

Data Protection Top 10

May 2025



Bristows



Mark Watts
Partner

Welcome to the Data Protection Top Ten!

This year, we're serving up a mix of data protection developments with a dash of mischief and a pinch of scepticism as we watch Trump ramp up calls for greater deregulation and 'freedom' from red tape to promote AI and growth. But at what cost to privacy and accountability? Will European governments listen? What about data protection authorities? How will they react to the formidable challenges to data protection presented by agentic AI—those unnervingly clever systems that don't just process data, but make decisions. What happens when your data is in the hands of a machine that thinks it knows best? The robots are coming, it seems, and a thrilling if slightly terrifying ride lies ahead.

Meanwhile, though not formally part of our Top Ten, we've also included a summary of the proposed changes to UK data protection law. It seems like there's always more for a data protection lawyer to do, doesn't it?

Happy reading!

Mark Watts

Contents...

10 **DSARvival guide: guidance for controllers from the courts**
Page 4

09 **Déjà vu: yet another busy year at the CJEU**
Page 6

08 **To determine your future, first understand your past: an update on transfers**
Page 8

07 **ICO enforcement & strategy: all (invisibility) cloak and no dagger?**
pg 10

06 **The sound of new regulatory mood music**
pg 12

05 **How do you solve a problem like special category data?**
pg 14

04 **The safest place in the (online) world?**
pg 16

03 **Consent or pay – alright for some?**
pg 18

02 **Fine and dandy?**
pg 20

01 **A(I)gents of change: agentic AI, generative AI and the regulators' response**
pg 22

The year in numbers
pg 25

Bonus article
Take two: UK data protection reform
pg 26

Meet our data protection team
pg 28



Kiran Sidhu
Associate

DSARvival guide: guidance for controllers from the courts

The right of access under Article 15 UK GDPR is a foundational right, yet data subject access requests (DSARs) can be legally challenging and time-consuming for controllers. Fortunately, two recent High Court decisions provide some practical guidance.

Ashley v HMRC concerned a DSAR submitted by businessman Mike Ashley to HMRC following its enquiry into his tax liability. The Court ultimately found that HMRC had taken an unduly restrictive approach in responding to Mr Ashley's DSAR and ordered HMRC to reconsider its response. Here are some of the key points:

- The Court held that HMRC failed to conduct a “reasonable and proportionate” search by limiting its search to the specific department that received the DSAR, rather than considering all locations where in-scope data was held by HMRC. Helpfully for controllers, the Court clarified that “proportionate” can encompass consideration of the practical difficulties beyond the search itself, such as the time to assess exemptions and make redactions.



- The Court rejected Mr Ashley's argument that *all* information associated with the enquiry was his personal data. However, it confirmed that information constitutes personal data if it relates to an individual by virtue of its purpose or effect, such as determining their tax liability. Therefore, HMRC's valuations of Mr Ashley's properties, which were relevant for assessing his tax liability, were deemed to be his personal data.
- Finally, the Court found HMRC had not adequately demonstrated how the information it had withheld under the tax exemption of the Data Protection Act 2018 was likely to significantly prejudice the assessment and collection of tax, as required for the exemption to apply.
- The Court found that Mr Cameron had acted in his capacity as a director of ACL when making and sharing the recordings. Therefore, he personally was not a controller of the personal data; ACL was the relevant controller.
- To determine whether ACL was required to disclose the recipients' names, the Court held that the CJEU's interpretation of Article 15(1)(c) GDPR in ***Austrian Post*** (C-154/21) was to be applied. Since Article 15 UK GDPR confers a data subject right (rather than a controller obligation) and identifying the 15 recipients was neither impossible nor manifestly excessive for ACL, the Court held disclosure was, in principle, warranted.
- However, the Court accepted ACL's reliance on the "mixed personal data" exemption to withhold the recipients' names. The Court emphasised that the controller is the "primary decision-maker" in assessing the reasonableness of disclosure and has a "wide margin of discretion" in evaluating the relevant factors. Of particular significance was the fact that Mr Harrison refused an offer to receive the recipients' names on the condition that he would not threaten or harass them.

The case of ***Harrison v Cameron & ACL*** arose from a nasty dispute between Mr Harrison and his gardener, Mr Cameron, who operated through his company, ACL. The case focused on whether a controller must disclose the names of the specific recipients of personal data or merely the categories of recipients in response to a DSAR.

The (somewhat colourful) facts were as follows: Mr Cameron had recorded phone calls in which Mr Harrison made threats of violence against him and his family. He subsequently shared the recordings with family, friends and ACL employees for advice. These recordings were further disseminated, which Mr Harrison believed led to missed business opportunities. He submitted DSARs to Mr Cameron and ACL, primarily to identify the direct recipients. The Court's decision?



Mac Macmillan
Of Counsel

Déjà vu: yet another busy year at the CJEU

The days when a data protection decision from the CJEU was an unusual event are long gone, and these days we've become accustomed to a steady stream of judgments. It's impossible to cover them all, but here's our selection.

Role of the DPA

Inevitably, some data subjects are unhappy with how a DPA handles (or doesn't) their complaint. In **TR v Land Hessen** (C-768/21), a data subject asked a national court to order the DPA to take action against a data controller. The CJEU has previously held that DPAs have discretion to determine what action is appropriate and reaffirmed this position. However, it went on to say that a DPA may not be required to use a corrective power "exceptionally and in the light of particular circumstances, provided that the situation in which the GDPR was infringed has already been made good", which may leave data subjects room to challenge inaction. In this case, the controller had notified the DPA of the data breach of its own volition, had taken disciplinary measures against the employee concerned and agreed to review its processes, so the situation had already been "made good".

Most controllers have pondered when a data subject request can be rejected as vexatious, so the publication of a decision about refusing to act on excessive requests caused a brief flurry of excitement. Sadly, **Austrian DP v FR** (C-416/23) related only to complaints submitted to a DPA. The same industrious individual had submitted 77 complaints concerning different controllers to the DPA within the space of 20 months. More unfortunately for the Austrian DPA, the Court found the DPA was not entitled to conclude that the complaints were excessive, unless there was an indication that the complaints were "not objectively justified by considerations relating to the data subject's GDPR rights", e.g. this might occur where an individual was seeking to disrupt the functioning of the DPA. The fact that the complaints were directed against different controllers could merely indicate a high number of failures.

DSARs

Given the increasing use of AI, one of the most useful decisions was **CK v Dun & Bradstreet Austria** (C-203/22). This decision focuses on the level of detail required from controllers when providing “meaningful information about the logic involved” in automated decision-making and how the right of access interacts with protecting IP rights. Helpfully, the Court held that providing actual mathematical formulae or a list of all the steps involved in the automated decision was not only unnecessary, but might actually be unhelpful, since these were unlikely to provide a “concise and intelligible explanation”.

Legitimate interests

The Dutch DPA has always interpreted legitimate interests narrowly, arguing they should only be interests enshrined in law. **Koninklijke Nederlandse Lawn Tennisbond** (C-621/22) considered whether a purely commercial interest could be regarded as a legitimate interest in the context of a sale of member data by the Royal Dutch Lawn Tennis Association to its commercial sponsors. The Court confirmed that it could, in theory, be a legitimate interest, but noted that the interest had to be lawful and the processing had to be strictly necessary for that interest. Judging by the Court’s comments about the failure to ask members first, and what members might reasonably have expected, it did not consider Article 6(1)(f) to be satisfied in this case.

Compensation

National courts continue to find compensation for non-material damage challenging. In **OL v Bulgarian Registration Agency** (C-200/23), the CJEU reaffirmed that a temporary loss of control of personal data through its publication online can suffice to cause non-material damage. The data subject does not have to clear a *de minimis* threshold, but the data subject must still demonstrate infringement, damage and a causal link between the two.

In **A v Consumer Rights Protection Centre** (C-507/23), the data subject claimed a court had underestimated the seriousness of the infringement of his rights when it awarded him

€100 compensation. The appeal court was unimpressed and asked the CJEU whether an obligation to apologise could be the sole form of compensation for non-material damage. The CJEU confirmed that an apology could suffice, provided that this would fully compensate the data subject for the damage they had suffered. It was not appropriate, however, to take into account the attitude of the controller when assessing the level of compensation, since the function was to compensate, not to punish the controller.

Rectification

In **Deldits** (C-247/23), a transgender refugee challenged the Hungarian asylum authority’s refusal to amend its register to reflect their transgender identity because they had not provided evidence of gender reassignment surgery. The Court noted that if the purpose of the register was to identify the data subject, the relevant data would be their lived gender, not the gender assigned at birth, particularly since the data subject had obtained refugee status in Hungary because they were transgender. Data subjects may be required to provide reasonable evidence to establish that data is inaccurate, but any such restriction must be in Member State law, not merely an administrative procedure, and must also be necessary and proportionate. The proposed requirement was merely administrative and undermined the rights to privacy and integrity.

Minimisation

Finally, in **Mousse v SNCF Connect** (C-394/23), the Court held that SNCF couldn’t justify requiring individuals to provide a title (e.g. Mr, Mrs, etc.) - and by extension a gender identity - for use in commercial communications based on contractual necessity or legitimate interests. In respect of the legitimate interests balancing test, the customer’s concern about discrimination based on gender identity prevailed. SNCF sought to argue that it needed the information to adapt night train services, which have carriages reserved for persons with the same gender identity. The Court pointed out that SNCF shouldn’t collect this information on all reservations if it is only relevant to certain services.



Marc Dautlich
Partner

To determine your future, first understand your past: an update on transfers

The field of international data transfers was relatively peaceful (can you imagine such a time!) until Edward Snowden's revelations in 2013 ignited a debate about mass surveillance by governments that will not go away. If the last few years are anything to go by, legal challenges to the mechanisms for transferring personal data to third countries are here to stay.

The past year has seen no change in this pattern. Here's a round-up of the most significant recent legal developments:

- **POTUS.** Of the long list of concerns for the protection of privacy rights following the re-election of President Trump, one serves to encapsulate the threat: the dismissal by Trump in January 2025 of three of the five members of the Privacy & Civil Liberties Oversight Board (PCLOB). Without its three Democrat members, the effect on the PCLOB, which is required by law to be bipartisan, is, in the words of the legal proceedings brought by two of the dismissed members:

“...to deny the Board a quorum, prevent Congress and the public from learning about how this Administration respects privacy and civil liberties, and starve Congress of the information it needs to legislate and to oversee the executive branch.”

The European Commission stated in April 2025 that it “is closely following the developments”, helpfully reminding everyone that it “has the power to propose suspension, amendment or repeal of the adequacy decision establishing the EU-US Data Privacy Framework (DPF) if it concludes that the required level of protection is no longer ensured.” It's worth adding that Noyb has repeatedly urged the Commission to take action regarding the Adequacy Decision, failing which Noyb threatens ‘Schrems III’ legal proceedings.

- **Uber.** In an indication of the reliance that can be placed on European Commission guidance (spoiler: not much) - in August 2024 the Dutch DPA fined Uber €290 million for GDPR data transfer violations during the period between invalidation of the EU-US Privacy Shield in 2020 and Uber's self-certification under the EU-US DPF in 2023. Uber had removed SCCs from its data sharing agreements between its EEA and US entities, relying on guidance in the Commission's Q&A that controller-controller SCCs were not appropriate when an importing entity's processing was already subject to GDPR.

- **TikTok.** On 2 May 2025, the DPC announced its decision to fine TikTok €530m for breaching GDPR data transfer restrictions. At the time of writing, we are still awaiting the written decision, but the DPC has been investigating allegations that some of TikTok's EU data may have been unlawfully accessible to teams in China since 2021. It is the second-largest fine ever issued by the DPC (after Meta's fine of €1.2 billion in 2023) and the third-largest in the EU, after the fine in Luxembourg against Amazon for €746 million.
- **Bindl.** In January 2025, the EU General Court concluded that the unauthorised transfer of Mr Bindl's data (his IP address) to Meta's US servers in 2022 through the ‘Sign in with Facebook’ feature which left Mr Bindl in a state of “some uncertainty as regards the processing of his personal data”, was “actual and certain” damage, worthy of €400 compensation. This has very unwelcome implications for potential data protection class actions in the EU (note that Mr Bindl is the founder of a litigation funding firm with a focus on EU data protection claims). At the time of writing, both Mr Bindl and the European Commission have appealed the decision to the CJEU.
- **EDPB Guidelines on Article 48 GDPR.** Less noticed but very interesting as an indication of the European DPAs' collective thinking about transfers, in December 2024 the EDPB published new guidelines on Article 48 of the GDPR, clarifying how EU-based organisations can lawfully respond to data transfer requests from foreign public authorities.

For now, companies are generally continuing to retain DPF certifications, but, as contingency planning, some are implementing EU SCCs that will come into effect only if the DPF is invalidated. The transfer turbulence looks set to continue.



Anna Ni Uiginn
Senior Associate

ICO enforcement & strategy: all (invisibility) cloak and no dagger?

Some have perceived the ICO's enforcement activity over the last year as overly lenient. However, does this simply reflect a different approach to regulation, one that focuses on engagement and empowering individuals through information to promote innovation?

With fines from European DPAs coming in thick and fast (see our 'Fine and dandy?' article on page 20), the ICO's enforcement activity has come under increased scrutiny. Over the last 12 months, the ICO has handed down, let's be honest, a modest number of penalty notices for GDPR breaches (4 in total), some of which have been viewed as too low to have the desired 'deterrent effect' a fine is meant to have.

Take, for example, the £3.06M fine issued against Advanced Computer Software Group for security failings which resulted in a ransomware attack on NHS systems, and the £750,000 fine issued against the Police Service of Northern Ireland (PSNI) for exposing the personal details of the entire workforce (a breach the ICO itself acknowledged brought tangible fear of threat to life). In both cases, the penalty figure initially proposed was significantly reduced - the ICO said the PSNI would have been fined £5.6 million had it not been a public body (you are just moving money around after all). Advanced Computer Software's penalty was reduced by almost 50%, demonstrating the ICO's willingness to negotiate where there are commitments from an organisation not to contest a penalty notice (thereby avoiding those pesky and expensive appeals processes which haven't always gone so well for the ICO).



Looking ahead to the next 12 months, however, we could see some significant enforcement activity. The ICO recently announced that it is investigating TikTok, Reddit, and Imgur and intends to focus on how social media and video sharing platforms process children's personal data. As part of its Children's Code Strategy for 2024-2025, the ICO emphasised that it would focus on issues such as default privacy and geolocation settings, recommender systems and age assurance. Additionally, as part of its online tracking strategy for 2025, the ICO has announced that it will expand its cookie sweep to cover the UK's top 1,000 most visited websites and start looking at apps and connected TVs (this is your 10 minute warning...).

Overall, it's fair to say that the ICO's strategy over the last 12 months has focused more on engagement and empowerment through information than large-scale enforcement. On a positive note, this has resulted in the publication of helpful guidance, including on anonymisation (who doesn't want to read 98 pages of guidance about this?) and the 'consent or pay' model.

While there is no denying that the ICO's enforcement figures look a little low compared to those of our European friends, the ICO is solidifying its identity as a regulator supporting economic growth. This much was made clear in a recent statement from the Commissioner:

"We could regulate in a way that makes businesses fearful and risk averse; however, we have chosen to take a regulatory approach that reduces friction and encourages businesses to invest and innovate."

The ICO's pro-growth approach to regulation seems to reflect the UK government's current focus and may be a response to transatlantic geopolitical tensions and concerns that administrative fines could disincentivise inward investment.



Simon McDougall
Senior Adviser

The sound of new regulatory mood music

A new regulatory mood is emerging across the US, UK and EU – and it's not what we've grown used to.

Since the banking crisis, legal and compliance teams have operated on the assumption that regulation only accumulates – GDPR, AI rules, online harms and ESG disclosures. But 2025 feels different. Across three of the world's biggest regulatory engines, there is growing political consensus that regulation has become a drag on innovation, growth and strategic resilience. This isn't a coordinated shift – the drivers differ – but the direction of travel is surprisingly consistent: fewer new rules, more scrutiny of existing ones, and a greater willingness to let the private sector move first.

In the US, Trump 2.0 has picked up where he left off

Since taking office, the administration has issued a stream of executive orders unwinding existing regulation and has instructed agencies to withdraw draft rules and freeze new initiatives. The philosophy is clear: if the federal government isn't explicitly required to regulate something, it shouldn't. For the tech sector, this means a halt to federal privacy law discussions, a return to voluntary frameworks for AI, and the weakening – even dissolution – of some regulators. Many of these moves will face legal challenges, and states may choose their own path, but at a federal level, the shift is real.



The UK's Labour government is deregulatory – just not in the way we're used to

In principle, Labour isn't opposed to regulation, but it is urgently focused on economic growth, increasingly framed as a 'growth at all costs' agenda. That priority now extends to regulators, who have been told to align with the government's investment and infrastructure plans, with interventions from the Chancellor and a newly appointed, on-message Chair at the CMA. Starmer's team has made clear that pro-growth regulatory reform – including in planning, infrastructure and digital markets – is a central policy tool, not an afterthought. A potential UK-US tech-focused economic deal, building on the recent, narrowly scoped trade deal, may also shape future regulatory policy.

The EU is reassessing its regulatory instincts in light of the Draghi Report

Delivered in 2024, the Draghi Report made a forceful case that Europe's lack of economic dynamism is partly self-inflicted. The response hasn't been a rollback – the AI Act and Digital Markets Act are still being implemented – but the tone has shifted. Even landmark frameworks like GDPR are expected to be reviewed.

That said, many national data protection authorities remain committed to robust enforcement and are perhaps out of step with the wider deregulatory mood. This could lead to divergence between member states in their approach to tech and innovation.

So, what should legal and compliance teams do now?

The task is no longer just interpreting what's prohibited; it's assessing what might now be permitted – and whether the organisation should act. That means revisiting risk appetites, updating policies and navigating ambiguity. Values, stakeholder expectations and reputation will increasingly fill the space left by retreating regulation.

This moment won't last forever, but those who adapt intelligently may be best placed when the cycle turns again.



Emma Macalister Hall
Senior Associate

How do you solve a problem like special category data?

Continuing the trend of recent years, the CJEU is marching towards an ever broader interpretation of special category data. Two decisions handed down by the Court over the past year have followed this pattern. And tricky questions remain about how special category data can be processed when training large language models (LLMs). The situation has led some to question whether special category data is becoming an intractable problem.

But first, a quick recap of the cases...

Lindenapotheker (C-21/23)

This case involved an online pharmacy that sold non-prescription but pharmacy-only medicines. Disagreeing with a (seemingly sensible) decision from the Advocate-General (AG), the CJEU held that data collected by the pharmacy to process online orders—such as customer name, delivery address, and the medicines ordered—*did* reveal data concerning an individual's health.

The Court considered this information indirectly revealed health data by establishing a link between a medicinal product known for specific therapeutic uses and an identified or identifiable individual. Significantly, no prescription was required, so the pharmacy couldn't confirm that the purchaser was the person who intended to take the medication. Nonetheless, the CJEU held it was sufficient if there was "a certain degree of probability", rather than absolute certainty, that the medicines were intended for the purchaser.

This broad interpretation has potentially significant implications. The AG noted that, on such reasoning, ordering a book online by a political figure could indicate the customer's political views and fall within the scope of Article 9 - some online shopping could now become a special category minefield...

Schrems (C-446/21)

It wouldn't be the Top 10 without a **Max Schrems v Meta** showdown - this time featuring a row about ads Schrems saw on his Facebook feed for products and events targeted at individuals who are homosexual. While Schrems had spoken about his sexual orientation at a public panel in 2019, he had not posted this data on his Facebook profile.

Perhaps unsurprisingly, the CJEU held that the fact that Schrems had made public statements about his sexual orientation did not permit Meta to process *other* data relating to his sexual orientation (which Meta had obtained off-Facebook using third-party websites and apps) to offer Schrems personalised advertising. In other words, the "manifestly made public" condition under Article 9(2)(e) was not available to Meta in this context.

An especially tricky issue

We can expect European DPAs to follow the CJEU's interpretation, which will have direct implications for those they regulate (and could be particularly relevant when assessing the categories of data impacted by a data breach). Although not bound by its judgments, the ICO still pays close attention to CJEU decisions and may follow this direction of travel.

The issue of what information constitutes special category data and how to establish an Article 9 condition is particularly 'live' for training LLMs. While the EDPB stated that its Opinion on AI models did not seek to analyse this issue, it did refer explicitly to the **Meta v Bundeskartellamt** CJEU decision - i.e. if a dataset contains sensitive and non-sensitive data which cannot be separated at the time of collection, the dataset should all be treated as special category data, and the "manifestly made public" exemption requires a clear, affirmative action from the individual to signal their intent. This gives a pretty strong indication of the EDPB's thinking on this subject. We can expect this especially tricky issue to become even more of a challenge in the year to come.




Faye Harrison
Of Counsel

The safest place in the (online) world?

It's been 18 months (or so) since the Online Safety Act (OSA) received royal assent, amidst claims from the UK government that it would make the country “the safest place in the world to be online”.

However, the process for bringing this new online safety regime into force (through the implementation of Ofcom's regulatory codes and guidance) is lengthy and complex, so it may be a while before we can assess the real impact on our digital lives.

That said, the progress made since we shoehorned online safety into our 2024 Top 10 is not something to be sniffed at. Ofcom has been working tirelessly to produce hundreds, if not thousands, of pages worth of consultation documents, with its first codes of practice and guidance (relating to illegal harms) being published in final form at the end of last year.



December 2024 saw the first OSA provisions in force, with obligations requiring in-scope service providers to complete illegal harms risk assessments and implement safety measures to mitigate the harms identified within a three-month window. This was promptly followed in January with finalised guidance on age assurance, part 5 (pornography services) and child access assessments, which kicked off another three-month period to have those assessments done and dusted.

In late April, Ofcom finalised its codes of practice and guidance addressing online harms affecting children, triggering requirements for providers to complete their children's risk assessments and take steps to implement the necessary children's safety measures by the end of July. Encouragingly, it's not just children who have been identified as requiring additional protections under the OSA. Among Ofcom's consultations issued in the last year was draft guidance aimed at creating a safer life online for women and girls, in recognition of the greater risks of harm that this demographic is exposed to.

And Ofcom's work doesn't end at producing codes and guidance. Over the last few months, it has firmly set out its position as a regulator that means business, launching milestone enforcement programs relating to: (i) age assurance requirements for pornography providers; (ii) monitoring of providers' compliance with the illegal content

duties; and (iii) CSAM on file sharing and storage services. While Ofcom's approach is to work collaboratively with online providers to help drive their OSA compliance, it has also consistently emphasised that it will not hesitate to take enforcement action where it identifies serious breaches.

On that note, Ofcom has not wasted any time in launching its first investigation under the OSA illegal harms provisions, which it announced in April, less than a month after the deadline passed for completing illegal harms risk assessments. This was followed swiftly by the announcement of investigations into two adult content providers in early May, regarding potential non-compliance with their OSA age assurance duties. Further, while we've not yet seen any OSA enforcement action as such, Ofcom has issued significant fines to TikTok and OnlyFans over the last year, both under the Video Sharing Platform (VSP) regime, which pre-dates (and is essentially absorbed into) the OSA. This may be a sign of things to come, as Ofcom's new powers continue to enter into force.

With Ofcom sending a strong message that it is taking its new duties and powers seriously, service providers who have not yet got their OSA ducks in a row should take note. And with that, there may be some hope that the UK will live up to the promise of becoming the safest place in the (online) world.



Jamie Drucker
Partner

Consent or pay – alright for some?

Regulatory scrutiny of adtech has shown no sign of slowing over the past year, with authorities across the UK and Europe maintaining a focus on online tracking.

In response, the industry continues to search for products and services that balance privacy with the need to ensure advertisers can reach the right audiences. Unsurprisingly, the very large online platforms face the greatest regulatory hurdles.

At the heart of the adtech compliance challenge is the requirement for valid consent. This is not new, but recent guidance may have significantly broadened the range of activities for which consent is now required. The EDPB's final guidance interpreting Article 5(3) of the ePrivacy Directive adopts a notably expansive approach, capturing technologies well beyond

cookies. Practices such as URL tracking, IP-based tracking, and device fingerprinting now fall clearly within its scope. As the industry develops alternatives to third-party cookies, regulators are making it clear that consent requirements will be difficult to sidestep.

Where required, consent must meet the GDPR standard: informed, specific, freely given and capable of being withdrawn. Meeting that standard across complex adtech ecosystems—typically involving multiple intermediaries and a range of tracking technologies—remains a major challenge.



Regulators have continued to press for compliance. In the UK, the ICO is working to bring the top 1,000 UK websites into compliance by writing to publishers and requiring consent notices to be improved. A key priority is ensuring users are presented with a balanced choice—most notably, ‘reject all’ is as prominent as ‘accept all’ in cookie banners.

Faced with the reality that these requirements often lead to lower consent rates (and therefore reduced ad revenue), many publishers have begun to adopt so-called ‘consent or pay’ models. These offer users a choice between agreeing to tracking technologies for personalised advertising or paying a fee for an ad-free experience. The regulatory view on these models, however, remains mixed.

In 2023, the EDPB concluded that for consent to be valid in this context, large platforms must offer not just a paid alternative, but a genuinely equivalent, free-of-charge service.

This year, the ICO published its own guidance following a public consultation. While some see it as more permissive, it similarly emphasises that consent must be ‘freely given’. Factors such as the existence of a power imbalance, the level of the fee, and the degree of equivalence between the free and paid services will all be relevant. In practice, the ICO’s position does not materially diverge from the EDPB’s, though it is more broadly framed, without singling out large platforms.

As a result, for smaller or mid-sized publishers, ‘consent or pay’ may offer a viable alternative to implementing more intrusive consent banners. Indeed, many ad-supported news websites have moved in this direction.

But challenges persist for very large platforms. In April 2025, the European Commission fined Meta €200 million under the Digital Markets Act (DMA). The Commission found that Meta failed to offer an equivalent service for users who refused data sharing, in breach of DMA obligations. So, even where GDPR hurdles can be cleared, other regulatory roadblocks remain.



Hannah Crowther
Partner

Fine and dandy?

A few GDPR fines make the headlines, but most don't. Since this time last year, there have been around 150 fines from the European DPAs, ranging from hundreds of Euros to hundreds of millions of Euros.

By far, the most active DPA in terms of enforcement is the Spanish AEPD, which cracked out over 50 in the last year. Despite some perception to the contrary, it's clear that your name doesn't have to rhyme with a Greek goat's cheese to receive a GDPR fine.

A few fines of particular note:



The **Dutch DPA** fined Netflix €4.75 million for failures in transparency (essentially, problems with its Privacy Statement). After a complaint from Noyb (that permanent thorn in the side of 'big tech'), the DPA found Netflix wasn't clear enough on the purpose and legal basis for processing, data sharing, data retention, and safeguards for data transfers.



The **Italian Garante** issued a €5 million fine to the food delivery app Foodinho for the unlawful biometric processing and geolocation tracking of its delivery riders. Point of interest - a surprising amount of GDPR enforcement activity has centred around 'gig economy' workers. They know their rights!



The **Italian Garante** also issued a €15 million fine against OpenAI, making findings regarding lawful basis and transparency in relation to the training of the ChatGPT model. OpenAI has since established a 'One Stop Shop' in Ireland, so any further enforcement would need to go via Ireland.



The **Irish Data Protection Commission (DPC)** fined LinkedIn €310 million following an inquiry into its processing of personal data for the purposes of behavioural analysis and targeted advertising. The DPC determined LinkedIn did not have a lawful basis and identified failings of transparency and fairness.



The DPC also fined TikTok €530 million for transferring user data to China. For more on this, see our article 'To determine your future, first understand your past: an update on transfers' on page 8.



In a rare enforcement action against a processor, the **ICO** issued a £3 million fine against Advanced Computer Software Group, an IT and software provider, in relation to a ransomware attack affecting customers in the healthcare sector. Back in August, the ICO had announced a provisional notice of intent to fine £6.09 million, so the final figure is a bit of a climb down.

In a sign that the DPC doesn't really know who else to fine, Meta got fined again. Twice. Of the three fines issued last year by the DPC, two went to Meta. In fact, of the 31 fines issued by DPC since the GDPR's inception, 10 have been against Meta. The 2024 Meta fines (€91 million and €251 million) both related to security breaches that took place in 2018 and 2019, respectively. Not quite swift justice.



Mike Edgar
Senior Associate

A(I)gents of change: agentic AI, generative AI and the regulators' response

The past year has seen a flurry of new AI models rolled out, with significant improvements in the size and capability of large language models (LLMs) and multi-modal models (for voice interactions, image and video generation).

Advances have also been made in the deployment of agentic AI, systems that can perform autonomous, goal-directed tasks such as scheduling meetings, responding to emails, or—in the future—placing weekly grocery orders, arranging holidays, or purchasing clothes to match your style.

Against this backdrop, the regulators have had a busy year. We reflect on some of the major developments over the past 12 months.

European DPAs focus on AI training

GenAI models need to understand human language and societal contexts. Big datasets featuring human interactions (posts, comments, reviews, commentary, debate, praise, criticism, etc.), such as those on user-to-user platforms, are useful for training the models that power increasingly human-like GenAI services. European regulators have been swift to intervene against large platforms where privacy concerns arise. Here's a quick round-up:

- In the summer of 2024, following concerns raised by the ICO and the Irish Data Protection Commission (DPC), Meta paused its plans to use public content shared by UK and EU users on Facebook and Instagram to train its GenAI models (known as LLAMA). Key issues centred around the lawful basis for such processing, transparency and users' ability to object.
- Around the same time, the DPC scrutinised X in connection with allegations that it had used EU public posts to train its AI model, Grok. The DPC initiated proceedings in the Irish High Court, which resulted in X agreeing to an undertaking.
- In September 2024, LinkedIn started using UK user data on its platform to train its AI models, but swiftly suspended such training after the ICO raised concerns about the transparency measures and user controls that LinkedIn had provided.
- Finally, the release of DeepSeek's open-source model in late 2024 sparked coordinated concern among several European DPAs, including those in Italy, France, Ireland, and Luxembourg, who have questioned the legality of its training data. The EDPB has stated that coordinated enforcement measures may follow.

The themes that emerge from these interventions are the need to demonstrate a valid legal basis for training, provide clear transparency measures, and honour user rights.

Deployment is also on the DPAs' radar (or at least the ICO's)

While there has been comparatively less regulatory focus on the deployment phase of GenAI services so far, Snapchat's My AI chatbot was an early service that faced scrutiny. Following its launch to UK users in early 2023, the ICO investigated whether Snap had properly assessed the privacy risks posed to users, especially teenage users. The risks identified by the ICO included:

- targeting teen users for advertising (this was later shown not to be the case, as My AI was only used for contextual ads)
- processing special category data on a large scale (arising from the free-text nature of user questions); and
- the risk that teen users may not make fully informed decisions about using this novel type of complex technology.

The investigation resulted in Snap carrying out a revised data protection impact assessment (DPIA) for the risks posed by My AI, and in June last year, the ICO concluded that no enforcement action was needed. This example highlights the importance of ensuring that DPIAs for GenAI products contain detailed and granular assessments of privacy risks and of implementing appropriate safeguards to mitigate them.

The EDPB issues its Opinion on AI models - but questions remain

To round off 2024 (and just in time for Christmas), the EDPB published an Opinion on personal data processing in the context of AI models. The Opinion considers when an AI model can be anonymous, when companies might rely on legitimate interests as a legal basis for the development and deployment phases, and what the consequences are for deploying an AI model based on unlawful training.

The Opinion provides a valuable insight into the current thinking of European DPAs when applying GDPR principles to GenAI technology, especially the factors to consider when conducting the balancing test for a legitimate interests assessment. The Opinion emphasises that the nature of the model and the intended operational uses should play a key part of the assessment, e.g., a therapy chatbot is likely to process more private and sensitive user information than a customer service chatbot.

The EDPB's conclusion on model anonymity raises significant questions and practical challenges. The Opinion states that the likelihood of obtaining personal data from queries should be "insignificant" for a model to be considered anonymous. This approach would result in a large number of GenAI models being treated as personal data, even though (from an engineering perspective) the model itself does not actually store copies of the data it is trained on (a point which the Hamburg DPA acknowledged in its paper on the topic in July 2024). If GenAI models are to be treated as personal data in many cases, how should data subjects' rights, such as the right of access or erasure, operate in practice?

Looking ahead

Agentic AI is expected to be the next game-changer in the AI space. Definitions vary, but its key characteristics include using proactive, autonomous and multi-step decision-making to achieve goals. For example, you might ask a holiday service powered by agentic AI to "plan a relaxing 7-day beach holiday for me and my partner in July, somewhere in Europe. Budget: £2,000. Prefer quiet locations, not tourist hotspots", and the assistant would do the rest. In addition to using an LLM to understand this goal, and support the multi-step holiday planning, this type of service would need appropriate interfaces in place to enable it to search for weather, appropriate destinations, flights and hotels (for example, APIs to exchange information with BBC Weather, Skyscanner, Booking.com, Google Maps, etc.).

From a data protection perspective, user data may flow both ways through these APIs, with the AI agent making decisions about what personal information to use, how to use it, and who to share it with. The complexity of these systems and the unpredictability of autonomous AI decision-making, lead to novel questions about how GDPR rules apply. For example, how should transparency requirements be met for data processing in large, multi-company ecosystems? What GDPR role applies to each company in the ecosystem, and where do their respective responsibilities start and end? Companies seeking to use such technologies must start thinking about these issues to ensure their compliance measures keep up with the impressive pace of technological change.

The year in numbers...



Vivien Zhu
Associate



100,000

Online services likely to be in scope of the Online Safety Act



1000

ICO expands their cookie enforcement to the UK's top 1000 websites (as part of the ICO's 2025 Online Tracking Strategy)



6 months

Extension on the validity of UK/EU adequacy decisions (until 27 December 2025)



€1.18 billion

Total GDPR fines issued by the Irish DPC

**based on published and publicly announced decisions from 1 Jan 2024 - 2 May 2025*



£3.89 million

Total UK GDPR fines issued by the ICO

**based on published decisions from 1 Jan 2024 - 2 May 2025*



4

UK GDPR fines issued by the ICO

**based on published decisions from 1 Jan 2024 - 2 May 2025*



2

Enforcement notices issued by the ICO (from 1 Jan 2024 - 1 April 2025)

**based on published decisions and excluding PECR ENs*



12,193

Security incidents reported to the ICO in 2024



74%

Of parents and carers have worries about online safety as developments with AI, virtual reality and new social media apps continue to accelerate

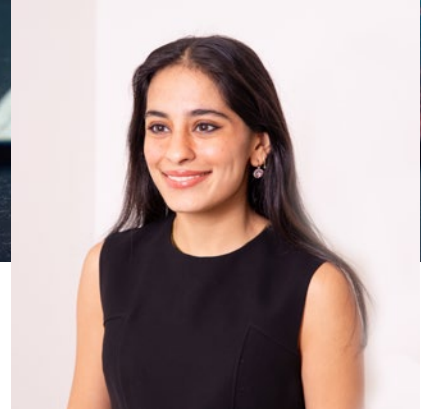
**UK Safer Internet Centre 2024 Research Report*



42%

Of parents and carers have an awareness of the Online Safety Act

**UK Safer Internet Centre 2024 Research Report*



Subha Kumar
Associate

Take two: UK data protection reform

A ‘bonus’ topic that didn’t quite make the Top 10....When the UK Data Protection and Digital Information (DPDI) Bill failed to pass before the July 2024 election, we wondered if the newly elected Labour government would resurrect it in some form. The answer turned out to be “yes”, and in October, the UK Government published the Data (Use and Access) Bill (DUA). So, what’s changed between the old and the new Bill? (answer: not a huge amount...)

What’s changed?

- One of the most eye-catching changes in the DUA is the increase in fines for breaches of ePrivacy rules. Right now, PECR fines are capped at £500,000, but the DUA aligns this amount with the UK GDPR, meaning that businesses could be fined a maximum of £17.5 million for PECR violations.
- Another big change is that the Secretary of State would have powers to expand (or narrow) the list of special categories of data (SCD). This is a pretty big deal, and it seems the intention is to future-proof the legislation as new types of sensitive data, e.g., cognitive biometric data, emerge.

- The DUA narrows the scope of the prohibition on automated decision-making (ADM) under Article 22 UK GDPR. Currently, ADM is allowed where the processing of personal data is (a) necessary for the performance of a contract, (b) authorised by law, or (c) explicit consent has been obtained. The DUA provides that one of these conditions only has to be established where the processing involves SCD (not 'regular' personal data) - opening up businesses' ability to use, e.g., AI in new use cases.

What's stayed the same?

- The DUA retains the concept of "recognised legitimate interests" for which no Legitimate Interests Assessment is required. Examples of such interests include safeguarding national security and public safety (some of which seem relatively high risk and perhaps would warrant a balancing test in our view).
- For the life sciences sector, the DUA keeps helpful DPDI provisions, which state that commercial research falls within the scientific research exemption under Article 89(2) UK GDPR (which disapplies certain data subject rights). The DUA also makes consent requirements more permissive, such that sponsors can obtain one consent for broad (secondary) purposes.
- The DUA clarifies that individuals are only entitled to personal data in response to a DSAR that is "based on a reasonable and proportionate search" - something all businesses are likely to welcome!
- What about international data transfers? The DUA borrows the adequacy test introduced in the DPDI, i.e., the level of protection in a third country must not be "materially lower" than the UK.
- The DUA keeps exemptions to cookie consent where the privacy risk is considered to be low. Such scenarios include cookies used for statistical purposes and to optimise website displays. This will hopefully minimise cookie consent fatigue. Note that transparency requirements and the need for an opt-out remain.
- Finally, the DPDI's proposed changes to the ICO's structure make the cut. If passed, the ICO will be known as the Information Commission and be led by a board of non-executive and executive members. The DUA retains additional proposed enforcement powers, e.g., the Commission can issue Interview Notices and enhanced Information Notices for specific documents to be produced.

Meet our data protection team

Victoria Baron

Senior Associate
victoria.baron@bristows.com

Jamie Cox

Associate
jamie.cox@bristows.com

Hannah Crowther

Partner
hannah.crowther@bristows.com

Marc Dautlich

Partner
marc.dautlich@bristows.com

Jamie Drucker

Partner
jamie.drucker@bristows.com

Julian Darrall

Partner
julian.darrall@bristows.com

Mike Edgar

Senior Associate
michael.edgar@bristows.com

Alice Esuola-Grant

Senior Associate
alice.esuola@bristows.com

Sophie French

Associate
sophie.french@bristows.com

Faye Harrison

Of Counsel
faye.harrison@bristows.com

Charlie Hawes

Of Counsel
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

Subha Kumar

Associate
subha.kumar@bristows.com

Janna Lawrence

Associate
janna.lawrence@bristows.com

Elisa Lindemann

Associate
elisa.lindemann@bristows.com

Rose Lynch

Associate
rose.lynch@bristows.com

Emma Macalister Hall

Senior Associate
emma.macalisterhall@bristows.com

Mac Macmillan

Of Counsel
mac.macmillan@bristows.com

Naina Mangrola

Associate
naina.mangrola@bristows.com

Simon McDougall

Senior Advisor
simon.mcdougall@bristows.com

Christopher Millard

Senior Counsel
christopher.millard@bristows.com

Anna Ni Uiginn

Associate
anna.niuginn@bristows.com

Rob Powell

Senior Associate
rob.powell@bristows.com

Manuel Rey

Associate
manuel.rey@bristows.com

Kiran Sidhu

Associate
kiran.sidhu@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