SLAUGHTER AND MAY/

13 DECEMBER 2023

KEY DEVELOPMENTS IN CONTENTIOUS DP IN 2023

Year-on-year, data becomes more of a concern for individuals, organisations and regulators as both commercial opportunities and regulatory risks increase. The GDPR kicked off the latest phase of the data revolution in May 2018 and has since been followed by similar legislation in other jurisdictions, most notably the wave of state privacy legislation in the US. In the UK, the new Online Safety Act imposes a duty on online platforms to protect UK users by assessing risks of harm and taking steps to address them. The EU has similarly sought to regulate online content through its Digital Services Act and has recently reached agreement on the EU AI Act, which seeks to mitigate the risks of artificial intelligence (AI) technologies by banning or regulating AI systems depending on the perceived level of risk.

Data protection authorities (DPAs) have made use of their wide powers under the GDPR and have issued more than 1900 fines totalling some €4.4 billion since its introduction. DPAs and organisations have also acknowledged its complexity with more than 50 cases having been referred to the Court of Justice of the European Union (CJEU) to determine how the GDPR should be applied, including in relation to fundamental questions such as data subjects' rights to compensation for breaches of the GDPR. Such questions are also being considered by national courts whether in the context of appeals of DPA decisions such as those being brought by Meta and TikTok in Ireland or in the various appeals against ICO decisions in the UK, including Clearview's successful (but under appeal) challenge of the ICO's jurisdiction to issue it with a £7.5 million penalty in 2021.

The fundamental importance of data to the global economy also means that it is no longer just the concern of DPAs and the courts. Regulators in other areas, in particular the competition and finance ones, are taking on an increasing role in the supervision of cybersecurity and data breaches. For example, the US SEC's new cybersecurity rules which come into force on 15 December 2023 include mandatory breach reporting requirements similar to those in the GDPR. In addition, there have been tensions between regulators as to their respective roles and remits as regards data. This was recently considered by the CJEU in *Meta Platforms* (with judgment given on 4 July 2023), which ruled that competition authorities can assess violations of data protection rules where necessary to establish an abuse of dominance and that there is a requirement for coordination and cooperation between competition and data protection authorities.

Set in this fast-moving context, four key developments stand out in the UK from the last 12 months and perhaps give a steer as to what lies ahead next year.

Re-focused regulatory activity

Whatever the approach taken in specific jurisdictions, the greatest risks come from processing the most sensitive data (and for the most sensitive data subjects), including in terms of challenge and enforcement from regulators as well as material brand and business damage in the event of a breach.

This is particularly the case in the UK where the ICO's action plan for October 2022 to October 2023 set out its key areas of focus, being: children's privacy; the impact of technology on vulnerable groups; deprivation; and personal safety. The focus on sensitive data and, in particular children's privacy, was evidenced by the £12.7 million fine imposed on TikTok for breaches of data protection law, including failing to use children's personal data lawfully. The ICO found that TikTok did not do enough to check who was using their platform or take sufficient action to remove the underage children that were there. Since the conclusion of the ICO's investigation into TikTok, the regulator has published their "Children's code" which contains 15 standards that online services need to follow to ensure they are complying with their obligations under data protection legislation to protect children's data online and guidance on how to establish the age of users (including a suggestion to use AI to analyse the way in which users interact with the service to estimate age).

The ICO has yet to release its next action plan but John Edwards' speech at the Data Protection Practitioners' Conference (DPPC) in October 2023 suggested that artificial intelligence and other innovative technologies will continue to be a priority for the ICO, particularly businesses using algorithmic decision-making and processing biometric data, with the use of employee monitoring software being singled out as a key area (the ICO just having issued guidance on the topic). The overlap of priorities with Ofcom's approach under the Online Safety Act will be key too.

Greater use of reprimands

John Edwards also announced at the DPPC that the ICO had completed its own risk review, which included a focus on its own end-to-end investigatory process. The ICO has acknowledged significant delays have affected investigations and suggested that one of the reasons for this has been over-resourcing lower-level regulatory activity. It is therefore unsurprising that the ICO has increased its use of reprimands for less serious infringements of the UK GDPR, including in relation to inadvertent or inappropriate disclosures of personal information, failures to respond to data subject access requests (DSARs) on time and, in particular, against public sector entities where the ICO has indicated that fines against the public purse serve no useful purpose.

What is more interesting is that, since December 2022, the ICO has published reprimands unless there is a good reason not to (previously reprimands were generally confidential). Reprimands typically include recommendations from the ICO to bring the organisation into compliance with the UK GDPR and it is expected that organisations will implement changes accordingly. By publishing reprimands, the ICO encourages compliance and highlights lessons for controllers. However, there is a concern that reprimands can lead to reputational harm (and potentially provide the basis for follow-on claims) without the organisation being given the chance to make representations to the ICO (as is provided for in the case of a fine) and, perhaps even more importantly, without the possibility of appeal.

A view from Ireland: the DPC's approach

Ciara Anderson, Senior Associate, Arthur Cox (Dublin)

Notwithstanding the pressures it faces, the Irish Data Protection Commission (DPC) appears committed to a supervisory approach which prioritises data compliance through extensive engagement with stakeholders and corrective measures promoting broader, longer-lasting behavioural change rather than simply focusing on "hard enforcement" options such as penalties and sanctions (as some have urged it to do).

This was certainly the case in the original DPC decision relating to data transfers by Meta Platform Ireland Limited in relation to its Facebook service. The DPC ordered Meta to: (i) suspend the data transfers; and (ii) cease unlawful processing of personal data of EEA users in the US transferred in violation of the GDPR. The decision not to impose an administrative fine on Meta was based on the DPC's belief that the imposition of a fine in addition to the corrective orders would not be "effective, proportionate and dissuasive" and "would not render the DPC's response to the findings of unlawfulness any more effective".

As part of the Article 65 consistency procedure, the EDPB insisted on the record-breaking €1.2 billion fine on the basis that this was necessary to punish unlawful historical behaviour. It believed that the corrective measures proposed by the DPC were solely forward-looking and did not address the historical processing.

Meta has filed an appeal in the General Court of the EU seeking to annul the EDPB's decision. The effectiveness of the decision hangs in the balance pending determination of the appeal. In the meantime, the DPC has continued to rely on Recital 148 GDPR when issuing reprimands in addition to administrative fines and/or orders for compliance, including in its recent decision against Airbnb Ireland UC for unlawful processing for the purposes of verifying users' identification. Whatever the result in the Meta appeal, and unless and until there are changes to the one-stop shop mechanism, the DPC's supervisory approach is likely to remain in the spotlight.

Clarity on fines

As regards more serious infringements, on 2 October 2023, the ICO published new draft fining guidance under the UK GDPR and the Data Protection Act 2018 (the "**draft Fining Guidance**"). The level of detail and practical guidance in the draft Fining Guidance makes clear that the ICO has considered previous feedback (and criticism) on its existing Regulatory Action Policy (and previous draft guidance).

- The draft Fining Guidance sets out:
- the legal framework that gives the ICO the power to impose fines;
- the circumstances in which the ICO would consider it appropriate to issue a penalty notice; and
- how the ICO calculates the appropriate amount of the fine, including the factors that determine that it is effective, proportionate and dissuasive.

The ICO has looked to the European Data Protection Board's (EDPB) Guidelines on the calculation of administrative fines (released in June 2023) and, like the EDPB, has proposed a five-step methodology setting fines, following the factors identified in Article 83 of the UK GDPR. Organisations will welcome the sense of alignment between the UK and EU which should assist in ensuring regulatory compliance across jurisdictions and provide greater certainty on enforcement action when things go wrong. Importantly, the draft Fining Guidance provides that once an infringement has been found, the starting point for a fine remains a percentage of turnover (rather than the nature of the infringement) so while the ICO is yet to enforce fines at the level of the Irish Data Protection Commission (DPC), it is clear it intends to retain the power to do so.

In view of the sizeable fines levied by the DPC over the past year, including the €1.2 billion fine imposed on Meta in May 2023 in relation to EU/US data transfers, it is interesting to note that there are suggestions that the ICO (and to some extent the DPC) is not convinced of the focus on, and benefits of, fines. This is especially the case in enforcement activity in the information security sphere, where there is concern that the imposition of substantial fines could ultimately end up reducing spending on remediation efforts and improved security for data subjects at scale.

An even higher bar for data-related class actions

While the limits of the GDPR are being tested continuously by the courts, whether at national or EU level, in the UK at least the scope for blockbuster individual claims remains relatively curtailed.

This year, those seeking to bring data-related class actions suffered a further setback with the High Court decision in *Prismall v Deepmind*. Mr Prismall's action was on the basis of misuse of private information and the High Court performed a "lowest common denominator" analysis in which it found not every member of the class had a viable claim (similar to the result in *Lloyd v Google*) but Mr Prismall has been granted permission to appeal. The "bifurcated process" envisioned by Lord Leggatt in *Lloyd v Google*, whereby common issues such as whether there is an actionable breach would be determined for the entire class with individual issues to be dealt with subsequently, was recently adopted in the High Court in *Barclays Bank UK Plc v Terry* (a financial rather than data claim) and may result in others looking at it again as a viable (if lengthy) route to recovery.

Claimants in the UK are also continuing to explore other means of pursuing mass data-related claims including group litigation orders, preliminary issues trials and bringing actions in the Competition Appeals Tribunal. In proceedings arising out of Equifax's 2017 data breach, the parties requested the use of a preliminary issues trial to decide the value of the case instead of seeking a group litigation order. The case was to proceed to a case management conference this autumn but Equifax announced a settlement before the issue was determined.

Less high value but often very time consuming, claimants are also increasingly using DSARs as a pre-disclosure tool in litigation, particularly in the context of employment claims. The ICO released new guidance for employers in May of this year off the back of receiving 15,000 complaints in relation to DSAR and, as flagged above, has indicated an increasing willingness to issue reprimands for failures to respond to DSARs.

While the floodgates on mass claims remain closed in the UK (for now), the courts remain an area to watch if not necessarily fear.

CONTACT

RICHARD JEENS
PARTNER
T: 020 7090 5281
E: Richard.Jeens@slaughterandmay.com

ROSS O'MAHONY
ASSOCIATE
T:020 7090 3856
E: Ross.OMahony@Slaughterandmay.com

CIARA ANDERSON
ASSOCIATE, ARTHUR COX
T: +353 1 920 1347
E: Ciara.Anderson@ArthurCox.com

London	**Brussels**	**Hong Kong**	**Beijing**
T +44 (0)20 7600 1200	T +32 (0)2 737 94 00	T +852 2521 0551	T +86 10 5965 0600
F +44 (0)20 7090 5000	F +32 (0)2 737 94 01	F +852 2845 2125	F +86 10 5965 0650

Published to provide general information and not as legal advice. © Slaughter and May, 2023.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com