Not quite two peas in a pod: UK and EU regulatory divergence

Peter Given
Partner
T: +44 (0) 20 7894 6077
pgiven@dacbeachcroft.com

Amanda Mackenzie
Associate
T: +44 (0) 20 7894 6297
ammackenzie@dacbeachcroft.com

The UK Information Commissioner's Office has long had a reputation of pragmatic regulation, particularly when compared to the more dogmatic approach of its EU counterparts. The ICO's recent two-year trial of an alternative enforcement regime for the public sector is an example of this pragmatic regulation.

The ICO trialled an approach to reduce the impact of fines on the public (who ultimately fund the payment of fines imposed on public sector bodies). In practice, this has resulted in an increase in public reprimands and the use of other powers, including enforcement notices, with fines intended to be reserved for only the most egregious cases (for example, fines were imposed on the Ministry of Defence and Police Service of Northern Ireland – albeit the application of the public sector approach also meant the amount of these fines was reduced). The ICO confirmed in December 2024 that this public sector approach will now be made permanent.

More recently, and beyond the public sector, during the ICO's annual Data Protection Practitioner's Conference in October 2024, the Information Commissioner noted that he had made a conscious decision to pursue fewer enforcement cases, instead focusing resources on delivering faster, more effective enforcement. Indeed, the Information Commissioner said he would rather have three cases with penalties and lessons for the broader economy delivered in six months, than ten cases delivered in five years.

Even where fines are issued by the ICO, the level of those fines pales in comparison with some of those issued in the EU. While there are undoubtedly numerous reasons for this, it is apparent that there is a growing divergence in the approach towards regulatory enforcement between supervisory authorities in the EU and the UK.

We set out to examine this divergence in approach (and its implications), starting with an analysis of circumstances in which such divergence has manifested.

Recent examples of the difference in the EU and UK approach

Cookie enforcement – two recipes for success?

Currently, EU and UK laws concerning the use of cookies and similar technologies are derived from the EU's ePrivacy Directive. Despite this common origin, the approach to enforcement differs between the UK and the EU (and indeed across the EU).

In the UK, the ICO has adopted a strategy of prior engagement, rather than immediately reaching for formal enforcement tools. For instance, at the end of 2023, the ICO carried out a review of cookie banners and policies on the most visited UK websites, proactively writing letters to those that were non-compliant and threatening enforcement action if changes weren't made. The ICO has stated that this was a successful strategy – with ultimately only one company not changing its practices as a result of the letter. This proactive approach was designed to change behaviours and, by that measure, has undoubtedly been a success, driving a renewed focus on cookie compliance both by those who were the recipient of an ICO letter but also more broadly given the high-profile nature of this activity. This success has been achieved without resort to fines as part of this particular campaign. The ICO recently announced an extension to this approach as part of its online tracking strategy for 2025, now involving a compliance review of the top 1,000 most popular websites in the UK.

By contrast, supervisory authorities in the EU have taken a more robust approach, including issuing substantial fines. For example, in December 2023, the CNIL (the French data protection authority) imposed a EUR10 million fine on Yahoo for placing advertising cookies on users' devices without consent and for not providing users with the ability to withdraw their consent freely. More recently, the CNIL fined ORANGE (a telecommunications operator) EUR50 million for, among other things, not complying with the French cookie laws.

The price of permission – consent or pay models under scrutiny

Following Meta's ongoing battles with EU supervisory authorities over its lawful basis of processing in the context of behavioural advertising, in November 2023 it introduced a subscription model known as 'consent or pay' for access to Facebook and Instagram services in the EEA and Switzerland. In response to this new model, several supervisory authorities requested an opinion from the European Data Protection Board (EDPB), specifically considering the extent to which consent collected in this way can be said to be valid and freely given. Activist groups, such as noyb, also issued open correspondence encouraging the rejection of these models.

The EDPB issued its Opinion in April 2024 and concluded that:

> *"in most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee."*

The EDPB was critical of the binary choice offered, stating that an 'equivalent alternative' should be made available. This third option should, according to the EDPB, enable the user to access the relevant service without paying a fee and *"with a form of advertising involving the processing of less (or no) personal data"*.

The ICO, in recently published guidance, has taken a more sympathetic position. The ICO highlighted that UK data protection law does not specifically prohibit business models that rely on 'pay or consent' so long as this does not undermine the validity of consent, taking into account factors like the balance of power, the equivalence of the ad-free or ad-funded service and the appropriateness of the fee.

This example of regulatory divergence has already had a tangible effect. Users of Facebook and Instagram in the EU are subject to the pay or consent model, unlike the users in the UK. UK users may arguably have a more seamless user experience, but do not have the option to pay for a version of the platform that doesn't involve processing their personal data for behavioural advertising.

Employee monitoring – tracking time or trampling privacy?

Post-pandemic remote workforces and advances in technology are in part driving developments in the field of employee monitoring. This continues to be an area of focus, where divergence is also apparent.

By way of example, in December 2023, the CNIL concluded its investigation into Amazon France Logistique (AFL) regarding its employee monitoring practices. AFL manages Amazon's large warehouses in France, which are used as part of the logistics and delivery network for Amazon's retail customers. The CNIL decision focused, in part, on hand scanners given to AFL's employees. These scanners are used by the employees to record certain actions (e.g., removing or returning an item to a shelf). The data collected by the scanners provided very granular information which was used by AFL to calculate indicators of quality, productivity and inactivity. Overall, the CNIL found that this data processing was excessive and disproportionate and fined AFL EUR32m.

By contrast, a few months later in February 2024, the ICO issued Serco (a multinational company specialising in the delivery of public services) with an enforcement notice in connection with Serco's use of biometric technology (including facial recognition) in its leisure centres. Specifically, the technology was used to monitor employee attendance. The scale of the use was significant, with just under 2,300 employees across 38 facilities affected, with approximately 7 million scans taking place since the system's inception. Ultimately, the ICO concluded that the processing of the employees' biometric data was unlawful (in particular, excessive and unnecessary) and yet, notwithstanding the scale of the infringement and the sensitivity of the data concerned, the ICO did not impose a fine – instead issuing an enforcement notice prohibiting Serco from continuing the activity and requiring that it delete the data already collected.

While both approaches have had the effect of raising awareness of the data protection issues that need to be addressed in undertaking employee monitoring, the absence of financial penalties imposed by the ICO will undoubtedly feed into the risk assessment undertaken by employers when considering the roll out of more intrusive monitoring tools.

The great AI divide

The ICO and EU supervisory authorities have also taken divergent approaches to the deployment of AI, including in relation to training AI models. For instance, some EU supervisory authorities have cast doubt on the extent to which the legitimate interests legal basis can be used to train AI models, particularly in relation to data obtained from online web scraping. Several US tech companies, including Meta, Google and X, have suspended or paused AI projects using EU data as a result.

This uncertainty has resulted in a number of technology companies questioning the stance on the application of the GDPR to AI models, resulting in an open letter to EU leaders warning that Europe will fall behind the rest of the world in the global AI race. The letter warned that:

> *"…regulatory decision making has become fragmented and unpredictable, while interventions by the European Data Protection Authorities have created huge uncertainty about what kinds of data can be used to train AI models. This means the next generation of open-source AI models, and products and services that we build on them, won't understand or reflect European knowledge, culture or languages".*

By contrast, the UK ICO has provided its own thoughts on the extent to which legitimate interests can be relied upon to process data scaped from the internet to train an AI model – essentially finding that legitimate interests remains the sole available lawful basis based on current practices – making the position clearer in the UK. As a manifestation of this, Meta recently confirmed that it will reinstate its plans to use personal data from Facebook and Instagram users in the UK to train its AI models, relying on 'legitimate interests' as its legal basis, having *"engaged positively"* with the ICO. Despite this, an ICO statement issued on 13 September 2024 made it clear that the ICO had not provided *"regulatory approval for the processing and it is for Meta to ensure and demonstrate ongoing compliance".*

Divergence in this area is also having tangible impacts – at the very least, AI developers seem more willing to develop their AI models using UK data. Could this ultimately mean the EU gets left behind in the global AI race? In an attempt to achieve some form of certainty and consistency across the EU, the Irish Data Protection Commission sought an opinion from the EDPB on, amongst other things, the extent to which personal data is processed at various stages of training and operating an AI model and the legal basis to legitimise processing. The EDPB's opinion was published on 18 December 2024.

What are the implications of this divergent regulatory approach?

It is clear from these examples that, thematically, the ICO is frequently taking a different path to its EU counterparts. The ICO takes a more pragmatic view when it comes to the interpretation of data protection law and, when using its enforcement powers, doesn't instantly reach for its power to impose fines. A speech made by John Edwards (the current UK Information Commissioner) at the National Association of Data Protection Officers annual conference in 2022 reinforces this where he said: *"There's nothing in the law or in contemporary regulatory theory that says that enforcement must equal fines. Enforcement happens across a spectrum. Rather than being one thing, it's a series of graduated responses to non-compliance."*. This sentiment was repeated by Edwards in December 2024 when confirming the public sector approach to enforcement (see above) would be made permanent.

While an arguably 'softer' regulatory approach still seems to be bearing fruit in some respects – the ICO would certainly point to the approach they have taken to enforcing cookies rules to drive change without imposing fines – it is becoming apparent that the differing approach is starting to have tangible impacts for data subjects in the UK and the EU. Whether that is the absence of EU data being used to train AI models, or the absence of the consent or pay mechanism for UK Facebook users. If there is increasing divergence between the UK and the EU approach, then the nature and extent of these manifestations will increase.

What does the future hold?

The UK's third attempt at data protection reform, the new Data (Use and Access) Bill (DUAB), is currently making its way through the UK legislative process. It seems unlikely that this Bill in and of itself will change the ICO's current enforcement approach. The DUAB maintains its predecessor's provisions for the creation of an Information Commission, introducing a body corporate with a statutory board, chair and chief executive. The government decided not to pursue the proposal put forward in the predecessor Bill which would have required the ICO to follow a statement of strategic priorities prepared by the Secretary of State. This proposal had generated concerns about the regulatory independence of the ICO. Arguably, this could have created even further regulatory divergence with the EU.

In the medium term though, could a change in the Information Commissioner (or the chair / chief executive of a newly formed Information Commission) affect the approach and lead to greater or lesser divergence? Potentially. The approach of Elizabeth Denham (the predecessor to the current Information Commissioner) was clearly different to the strategy pursued by the current Commissioner. Denham favoured overt action and big-ticket fines (readers will recall the eye watering provisional fines for the British Airways and Marriott data breaches, together with the FBI-style ICO jackets worn by staff during the raid on Cambridge Analytica's offices, which all took place under Denham's tenure). As the current Commissioner is at the helm until 2027, any change in approach is a few years away. For now, we wait to see where and when UK-EU regulatory divergence will next manifest itself.

Full list of references available upon request