SLAUGHTER AND MAY/

January 2023

THE YEAR IN UK GDPR REGULATORY ENFORCEMENT ACTION

THE ICO'S APPROACH TO ENFORCEMENT IS STILL RISK-BASED, BUT INCREASINGLY TARGETED

A version of this article first appeared in the Privacy Laws & Business UK Report, Issue 125 (January 2023)

When John Edwards took office as the new Information Commissioner in January 2022, he faced a dauntingly full in-tray. Since the introduction of the GDPR in May 2018, the ICO has been criticised for a sometimes inconsistent and opaque approach to regulatory enforcement, with concerns expressed about decision-making regarding fines, resourcing issues and technical capacity. More recently, the ICO has, perhaps unfairly, come under scrutiny for "going easy" on the public sector and endorsing the DCMS' controversial data protection legislative reform plans.

A year in, how much has changed? What evidence is there that the UK has, in the Commissioner's words, "*gone [its] own way*" in empowering businesses to use information responsibly to invest and innovate whilst encouraging individuals to confidently share their information when engaging in products and services that drive the economy? And what role has the administrative court system had in 'regulating' the regulator and shaping the enforcement landscape?

The current regulatory enforcement action landscape

Over the past twelve months, against the backdrop of increasingly 'mega' fines in the EU and US, the ICO has maintained its risk-based approach to investigation and enforcement action, consistent with statements from former Commissioner Denham that the ICO must reserve the most serious sanctions for those who mishandle or misuse data. The five monetary penalty notices (MPNs) published by the ICO in 2022 focus on:

I. large-scale organisations that handle and process huge quantities of data, where there is an expectation of a substantial GDPR implementation strategy (and sufficient resources allocated to do so); and

II. organisations that should be aware of the higher risks inherent in processing sensitive data.

The ICO set out in 'ICO25: Our Regulatory Approach' that its main focus is on high-risk areas "*where non-compliance could do the most harm*", consistent with the DCMS' response to 'Data: a new direction' and its call for the ICO to focus on "*the most serious threats to public trust and barriers to responsible data use*". The Commissioner has placed greater emphasis on 'Privacy by Design' and has come down hard on organisations for their failure to take the necessary remediation efforts in the aftermath of prior data incidents.

However, at the same time, the Commissioner recently announced his intention to avoid "*whack-a-mole*" enforcement by designing a suite of tools for organisations to reduce their UK GDPR compliance burden and reduce their external advisor costs, "*reducing their excuses for non-compliance*".[1]

In addition, the Commissioner has emphasised that the ICO's attitude to enforcement should be understood as existing across a spectrum: "*a series of graduated responses to non-compliance*", resulting in a decision to publish all reprimands (applied with effect from January 2022, including one against Grindr) on the ICO website. The ICO has also started publishing information on data breach investigations (including details of the breaches themselves, complaints and civil investigations) dating back to Q4 2021. Together, these factors suggest a reframing of ICO enforcement priorities to accountability, transparency and ultimately certainty (reinforced by the regulator's commitments in 'ICO25: Our Regulatory Approach'), with a greater emphasis on giving an informal 'slap on the wrist' to low-level and first-time offenders.

This more targeted approach to enforcement action by the ICO has been supported by UK courts. In early December 2022, a High Court judge ruled (in dismissing a judicial review application by Wise against the ICO relating to DSAR failures) that the ICO is not obliged to

[1] John Edwards interview, MLex, 24 November 2022.

fully investigate every complaint it receives, as to do so would stretch its resources "to a breaking point". To put this in context, 9,571 personal data breaches were notified to the ICO but only 9.6% of breaches notified resulted in investigation in 2021-22 (against 21.6% in 2020-2021).

Key takeaways from this year's penalties

Some clear themes have emerged from the MPNs issued in 2022, providing guidance on how the ICO and courts expect organisations to handle cyber and data risk. However, MPNs must be understood as only the 'tip of the iceberg' given the renewed focus on informal enforcement action in the UK and EU. Indeed, as Andrea Jelinek, chair of the EDPB, commented at the IAPP Conference in Brussels in November 2022, the 'toolkit' for GDPR enforcement is now much clearer and, subject to Member States' administrative rules, can be expected to be applied more going forward.

All organisations are expected to stay on top of security standards and practices

As set out in the MPNs against Tuckers Solicitors and Interserve this year, "*appropriate technical and organisational measures*" must reflect relevant industry standards and good practice, even if the organisation operates as B2B or is experiencing significant financial challenges. The ICO has expressly referenced the ISO27000 and the US National Institute of Standards and Technology (NIST) standards, as well as publicly available guidance such as that from the ICO and UK National Cyber Security Centre (NCSC) on, for example, the appropriate use of multi-factor authentication, patch management and encryption, legacy protocol removal and endpoint protection, data protection training and streamlining incident response.

By referring to objective standards against which organisations will be held to account, the ICO brings welcome clarity and certainty to the application of the UK GDPR, UK DP Act 2018 and its own regulatory action policy. The First-Tier Tribunal (FTT) has reinforced this with the notion that the ICO should sometimes seek external views when information is technically complex, so as to make the assessment of organisations' compliance efforts more structured and transparent to organisations themselves.

Organisations should therefore ensure that they record how they have addressed both: (i) relevant regulatory and law enforcement recommendations or guidelines; and (ii) applicable industry standards. Being able to produce evidence at short notice should help with ongoing internal risk management and any ICO enquiry or action.

The importance of proactive remediation and investigation

The ICO has acknowledged extensive remedial efforts made by organisations to address the impact of a breach and mitigate the risk of harm to data subjects, often reflected in substantial penalty reductions (e.g. Interserve). However, the ICO has noted that such remedial actions must be proactive rather than reactive; as reflected in the Easylife MPN, an organisation should not wait until it is told to make changes by a regulator.

Also relevant here are often unrealistic expectations about the reasonableness of time taken to remediate and restore access to data in the event of a data incident. Even where data restoration was prioritised, consistent with the principle of data minimisation, the ICO can be critical of the time taken (e.g. Interserve). Challenging this will require detailed investigation by the organisation and its advisers so as to present clear facts to the ICO from the outset, not only in relation to how the breach occurred and what data was affected, but also how it proactively addressed the risk of harm. In addition, undertaking a detailed investigation can empower an organisation to effectively challenge the ICO's findings if required, as demonstrated by the penalty reductions obtained by DSG Retail and Doorstep Dispensaree before the FTT.

The ICO punishes organisations for complacency and past behaviours

This year's penalties indicate that a prior data incident and any unaddressed remediation efforts arising from such incident will be taken into account as aggravating factors. This is emphasised in the ICO's draft enforcement guidelines as well as in the MPNs issued to Interserve and The Tavistock & Portman NHS Foundation Trust. The Commissioner has stated that he considers "complacency" to be the most serious cyber risk and that organisations will face fines if they fail to monitor for suspicious activity on an ongoing basis, act on warnings, update software or train their staff.

On this basis, the ICO will not look favourably upon any instances where an organisation has failed to address known vulnerabilities in their technical or organisational security, especially where such vulnerabilities have been exploited previously and effectively "leave the door open to cyber attackers".

Real risk vs. perceived slights to data subjects

In spite of the core aims set out in ICO25 to "protect people and prevent harm" and guarantee the protection of vulnerable individuals, the mere risk of (non-material) harm to individuals seems unlikely to be a key consideration in ICO enforcement action

(arguably lending credence to recent complaints by MEPs that the ICO and DCMS are "giving in on privacy in exchange for business gain").

In the Interserve case, a ransomware group accessed data of 113,000 individuals but Interserve's investigation made clear that there was there was no evidence of identifiable harm to individuals from the attack. The ICO agreed with this conclusion and the core failings leading to enforcement in the MPN therefore related to the failure to have appropriate measures to keep data secure. In the same vein, though the ICO recognised the substantial distress caused by Tavistock & Portman's disclosure of names in relation to gender identity support, the gravity of the harm was ultimately not reflected in the final penalty figure due to the ICO's new approach to public authorities (discussed further below).

Although the data scraping undertaken by Clearview AI of a substantial number of UK citizens from publicly available sources such as social media platforms was categorised as novel or invasive technology causing a "high level of intrusion into the privacy of individuals", the ICO focused on penalising Clearview's (evident) compliance failures rather than seek to assess levels of harm suffered by individual data subjects. Similarly, in the Easylife MPN, the ICO acknowledged that the resulting harm to individuals could range from financial damage to the harassment and targeting of potentially vulnerable individuals, but did not engage with the weighing up of this damage due to the "invisible" nature of the health profiling undertaken by Easylife.

This attitude is consistent with broader trends in data-related litigation where the courts in England and Wales (and indeed in Europe) have displayed a reluctance to award substantial compensation for non-material damages in data breach cases (see Lloyd v Google and Österreichische Post). Recent settlements in the US and ongoing litigation in the Netherlands (see Foundations v Tiktok et al.) suggest cases where there is evidence of material damage and/or active use of personal data could prove more costly.

The challenge to ICO decisions posed by regulatory appeals

Doorstep Dispensaree's successful challenge against the ICO before the FTT in 2021 (which saw the FTT reduce the fine imposed by the ICO by over 50%) indicated a growing appetite among controllers to challenge the ICO's decisions and the FTT's increasing willingness to hold the regulator to account. To its credit, the ICO seems happy to accept these challenges head-on, having secured new funding for litigation from civil monetary penalties up to a maximum of £7.5 million, to cover "pre-agreed, specific and externally audited litigation costs".

However, FTT decisions, such as DSG Retail (against a penalty for data security failings under the DPA 1998) provide useful guidance for data controllers and the ICO, particularly regarding the scope to exercise their own discretion in how they chose to comply with their data security duties and their assessment of the cost of implementing technical and organisational measures (against the risk of harm if they are not in place). The FTT has made clear that organisations should take a 'risk-based' approach to compliance. This aligns with the ICO's aim to equip organisations with the requisite knowledge to take control of their own compliance.

More controversial was the ICO's agreement in November to reduce its MPN against the Cabinet Office from £500,000 to a mere £50,000 (approved by the FTT, dismissing the appeal). This put into practice the ICO's two-year trial of a more conciliatory approach to enforcement against public authorities. Though an obvious criticism may be that the ICO is "going easy" on government departments to the detriment of individuals, this approach is consistent with Commissioner Edwards' reiteration that large fines are not the be-all-and-end-all for effective enforcement. Lower public sector fines "coupled with better engagement including publicising lessons learned and sharing good practice" should foster better understanding and application of fundamental data protection principles rather than encouraging defensive or uncooperative practices from public bodies fearful of punitive enforcement.

This approach addresses previous criticisms regarding the "money-go-round" between public authorities, and tacitly recognises that the impact of a public sector penalty is often felt most by the victims of the breach itself. In the words of the Commissioner, "put coarsely: your data is included in a leak, so the punishment for the NHS is that you can't have your hip operation". The ICO is not letting public authorities off the hook for serious infringements of data protection rights (as clearly evidenced in the MPN against Tavistock & Portman for exposing gender reassignment patients' email addresses in a bulk mail), but it does show a more pragmatic and tailored approach.

In addition, the extra-territorial effect of the UK GDPR and the extent to which the ICO may seek to enforce against controllers based overseas, playing the role of "the world's data protection policeman" will be scrutinised in the course of the appeal brought by Clearview AI against the MPN it was issued in May.

Where does this leave us?

Over the course of 2022, the ICO took a number of welcome steps to bring greater certainty to enforcement. The regulator's increasingly targeted approach and its willingness to use the full range of regulatory tools at its

disposal, from MPNs to lower-level reprimands and informal action, challenges the perception that the ICO (as compared to more active European DPAs such as the AEPD in Spain) has little appetite to protect the rights of the individual data subject. The ICO's MPNs may be less headline-grabbing than some across Europe, but these sanctions (rightly) form only part of the story.

In fact, the ICO has adopted a more constructive approach to guiding organisations towards taking control of their own risk-based compliance, ultimately striving to create greater certainty for organisations and individuals by providing a more predictable and well-publicised approach. Key examples of this (and where organisations can look to focus their own risk assessments) are the regulator's commitments to:

I. expand the resources available to organisations to manage their compliance effectively;

II. make decisions by reference to more objective industry standards (consistent with the approach of the FTT in scrutinising the ICO's decisions);

III. acknowledge (and reward) controllers' proactive remediatory and investigatory efforts;

IV. punish organisations that fail to learn from past failings;

V. publish reprimands and data breach investigation details to increase transparency and accountability (consistent with the regulator's ICO25 commitments); and

VI. take a more pragmatic approach to public sector enforcement.

Commissioner Edwards has expressed his confidence in such certainty encouraging flexibility and increased innovation for organisations. However, further clarity will be brought by the long-awaited results of the ICO's consultation on its draft regulatory action policy and statutory guidance.

The ICO and FTT have a dual role in "[helping] businesses to help people". Although regulatory appeals in the FTT will continue to rise while the limits and alternative approaches to enforcement are tested (arguably threatening certainty in the short term), the outcome of such appeals will play a vital role in refining the ICO's approach to enforcement action over time in the same vein as the clarification-by-litigation process across the EU, bringing greater medium/long-term certainty to organisations and ultimately to data subjects seeking to protect their rights.

CONTACT

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

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

ALEX BUCHANAN
ASSOCIATE
T: 020 7090 4045
E: Alex.Buchanan@slaughterandmay.com