagram based on the contractual necessity legal basis and the legitimate interests legal basis. Subsequently, at the EDPB’s instruction, the IDPC extended that ban to users across the entire EEA on 10 November 2023. This essentially left consent as the only legal basis for Meta to rely on for serving personalised ads to users in the EEA.

This brings us, not so neatly, to Meta rolling out its pay-or-consent model in the EEA. This move was followed by complaints being filed by opponents of the business model (such as by the Austrian data rights organisation, *noyb*), the Dutch, Norwegian and Hamburg data protection authorities referring the matter to the EDPB and, last but not least, by the European Commission announcing that it is also investigating the model under the EU’s landmark new competition law, the Digital Markets Act.

This brings us up to date because on 17th April 2024, the EDPB published its opinion on such ‘pay-or-consent’ models, and, perhaps unsurprisingly, it does not believe that valid consent can be obtained by such models, at least not by a large online platform, such as Meta. Essentially, the EDPB requires that for consent to personalised advertising to be valid, as well as offering a paid, ad-free equivalent service, it should also offer a free-of-charge, equivalent service. The EDPB points out that personal data is not a commodity to be traded in exchange for money. One point that the EDPB doesn’t make, though, which would be interesting to hear, is how a large platform can fund any ‘free’ online service. Imposing unrealistic requirements identified by the EDPB pushes online services towards paid subscription models, thereby reducing consumer choice.

Meet the data protection team

Victoria Baron

Associate
victoria.baron@bristows.com

Jo Baynes

PA
josephine.baynes@bristows.com

Jamie Cox

Associate
jamie.cox@bristows.com

Hannah Crowther

Partner
hannah.crowther@bristows.com

Marc Dautlich

Partner
marc.dautlich@bristows.com

Samantha Dodds

PA
samantha.dodds@bristows.com

Jamie Drucker

Of Counsel
jamie.drucker@bristows.com

Mike Edgar

Senior Associate
michael.edgar@bristows.com

Alice Esuola-Grant

Associate
alice.esuola@bristows.com

Sophie French

Associate
sophie.french@bristows.com

Faye Harrison

Of Counsel
faye.harrison@bristows.com

Laura Harwood

Senior Associate
laura.harwood@bristows.com

Charlie Hawes

Senior Associate
charlie.hawes@bristows.com

Will Hewitt

Associate
will.hewitt@bristows.com

Alex Keenlyside

Partner
alex.keenlyside@bristows.com

Rebecca Kirtley

Associate
rebecca.kirtley@bristows.com

Janna Lawrence

Associate
janna.lawrence@bristows.com

Sarah Jane Lewis

PA
sarahjane.lewis@bristows.com

Elisa Lindemann

Associate
elisa.lindemann@bristows.com

Emma Macalister Hall

Associate
emma.macalisterhall@bristows.com

Mac Macmillan

Of Counsel
mac.macmillan@bristows.com

Naina Mangrola

Associate
naina.mangrola@bristows.com

Christopher Millard

Senior Counsel
christopher.millard@bristows.com

Anna Ni Uiginn

Associate
anna.niuginn@bristows.com

Gemma O'Kane

PA
gemma.o'kane@bristows.com

Daniel Owen

Associate
daniel.owen@bristows.com

Rob Powell

Associate
rob.powell@bristows.com

Manuel Rey

Associate
manuel.rey@bristows.com

Becky Ross

PA
becky.ross@bristows.com

Kiran Sidhu

Associate
kiran.sidhu@bristows.com

Molly Sparks

PA
molly.sparks@bristows.com

Mark Watts

Partner
mark.watts@bristows.com

William White

Associate
william.white@bristows.com

Vivien Zhu

Associate
vivien.zhu@bristows.com



Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44 20 7400 8000

Bristows LLP
Avenue des Arts 56
1000 Bruxelles
Belgium
T +32 2 801 1391

Bristows (Ireland) LLP
18 - 20 Merrion St Upper
Dublin 2 D02 XH98
Ireland
T +353 1 270 7755

Bristows