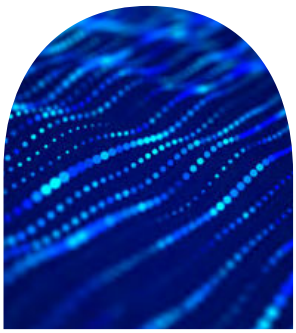
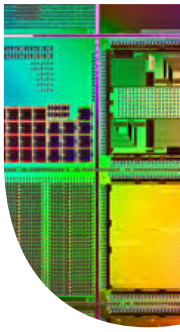


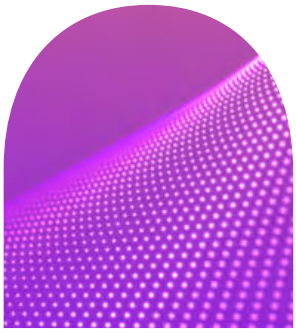
Bristows

# Data Protection Top 10

## A look to the future

May 2023





**Mark Watts**
Partner

# Welcome...

The temptation to get ChatGPT to write this was overwhelming. Here's what it came up with...

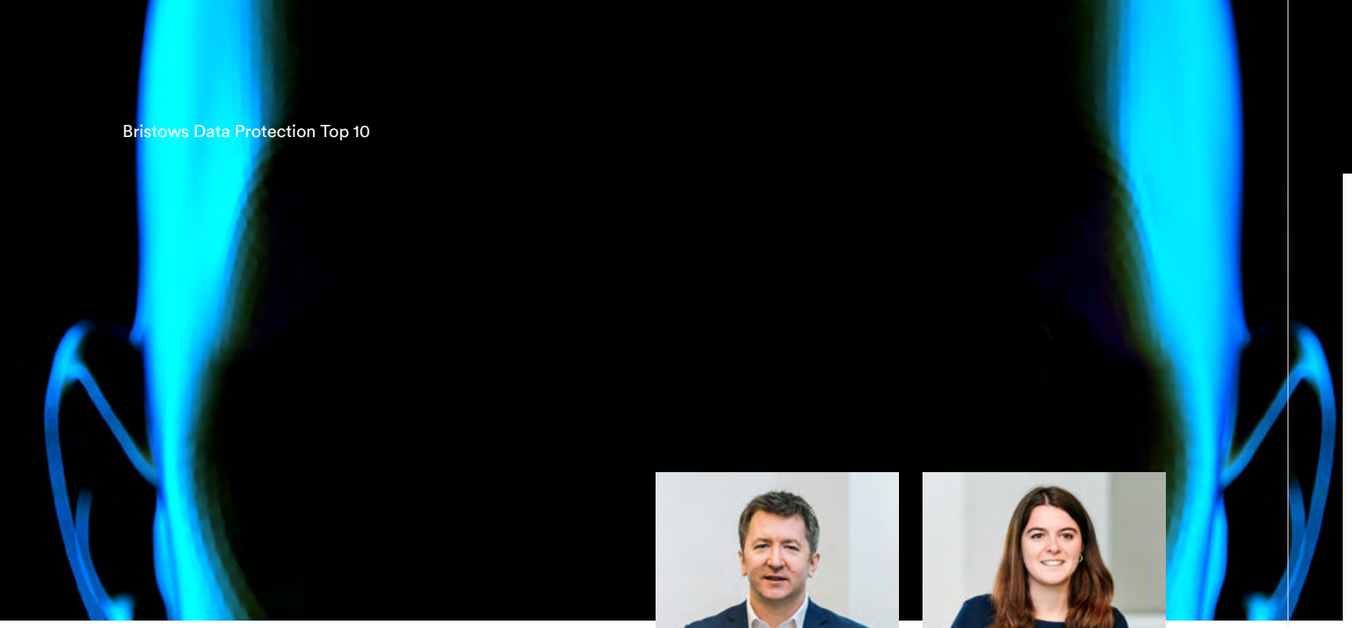
"Hello and welcome to our latest publication on the latest legal developments in data protection law! We'll be discussing all the newest regulations and guidelines in the ever-changing landscape of data protection law. Our aim is to provide you with all the information you need to ensure that your business is fully compliant with the latest data protection regulations and is keeping your customers' data safe and secure. We'll be breaking down complex legal jargon into easy-to-understand language, so you don't need to be a legal expert to understand what's going on. So, let's dive into the world of data protection law together!"

Not bad, eh?

What this doesn't get across, though, is the peculiar sense we felt putting this publication together that while there are lots of changes in law — a new UK Bill and a new US transfer mechanism — many of them aren't so new. Most of the new Bill is as we've seen before in one form or another, and most of the new US transfer mechanism is as we had under the US Privacy Shield. So, once again, it's technology that's providing the greatest data protection challenges. Even this time last year, who would have thought that generative AI would have progressed to the point where it can write a credible (if slightly bland...) introduction?

Anyway, as ChatGPT would say, let's dive into the world of data protection together!

## Contents...



# Generative AI's here – are *you* prepared?

**Now and again, there are tipping points in technology. Moments in time where a series of smaller incremental developments turn into something larger that catapults a technology into the public imagination and ushers in a phase of rapid innovation and change. 2023 may be that year for generative artificial intelligence (AI).**



**Charlie Hawes**
Senior Associate



**Cosima Lumley**
Associate

With the launch of OpenAI's ChatGPT in November last year, "generative AI" – machine learning software which, from simple prompts, can generate new content such as text, audio, images, and videos – has now truly broken through into the public consciousness. ChatGPT garnered over 100 million users in two months, making it the fastest-growing commercial product ever released. And the pace of innovation in the generative AI space shows no signs of slowing down as technology companies large and small are racing to get their generative AI products to market.

First, Microsoft announced its multi-billion investment in OpenAI. Then in February this year, it unveiled its new Bing search engine, which includes an AI chat function powered by ChatGPT. In March, Google announced the launch of its own AI chatbot, Bard. Microsoft and Google are also embedding generative AI functionality in their existing products and services. Microsoft has announced the GPT-4 powered Copilot for Microsoft 365, and Google has previewed AI-powered writing features for Google Workspace.



Bristows Data Protection Top 10

> **"Every once in a while a revolutionary product comes along that changes everything."**
>
> Steve Jobs

While these products are incredibly useful tools to enhance productivity and drive innovation, it is important to be aware of their limitations and the legal risks associated with their use.

Large Language Models (LLMs) such as ChatGPT and Bard work by predicting and generating statistically likely sequences of "tokens" (i.e. words, word fragments, characters or code) in response to specific prompts. They do not "understand" the content they generate, nor is this content guaranteed to be factually correct or, in the case of code, functionally accurate.

But because the success of dialogue-based LLMs comes in part from their ability to mimic human conversational speech, there is a risk of users and the general public anthropomorphising LLMs and ascribing to them human-like qualities of judgement and comprehension which they do not have. In a business context, where employees may be using products such as ChatGPT or Stable Diffusion, organisations should be aware of the risks which result from the information that is fed into the models (the inputs) and the information which the models generate (the output).

Given the volume of documents and other material that can be uploaded to these products, risks can arise in respect of confidential or privileged information; employees may be tempted to upload sensitive legal or commercial documents to these models (and so to a third party) to assist in analysing or summarising.

Additionally, generative AI models have a tendency to "hallucinate" where the model generates plausible but factually incorrect text or code. In relation to text-to-text models, reliance on factually incorrect content could lead employees to make misinformed decisions or disseminate misinformation. In relation to text-to-code models, reliance on code generated by AI without appropriate checks and testing could lead to security risks or affect the functionality of services.

Clearly, generative AI offers extraordinary opportunities, but implementing appropriate policies to regulate its use is going to be critical in mitigating the legal risks. Usage policies should clearly delineate the use cases for generative AI products and differentiate between uses which are purely internal and those which are external, particularly in regulated sectors. While the number of factors which need to be considered in drafting such policies are highly tailored to the specific sector and company, there are overarching principles which are universally applicable, such as ensuring that generative AI models are not being used in any form of automated decision making which has a significant impact on individuals, or to make any form of qualitative judgement, or process confidential or privileged information.

It is clear that it is a rapidly shifting landscape when it comes to the use and implementation of generative AI. We should all be prepared to be flexible and adapt to make the most of this. We see robust policies and risk management procedures as vital in ensuring that clients do not fall into the various potential pitfalls related to their use.

# Commotion at the One Stop Shop

**Mike Edgar**
Senior Associate

**Elisa Lindemann**
Associate

**The One Stop Shop (OSS) has been heating up in the past year: of the eight binding decisions issued by the European Data Protection Board (EDPB) since its inception, five were issued in the past 12 months. The big issue is "scope creep", as concerned supervisory authorities (CSAs) have not only raised objections to the lead supervisory authority's (LSA) assessment on potential infringements but have added new infringements of their own.**

The result has been significantly larger fines and concerns about due process as no further investigation is conducted into any such additional infringements, and there are question marks over how EDPB decisions can be appealed by organisations.

Of particular interest, WhatsApp Ireland's appeal against the Irish Data Protection Commission's (DPC) final decision in August 2021 raised questions about an organisation's right to an effective remedy and to a fair trial under Article 47 of the Charter of Fundamental Rights of the European Union. The usual principle is that an organisation can appeal an EDPB decision to the EU's General Court where it is of "*direct and individual concern to them*". One might have thought that the EDPB's instruction to the Irish DPC to fine WhatsApp a (substantially) larger amount, including for additional infringements, would be of direct and individual concern to WhatsApp.



Bristows Data Protection Top 10

However, in December 2022, the General Court held otherwise due to the nuance that the DPC had discretion on how to implement the EDPB's binding decision, for example, in setting the precise amount of the fine. Accordingly, WhatsApp's application to the General Court was inadmissible, and it had to rely on appealing through the national (Irish) courts. Another notable factor was the General Court's concern about parallel proceedings being brought in the EU courts; that is, an appeal of an LSA's final decision being referred by the national courts to the CJEU, as well as proceedings being brought for annulment of the EDPB decision in the General Court. WhatsApp is currently appealing this Order to the CJEU, so we'll see what they make of this concern.

Another skirmish to watch out for in 2023 follows the Irish DPC's applications to the General Court to annul the EDPB's instructions to conduct fresh investigations into Facebook, Instagram and WhatsApp's processing operations. The EDPB issued the instructions as part of its Binding Decisions 4/2022 and 5/2022, with the DPC responding via a post on its website that it considered such instructions to be problematic in jurisdictional terms and inconsistent with the structure of the cooperation and consistency mechanisms laid down in the GDPR (ouch!). The DPC formally issued its applications to annul in February this year, and the cases are pending. Has the EDPB overreached its authority? Stay tuned for what happens next.

What with massive fines, new infringements being added at the last minute, a lack of a direct appeal process – and the ever-present possibility of a finding of "joint control" with a US parent enabling other Data Protection Authorities (DPA) to simply bypass it altogether – is the OSS all it's cracked up to be?

**Emma Macalister Hall**
Associate

**Jamie Cox**
Associate

# Bridging the data transfer quagmire?

**As weary transfer watchers will be aware, the EU-US Data Privacy Framework (DPF) is currently winding its way through the EU's adequacy process. The proposed successor to Privacy Shield (invalidated by the CJEU in *Schrems II*), the DPF will, if adopted, enable the free transfer of EU personal data to participating organisations in the US – a welcome alternative to implementing Standard Contractual Clauses (SCCs) and conducting lengthy Transfer Impact Assessments (TIAs).**

For those who zoned out of the various opinions and orders, after political agreement was reached in March last year, President Biden issued an Executive Order on 7 October, outlining the safeguards and independent redress mechanisms the US Government would implement to address the concerns raised by the CJEU in *Schrems II*. The Commission then produced a draft adequacy decision, which now needs to be approved by Member State representatives before the final decision can be formally adopted. The European Parliament and EDPB have also thrown in their (non-binding) two cents, and while a committee of MEPs urged the Commission not to adopt the adequacy decision, the EDPB was (somewhat surprisingly) more positive, recognising that substantial improvements had been made. With opinions and criticisms still swirling, the timeline for adoption of the DPF remains unclear.

So where does all of this leave us? Could the EU-US transfer saga finally be drawing to a close? We wouldn't bet on it.

Although the Executive Order addressed some of the issues raised in *Schrems II*, the DPF remains vulnerable to challenge. The European Parliament's opinion doesn't bode well for future legal battles and, unsurprisingly, Mr Schrems has already levelled criticism at the DPF. The transparency of the Data Protection Review Court, established as an independent redress mechanism by the US Government, has come under particular fire because its rulings will be classified.



Bristows Data Prote… Top 10

Despite the challenges, the optimists amongst us still expect the DPF will be adopted later this year. As to the precise timing, the Commission may decide to wait until the US intelligence agencies have updated their procedures in line with the Executive Order (as recommended by the EDPB), in which case it will delay adoption until at least October 2023. The current expectation is that existing Privacy Shield participants will be able to re-certify to the DPF, as the principles to which organisations must self-certify remain largely the same (with some minor tweaks).

The Executive Order also offers good news for EU-US transfers beyond participants in the DPF. The safeguards set out in the Order, and the Commission's draft assessment of US laws and practices, are not limited to personal data transferred using the DPF. They can be relied on too when assessing the risks of transferring data to the US under the SCCs or Binding Corporate Rules (BCRs), so should help with those pesky TIAs.

Meanwhile, the UK and the US affirmed in January this year their intention to agree a "data bridge" (the UK's equivalent to adequacy decisions) between the UK and the US. Whilst this UK-US data bridge would be safe from any direct consequences of an invalidity declaration to the DPF, the UK will need to tread carefully to ensure that a UK-US data bridge does not end up jeopardising the UK's own adequacy decision with the EU.

While there's reason to be cautiously optimistic for the DPF and UK-US data bridge, the prospect of a *Schrems III* challenge still looms large, and we expect the saga of US transfers still has some way to go before its conclusion.

# The bare (contractual) necessities

**Last time you used a social media platform, how did you feel about all the personalised ads that were about to head your way? What if you'd seen random ads instead? Or even had to pay a subscription fee? What was your understanding of the "bargain"?**

**Mac Macmillan**
Of Counsel

**Sophie French**
Associate

It is GDPR 101 that processing personal data needs to have a legal basis. Recent decisions concerning processing by Instagram and Facebook have highlighted disagreements amongst the EU data protection authorities regarding the interpretation of one particular lawful basis – contractual necessity – and the role advertising plays.

The EDPB has always insisted on a narrow interpretation of contractual necessity; the processing needs to be objectively necessary for performing the "core" functions of the contract. A function is core when the service cannot be provided without the specific processing, and there must be no "less intrusive" alternatives to the processing. The EDPB's view is that this is unlikely for personalised advertising. It considers, for example, that users sign up to social media to "*share content and communicate with others, not to receive personalised advertisements*".





This is a frustratingly unrealistic approach if you are one of the many businesses operating in an online ecosystem largely financed by advertising. Meta, as one of the most high-profile operators, is providing the test cases for whether the EDPB's interpretation is correct. Meta presents its personalised advertising as forming part of its services "*to help you discover content, products and services...*". Even if you don't see this as part of the service, Meta's platforms are funded by personalised advertising. Users know this. Is it not then reasonable to argue that processing to deliver that advertising is a core part of the contract, just as a traditional financial payment is? Structuring the contract this way is an exercise of the freedom to conduct a business, recognised in the EU Charter of Fundamental Rights, though this right must, of course, be balanced against other fundamental rights, including those relating to data protection.

This approach had some success with the Irish DPC, the lead regulator for both Facebook and Instagram under the GDPR's One Stop Shop. The DPC's draft decisions held that the provision of behavioural advertising could be considered necessary "*in so far as this forms a core part of the service offered to and accepted by users*". However, in binding determinations issued by the EDPB under Article 65's "dispute resolution" procedure, the DPC was instructed to alter these decisions to find that contractual necessity could not be relied on for Meta's behavioural advertising. It is evident from the pointed manner in which the DPC pasted that instruction into its own decision that the dispute between the DPAs was not actually resolved, and the DPC remains unconvinced by the EDPB's "*strict threshold of 'impossibility'*" – that Art 6(1)(b) requires that it be impossible to perform the obligations under the contract without processing the personal data.

Meta Ireland intends to appeal. The courts will be faced with two diametrically opposed positions. Businesses will be hoping that a judgement gives some guidance on where the boundary lies between them. Until such an appeal is determined, the EDPB's finding sends a strong message to organisations and regulators alike; its narrow approach should be considered the touchstone for assessments of contractual necessity.

# A year in review, by the numbers...

## 5 CJEU questions

As reported last year, the Belgian DPA found that IAB's Transparency & Consent Framework (TCF) (which is relied on by much of the adtech ecosystem) breached the GDPR on a number of grounds. Unsurprisingly, IAB appealed the decision, and in September 2022, the Belgian Court of Appeal issued an interim ruling in which it referred 5 substantive questions to the CJEU. The questions are focussed on IAB's role as a possible joint controller and on whether the consent "strings" transmitted through TCF constitute personal data.

## 60 million

### CNIL fines Criteo

French adtech firm Criteo is facing a fine of **€60m** from the CNIL following a complaint alleging various breaches of GDPR principles relating to targeted advertising. The final decision is expected later in 2023. This follows the CNIL's decisions last year to fine Facebook and Google over cookie consent breaches (in particular for not having a "reject all" button).

## 1 First CCPA adtech fine

Leading US retailer Sephora became the unfortunate subject of the first fine issued under the CCPA, taking the form of a **$1.2 million settlement**. The Attorney General of California alleged that Sephora failed to disclose to website visitors that their personal information would be sold and failed to provide opt-out functionality. Given the somewhat ominous warning the AG issued to non-compliant businesses in a press release ("*My office is watching, and we will hold you accountable*."), more enforcement action is likely to follow.

## 51 million

### Number of UK individuals whose data is processed by Experian Marketing Services

The ICO and Experian took their arguments over Experian's use of data in its direct marketing services business up to the First Tier Tribunal. The FTT found that, while Experian Marketing Services processed the personal data of around 51 million people in the UK, it could generally do so without "actively" providing privacy notices and in reliance on "legitimate interests". The FTT emphasised the importance of proportionality in data protection enforcement, taking into account the outcomes for data subjects and the costs of compliance for the data controller. This was a significant defeat for the ICO, and so a further appeal is very possible!





## 390 million

### Irish DPC fines Meta

The Irish DPC fined Meta a total of **€390 million** this year for GDPR breaches across Facebook and Instagram. The DPC's key initial finding — that Meta was entitled to rely on contractual necessity as a basis for processing data for personalised advertising — did not survive the One Stop Shop process. The EDPB rejected the DPC's conclusion, finding that processing personal data for personalised advertising was not necessary for Meta's performance of its contracts with users.

## 45 million

### Digital Markets Act — implications for online advertising

Providers of "core platform services" will soon need to notify the EU Commission if their platforms are significant enough to make them a "gatekeeper". The EU Digital Markets Act, which came into force in 2022, takes aim at internet platform providers who turn over at least **€7.5 billion** in the EU and can consistently claim at least **45 million** monthly EU users. The few firms unlucky enough to be designated gatekeepers will face new restrictions on their use of personal data for targeted advertising and will have to provide third-party advertisers and publishers with detailed and transparent ad metrics. Time will tell whether the Commission will find cause to exercise its new fining powers of up to 10% of worldwide revenue.

**Jamie Drucker**
Senior Associate

**William White**
Associate

## 700

### Number of cookie banner complaints issued by interest group *noyb*

Following a continued campaign this year, the total number of cookie banner complaints issued by interest group *noyb* now stands at over **700**. The Cookie Banner Taskforce, which was set up to deal with these complaints, published its report in January 2023, providing some clarity on how supervisory authorities may interpret ePrivacy and GDPR requirements as they apply to cookie banners. Whilst the report emphasises that each cookie banner must be assessed on its own merits, it is a useful indication of regulatory expectations on what must, and must not, be included.

## 3 Primary APIs in the Google Privacy Sandbox

Google's deprecation of third-party cookies and its long-anticipated replacement, the suite of products known as the Privacy Sandbox, was delayed again as further development and trials are carried out. The revised timeline has all Privacy Sandbox technologies (primarily the "Topics", "Protected Audience" and "Attribution Reporting" APIs) generally available by Q3 2023, with third-party cookies to be disabled a year later in 2024. This year also saw the UK Competition & Markets Authority conclude its competition investigation into the Privacy Sandbox when it accepted a set of binding commitments from Google. The commitments aim to ensure that Google does not use the new adtech architecture to restrict competition with its own ad business.

# Online safety for digital natives

**Ofcom research published in March showed that 87% of 3-4-year-olds are online. Sure, many of these kids are just watching non-stop Bluey (a cartoon dog, for the uninitiated), but with children accessing the internet from an ever younger age, their online safety is of increasing concern. In the EU and UK, new legislation, such as the Digital Services Act and the Online Safety Bill, has been introduced to help address the issue. At the same time, data protection regulators are taking significant action to protect children's privacy online.**

**Faye Harrison**
Senior Associate

**Manuel Rey**
Associate

After the UK ICO's Age Appropriate Design Code (AADC) became the first statutory children's privacy code to come into force in 2021, other countries have followed suit, including the introduction of the Irish DPC's "Fundamentals" and the recently enacted Californian Code, closely based on the AADC. The EDPB is also planning to publish guidelines on children's data as part of its work program for 2023-2024, which may result in further national authorities moving their focus to children's privacy.

The regulators have also started flexing their muscles in this space. Last year the Irish DPC imposed a €405m fine on Meta as a result of Instagram having public-by-default profile settings for under 18s and making contact information of underage business account users public. More recently, the ICO issued a £12.7m fine to TikTok for processing the data of children under 13 without appropriate parental consent and for transparency shortcomings. While these fines apply to data processing predating the AADC and Fundamentals, the principles underpinning these codes are reflected in the regulators' decision-making.



Bristows Data Protection Top 10

To assist organisations with AADC compliance, the ICO has issued new guidance, most recently draft guidance addressing when an online service may be considered "*likely to be accessed by children*" even if not necessarily being intended for use by children (and so still subject to the AADC). The guidance touches on the hot topic of age assurance, noting the need to ensure the effective age-gating of services not intended for use by minors. However, there remains a distinct lack of clear EU or UK guidance on what a compliant age assurance solution should look like in practice. The ICO has also published a set of "top tips" for game designers, providing an opportunity for the ICO to show off how up-to-date they are on the latest in Yoof Speak (we're just off to "Buff our age assurance").

Speaking of which, age assurance tools are developing rapidly, with services like Instagram testing measures such as "video selfie analysis" and "social vouching". Of course, age assurance tools can sometimes introduce additional privacy risks, particularly in the areas of data minimisation and proportionality, so a careful balance needs to be struck.

Looking ahead, as regulators continue to concentrate their efforts on protecting children's privacy, we will no doubt see plenty of further developments in this area in the coming year. The message is clear for providers of online services: children's privacy compliance must be treated as a key priority.

# The European health data space (race)

**The European Commission has declared its intentions to unleash the full potential of health data in Europe, while the UK has set its sights on strengthening its position as a global science and technology superpower. Only time will tell who will win this modern-day space race.**

**Fiona Campbell**
Senior Associate

**Will Hewitt**
Associate

On 3 May 2022, the European Commission launched its proposed regulation for a European Health Data Space (EHDS). This ambitious proposal includes: (1) facilitating easier movement of patients' electronic healthcare records (EHRs) between healthcare providers and between Member States, which will also enable patients to gain easier access to their data; and (2) regulating and facilitating the re-use of health data for research, policy-making and commercial purposes.

Part (2) has caused a particular stir in the life science sector. It introduces a permit scheme under which a healthcare provider, pharmaceutical or even an AI device manufacturer can make a data access request to a newly established regulatory authority. There will be some prohibited uses (marketing, tailoring insurance premiums), but importantly, commercial product development use is allowed.



Bristows Data Protection Top 10

One purported benefit of the new scheme is to facilitate a workaround for the perceived Article 9 GDPR "stifling" of re-use of health data, allowing the EU to compete on the international health research front. Additionally, SMEs and data-driven start-ups will now have access to the same datasets as larger players in the market, enabling fairer access and increased competition, hopefully leading to greater innovation.

On the flip side, those already holding rich datasets, including larger pharmaceutical companies and AI developers, may see their crown jewels shared out. There are also a number of issues concerning the interplay between provisions of the GDPR and the proposed EHDS Regulation, such as the overlapping roles of the current DPAs and the proposed new Digital Health Authorities, which will need to be ironed out.

Turning the Commission's dreams into a practical reality will also be challenging. Building the secure data hosting environment the Commission proposes will take a number of years, with cybersecurity risk a key consideration. There are then the logistics of establishing a new regulatory authority in each member state, along with an EU-wide oversight body.

Meanwhile, the UK, which will not have any involvement in the EHDS following Brexit, appears keen to go head to head for the title of the leading centre for scientific research. Use of data for research is at the forefront of its National Data Strategy, and a new proposed definition of "Scientific Research" in the current draft Data Protection and Digital Information Bill includes an explicit acknowledgement that scientific research can include commercial purposes.

The NHS has long provided access to certain large anonymised datasets gathered from NHS data. Organisations can also use non-anonymised datasets, either by consenting all patients involved (which can prove impossible in larger and/or historical datasets) or by making a research application to bypass the need for consent. However, the system for data access is confusing, with numerous overlapping bodies and processes, and can appear impenetrable to new players. The EHDS is proposed to be one straightforward, centralised system, which would provide research, health and commercial organisations with access to richer datasets and allow them to be used for far wider commercial purposes.

The Commission's legislative proposal to unleash the full potential of health data is certainly more ambitious than the UK's current processes and proposed new legislation, but is also much further from being achieved in practice. Only time will tell if the EU can achieve lift-off and overtake the UK in this modern day space race.

# Ding ding ding! It's competition (law) time!

**The best way to protect your personal data and enforce your data protection rights is through your friendly local data protection authority and, of course, the GDPR, right? Well, maybe not.**

**Hannah Crowther**
Partner

**Rebecca Kirtley**
Associate

Some of you might recall our discussion of *Lloyd v Google* in the last edition of this publication. In this landmark decision, the UK Supreme Court firmly rejected the argument that data subjects were entitled to damages for mere "*loss of control*", stopping many data protection claims in their tracks. Since then, claimant firms have been on the hunt for other options, particularly for group actions, and some think they may have found an answer in competition law.

In the UK, at least one attempt to use competition law to challenge data practices is already under way. A collective action claim brought against Meta, in which some of the key questions centre around how Facebook collects and uses its users' personal data, is currently in front of the Competition Appeals Tribunal.



Bristows Data Protection Top 10

It's not only claimants who are testing the intersection between data protection and competition law though. Some competition authorities have started dipping their toes in, too. The pioneer here has been Germany's *Bundeskartellamt*. In 2019, it conducted an extensive investigation into Facebook's data collection practices. The conclusion of that investigation has since been the subject of a long legal saga, in which the most recent twist has been an Opinion by AG Rantos where he concluded that a competition authority could take into account compatibility with the GDPR "*as an incidental question*". What does "*incidental*" mean here? Well, it's not entirely clear, but perhaps the CJEU will shed some light on this when it considers the case. In the meantime, the *Bundeskartellamt* hasn't been idle. At the beginning of this year, it announced a statement of objections to Google's data processing terms.

Legislators have also been keeping busy. The European Commission's Digital Markets Act (DMA) – competition law legislation aimed at certain large online platforms – will apply to large platforms that are designated as "gatekeepers" in 2024. Among the obligations it imposes are a number of requirements around the use, collection and sharing of personal data (as defined in the GDPR), but it will be enforced by the Commission rather than the DPAs.

So, what does this mean? You might find your competition colleagues are suddenly being a lot more friendly, trying to work out what this data protection malarkey is all about. But in legal terms, there is still a lot that remains to be seen about how competition law and data protection will interact and intersect over the years to come. The CJEU still needs to consider the *Bundeskartellamt's* Facebook investigation, and here in the UK, the Meta case has, so far, been far from smooth sailing with the Tribunal recently having some pretty choice things to say about the claim, as currently pleaded. What is clear, though, is that we're unlikely to be able to avoid competition law entirely in the years to come, particularly following the advent of the DMA.

# UK data protection reform: the sequel

## Marc & Anna discuss the UK's updated data protection reform proposal...

A new draft of the UK Data Protection Bill was introduced in March this year. I've been trying to find out more about how it will, it is promised, save the UK economy £4.7 billion over the next 10 years.

**It's difficult to find reliable information about this, as the web link to that promise is broken at the time of writing. [Ed: we checked this daily, over a period of two weeks during April 2023].**

I nearly misheard you there, talking about broken promises and the UK government. Is that the reason why so few have so far called out this figure as highly unlikely?

**More simply, the figure is hard to disprove. Suppose we say for now these reforms will save £47 per year – at least.**

They are described by the government as "common sense-led" reforms. That's making me wonder what all the other reforms are. The Bill keeps us keen with just 206 pages of common sense. Can you give us some highlights?

**You won't need to do any of the following: (i) complete a "record of processing" (also known as a "ROPA") any longer, unless you undertake processing activities that are likely to result in a "high risk" to the rights and freedoms of data subjects; (ii) get consent for cookies if you use them on your website only for statistical purposes; or (iii) comply with a subject access request that is "vexatious or excessive" (or you can decide to charge a fee for doing so).**

You don't need to comply with a subject access request now, if it is "manifestly unfounded or excessive", which sounds like a virtually identical test, and you can already choose to charge a fee now. I'm going to say nothing about cookies, except that the Department for Science, Innovation and Technology webpages refer repeatedly to "pops-up" (sic) which I think are the same thing as "pop-ups" but I'm not sure any longer.



Bristows Data Protection Top 10

**Marc Dautlich**
Partner

**Anna Ni Uiginn**
Associate

**Perhaps more importantly, if the website is also subject to EU GDPR/the ePrivacy Directive, it will be more practical for a business to collect cookie consents under the existing rules, rather than designing and operating two sets of cookie banners, one for their UK-only sites and one for their EU-facing sites.**

The fines, though, for failure to comply with the PECR rules (including the rules on nuisance calls and texts) are changing from £500,000 to 4% of global turnover or £17.5 million, whichever is greater.

**Yes.**

Tell me more about the rest of this "easier to understand" system of data protection, and exactly how it will be "easier to comply with and take advantage of the many opportunities of post-Brexit Britain"?

**Building on your verbatim quotation from the minister there, the Bill broadens the scope of activities which can be categorised as "scientific research" to cover "*any research that can be reasonably described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity*." The Bill does not, however, define "scientific research". So there is still a lack of clarity about the nature of the activities which would fall within its scope.**

Loads of such projects obviously involve the EU, but this would work for those that don't...

**Additionally, the Bill allows for general consent to processing for scientific research to be obtained from data subjects, removing the requirement to specifically outline the relevant scientific purpose.**

That reminds me about lawful bases. What are the new "pre-approved" processing activities where a legitimate interests assessment will no longer be necessary?

**The draft list of recognised legitimate interests is: processing for reasons of public interest, public security, detecting and preventing crime, and democratic engagement. There is, therefore, a relatively limited cohort of controllers to whom these interests will be applicable.**

In the time available, we can do justice only to so much of the Bill. On a scale of 1-10, what score are you giving this reform for its overall impact?

**2. Maybe 1...**



# Ready player GDPR

**The Metaverse, like many emerging consumer technologies, presents plenty of knotty challenges from a GDPR perspective. As well as collecting extensive information about the user (e.g. head and eye position tracking, vital signs, and facial expressions), extended reality devices also record information about their environment and the people around them.**



**Daniel Owen**
Associate



**Tarryn Smith**
Associate

It is these non-users who often present the biggest challenge. Does the user's partner need GDPR transparency information when they're recorded telling the user to take the headset off and join them in the real world for once? When they eventually lose patience and dump said user, do they have a right to erase the captured footage?

The Metaverse is the name given to a developing concept of an immersive digital world based around various extended reality (XR) technologies designed to enhance the way we interact over a network. Inspired by science fiction like Ernest Cline's *Ready Player One*, the goal is to create an online world which we experience through our senses as avatars rather than through a mouse click.

It's unlikely that this vision of the Metaverse can be delivered by one entity, and many commentators cite interoperability (i.e. the ability to move seamlessly between platforms operated by different providers) as a key success criterion. The most ambitious visions for the Metaverse see Web3 concepts, particularly decentralised ownership and control based on a blockchain, as the way to deliver interoperability.

Given the grand aims of the Metaverse to succeed or fundamentally change the internet, it presents an interesting test case for the technological neutrality of the GDPR. Can a regulation essentially designed around Web 2.0 adapt to an extended reality of senses and emotions? Does a responsibility model based on hefty global fines for large corporate entities work for a decentralised user-governed world?

At least the types of personal data used by XR technology to render a virtual world all fit neatly into the GDPR concept of personal data. Given recent broad interpretations of special category data, a Metaverse operator processing physical data such as how high your heart rate gets when exploring a virtual mall, better get familiar with Article 9 before they start making inferences.

Bystander data presents another test for the GDPR since XR devices don't only record information about the user but also about their environment and the people around them. It's perhaps unsurprising that this type of bystander question often gets referred to as a key difficulty in guidance, like the ICO's guidance on Video Surveillance and the EDPB's guidance on Virtual Voice Assistants. Again, this doesn't seem like a test that the GDPR can't respond to, but more an issue that a Metaverse operator will need to consider.

To borrow a gaming phrase, the boss battle for the GDPR in the Metaverse may come in determining the roles played by the various actors in an interoperable Metaverse. At its easiest, this involves working out who are the controllers and processors in a complicated web of privately-owned Metaverse platform hosts, device providers, content developers and users, all of whom will want to reduce the friction caused by legal notices and consent requests. At the more difficult end of the spectrum is assigning responsibility in a Metaverse that is owned by its users according to their ownership of blockchain linked assets, such as digital land or currency. The top-down model of controllers, processors and data subjects may need revisiting in a world without owners, although like cryptocurrencies before it, decentralised ownership may remain more of a fringe idea rather than a core tenet of the Metaverse.

So it looks like the GDPR is ready to pull on its technology-neutral VR headset, but it's up to us privacy lawyers to work out the practical steps that need to be taken. Perhaps the more fashionable (and functional…) technology trend of AI can help with that!

# Our team

**Rebecca Andersen**
Senior Associate
rebecca.andersen@bristows.com

**Victoria Baron**
Associate
victoria.baron@bristows.com

**Jo Baynes**
PA
josephine.baynes@bristows.com

**Fiona Campbell**
Senior Associate
fiona.campbell@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**
Senior Associate
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**
Senior Associate
faye.harrison@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

**Elisa Lindemann**
Associate
elisa.lindemann@bristows.com

**Cosima Lumley**
Associate
cosima.lumley@bristows.com

**Sarah Jane Lewis**
PA
sarahjane.lewis@bristows.com

**Emma Macalister Hall**
Associate
emma.macalisterhall@bristows.com

**Mac Macmillan**
Of Counsel
mac.macmillan@bristows.com

**Christopher Millard**
Of Counsel
mac.macmillian@bristows.com

**Anna Ni Uiginn**
Associate
anna.niuiginn@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

**Helen Rose**
Senior Associate
helen.rose@bristows.com

**Becky Ross**
PA
becky.ross@bristows.com

**Tarryn Smith**
Associate
tarryn.smith@bristows.com

**Molly Sparks**
PA
molly.sparks@bristows.com

**Mark Watts**
Partner
mark.watts@bristows.com

**William White**
Associate
william.white@bristows.com

**Bristows LLP**
100 Victoria Embankment
London EC4Y 0DH

T +44 20 7400 8000

Bristows Brussels
Avenue des Arts 56
1000 Bruxelles

T +32 2 808 7500

bristows.com

Bristows