PR and penalties: Behind the ICO regulatory strategy

05

Hans Allnutt
Partner
hallnutt@dacbeachcroft.com

Lara Maslowska
Associate
lmaslowska@dacbeachcroft.com

Published in November 2022, the ICO25 plan stated that the ICO aims to provide *"certainty on what the law requires, what represents good practice and* [its] *approach as the* [data protection] *regulator."* As a regulator, it aims to *"intervene proportionately, clearly and only where needed."* Recent criticism suggests that there is a great need for the ICO to intervene with enforcement but is failing to do so.

An open letter issued by civil society organisations, academics and data protection experts called out a 'collapse' in ICO enforcement activity. The letter argues that current ICO enforcement strategies in respect of both public and private sector, deprioritising enforcement, are resulting in more data breaches than the regulations are supposed to prevent. The open letter claims a *"strong correlation between the ICO lack of formal regulatory action and a surge in, sometimes egregious, data breaches in the UK."*

The open letter points to the ICO's interpretation of its duty to promote growth and its softer public sector approach as reasons why the ICO is not enforcing. The open letter recognises the recently concluded ICO call for views on how it investigates infringements, but notes that this stops short of consulting on the ICO's overarching approach to enforcement, claiming that alleged deeper structural failures should be the subject of a public inquiry.

The open letter is scathing in its criticism but is by no means an exceptional critique of the ICO's approach to enforcement. As in the open letter, the public sector approach is often cited as an example of the ICO being a toothless regulator. For the private sector, of those precious few fines that are levied, a disproportionate number are reduced through appeal.

We do see, anecdotally, an effect on an organisations' assessment of risk. In the immediate aftermath of a breach, clients will often ask whether they should expect to receive a fine from the ICO. Irrespective of the circumstances of the breach, the reality is that a fine is statistically unlikely, if not very unlikely. Over 4,500 ransomware incidents have been reported to the ICO since 2019 with a small handful resulting in a fine. It is no surprise that critics, such as the signatories to the open letter, say this has led to organisations underfunding and under-resourcing data protection with a resulting rise in breaches.

If the probability of a fine being issued weighs in favour of a breached organisation, what then determines if the ICO will issue a fine? The ICO has published a range of factors in its Regulatory Action Policy (**RAP**) for all to see. However, this has arguably highlighted a significant level of inconsistency between comparable breaches, with some facing enforcement whilst others do not (ransomware, being one such example). Could the answer lie in one factor, which is notable by its absence in the RAP despite appearing in other policy documents that drive the ICO's objectives; that of the ICO's reputation. Before exploring this further, we delve into some of the examples cited as ICO enforcement inactivity.

The ICO public sector approach

In November 2025, the ICO published an update to the much-discussed public sector approach, clarifying those organisations in scope, and crucially, the circumstances in which a fine may be issued. Introduced in 2022, the public sector approach saw the increased use of the Commissioner's discretion to reduce the impact of fines on public bodies, with the additional aim of improving data protection standards.

Following a two-year trial, and subsequent consultation on its extension, the ICO confirmed the approach would continue, publishing clearer guidance on the circumstances in which a fine may be considered. Only in the 'most egregious' cases will a fine be issued to a public authority, following an assessment of a number of factors including:

- Actual or potential harm to people: physical or bodily harm, psychological harm, economic or financial harm, discrimination, reputational harm or loss of human dignity.
- Intentional or negligent character of the infringement.
- Relevant previous infringements, or recent infringements, by the controller or processor.

The value of any fine will be determined by the application of the five-step approach set in the ICO Data Protection Fining Guidance.

Reflecting on those fines issued since the public sector approach was introduced in June 2022, the £750,000 fine issued to the Police Service of Northern Ireland (**PSNI**) remains the high water mark. The PSNI was fined for exposing the personal information of its entire workforce, with individuals affected leaving the police, taking steps to remove their online presence and expressing concern for not only their safety but that of their families.

The ICO applied its public sector approach in issuing the fine of £750,000 as opposed to a fine of £5.6 million had the usual fining guidance applied. The Information Commissioner commented that PSNI's financial pressures had to be balanced against need to protect people's rights. Clearly to the casual observer, this incident fell within the definition of 'most egregious'.

However, other actions indicate that that further fines for public authority data breaches remain unlikely, even after clarification on what is considered a 'most egregious' case.

The accidental disclosure of personal details of thousands of Afghans who had worked with British forces by the Ministry of Defence (**MoD**) was described as *"unacceptable and should never happen again – the stakes are simply too high."* This sounds not too dissimilar to the ICO's criticism following the PSNI breach, yet the ICO elected to take no regulatory action in this instance. Unsurprisingly, accusations of inconsistency in the ICO's approach were raised.

The Information Commissioner published his comments on that decision, emphasising the wide range of issues in play. It was made clear that the impact of the data breach brought it within the range of a 'most egregious' incident justifying a fine. However, other circumstances justified no further investigation such as the considerable expense to the public purse due to the MoD's prompt response.

The ICO record of the data breach concluded that *"while no formal investigation had been commenced, it was considered that, in line with the ICO public sector approach, further engagement with the MoD would be more effective than seeking to impose additional cost to the tax payer at this time."*

Interestingly, this reason is not included in the factors listed in the RAP which the ICO has stated will determine whether it selects a breach for enforcement. The list is, admittedly, not exhaustive but this response highlights that the ICO's reasons for not acting are potentially unlimited and unknown.

The ICO's messaging appears to indicate that organisations are fortunate to attract leniency and that the policy serves the public good.

However, critics have suggested that the policy is perhaps more self-serving. It has not been lost on a number of organisations facing reprimands that it enables the ICO to avoid the scrutiny, cost and uncertainty of the appeals process that could be followed if a financial sanction were issued. It is not open to an organisation to appeal a reprimand to the First-tier Tribunal, only the unconventional and higher threshold of judicial review. Unsurprisingly, no public organisation has sought to subject a reprimand to judicial review.

The public sector approach therefore arguably allows the ICO to act with a wider licence in actions where an appeal is possible. Indeed, one of the responses to the ICO's consultation on the continued use of the public sector approach suggested "formalising public reprimands as formal enforcement tools in legislation and putting in place an accompanying appeals process." Concern is rising that an ICO reprimand alone does not drive the systemic change the ICO seeks in the public sector.

In support of the public sector approach, the ICO has maintained that reprimands are an effective deterrent, mainly due to the reputational damage and public trust relating to the reprimanded organisation. Reputational consequences, both for the investigated organisation and the ICO, is a lever considered in greater detail below. However, the public sector approach is increasingly being seen as a watering down of enforcement and it is now questionable whether the reputational and public trust damage is that of the ICO's.

This watering down can be seen in some of the more recent reprimand language. Whereas previously the ICO has listed the fine that would have been applied, but for the reprimand, the ICO has taken to using "up to" language. This reflects the fact that if it were to issue a fine, it would have to offer the discounts that it has afforded to other organisations for mitigating circumstances, cooperation, early payment, and general negotiation (see Capita below). One might question the effectiveness of a deterrent if the ICO is having to implement caveats on its own predicted enforcement.

Finally, in another notable reprimand against a public sector organisation, that organisation simply responded with a statement to the effect that it disagreed with the ICO's finding but that it would not use its limited resources to challenge it. Again, an effective appeals process may have enabled a judicial finding of a winner in this particular example but unless and until the ICO adopts this recommendation, the public sector approach will continue have these outcomes.

All fine but no fines?

When it comes to the fines themselves, a review of the ICO's Annual Reports indicates a clear direction of travel for the ICO's enforcement strategy against the private sector.

Between 2021–22 and the present, the ICO's enforcement trends have shifted from a model of occasional but significant financial penalties toward a more collaborative and proportionate approach. While early reports emphasized large monetary penalties for serious breaches, subsequent years saw a marked increase in the use of reprimands and negotiated settlements (as noted for public sector bodies). The ICO has arguably moved towards balancing deterrence with practical compliance support, aligning enforcement with broader objectives of trust, innovation, and proportionality.

The difficulty with this approach in reality is that few breaches impacting large numbers of individuals and/or affecting individuals in significant ways, will be subject to enforcement. Those few matters that do progress to enforcement face potential leniency which undermines their effect.

A recent regulatory fine issued highlights the signals the ICO is sending, and perceptions of leniency even where fines are levied. The outsourcing organisation Capita received a fine of £14 million in October 2023 for failing to ensure the security of personal data during a 2023 data breach. The fine covered Capita's failings as both data controller and processor.

Interestingly, Capita argued it should be treated like its public-sector clients, who would typically expect to receive reprimands instead of fines per the public sector approach. This could reflect a view that the public sector receives enforcement leniency, encouraging Capita to make such submissions as a result.

Nonetheless, Capita successfully achieved a significant reduction on the fine proposed. The proposed £45 million fine was reduced to £14 million after Capita admitted liability, agreed not to appeal, and demonstrated remediation efforts, victim support, and cooperation with regulators.

The significant reductions given to Capita, received in response to the above factors, totalled almost 70%. Notwithstanding the reasons given in the Monetary Penalty Notice, the Commissioner noted the wider consideration of the *"impact a penalty of this nature will have on the growth of the UK economy, and the desirability to promote economic growth, innovation, and competition."* Furthermore, Capita's voluntary admission and commitment to refrain from appealing contributed to the overall context.

Of course, a reduction of 70% is still arguably better than the overturning of a fine altogether. The £7.5 million fine imposed on Clearview AI by the ICO in 2022, one of the first multi-million pound penalties, is now the subject of a further appeal to the Court of Appeal. The most recent ruling from the Upper Tribunal has supported the ICO's initial stance, but the lengthy appeals process reveals vulnerabilities in the ICO's enforcement system, especially when dealing with matters involving extraterritorial jurisdiction.

Aspect	Public Sector	Private Sector
Policy Basis	Public Sector Approach (permanent since Dec 2024)	Standard enforcement under UK GDPR and PECR
Primary Enforcement Tools	Reprimands and Enforcement Notices Corrective action plans	- Monetary Penalties (fines) - Enforcement Notices - Reprimands
Use of Fines	Rare – reserved for 'egregious' cases. Hypothetical fine amount now published for transparency (Post Office)	Common for serious breaches Fines calculated based on severity and turnover
Transparency	ICO may publish what amount the fine would have been "up to", had a fine been levied	Actual fine amounts published, including details of reductions
Impact on Budgets	Designed to avoid diverting taxpayer funds from essential services	No special consideration – fines intended as a deterrent
Scope	Government departments, local authorities, NHS bodies	All private organisations, including charities and social enterprises
Criticism	Concerns about reduced deterrent effect and accountability	Criticism usually relates to proportionality of fines

Reputation, reputation, reputation

One would be forgiven for thinking that the ICO is more frequently explaining why it has not enforced a fine, or reduced it, than pursuing enforcement. Further, one might ask what drives the ICO to decide take enforcement action in one breach over another.

As noted above, the RAP includes a range of factors that the ICO will consider when deciding to take enforcement action. This is a non-inclusive list and, also noted above, the ICO has not shied away from citing previously unpublished factors in its enforcement decision making.

One further factor, however, that isn't immediately obvious is the ICO's own reputation and public relations image.

In the ICO's former regulatory action policy of 2013, the ICO was more candid in including the impact on its own reputation within the criteria for deciding whether to take enforcement. The criteria included:

> ***"What is the risk to the credibility of the law or to our reputation and influence of taking or not taking action as a reputational factor when considering enforcement."***

More recently, examples are a little harder to find although the ICO's own disclosures of internal ICO messaging between ICO senior management following the MoD Afghan incident, are instructive:

> ***"There is a reputational risk we face if we can't sufficiently explain why we took the course of action we took (or in this case - didn't take)."***

In some ways, the PR influence on enforcement is not surprising. Following a well publicised breach in the mainstream media, public attention is directed at the ICO for comment. Public expectations of the ICO will be higher in a publicised breach compared to a breach that has not garnered wider publicity.

That being said, it may not be fully appreciated by organisations that a factor in whether it will face enforcement could be the level of publicity and the ICO's own reputation as opposed to the pure technicalities of the breach itself.

The 'new' Information Commission, will it prompt a change in approach?

The Data (Use and Access) Act (**DUAA**) introduced a number of significant changes to the structure and operation of the ICO. The ICO as it is currently structured is to be abolished and replaced with the Information Commission. At the time of writing, the changes (identified as Stage 4 of the commencement provisions) are expected to take effect from early 2026.

The change moves the regulator to a body corporate with a statutory board with a chair and chief executive. The Information Commissioner responded positively to these changes, stating the *"refreshed governance arrangements will maintain our independence and enhance our accountability."*

The DUAA also provides the Information Commission with additional powers in respect of a breach of the Privacy and Electronic Communications Regulations 2003 (**PECR**) as provided under the UK GDPR or Data Protection Act 2018. However, the question remains whether this organisational change will prompt any change in the ICO's approach to either public or private sector enforcement.

This is where politics and performance may play their role. The DUAA introduces a new principal objective for the Information Commissioner as follows:

> ***(a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and***
>
> ***(b) to promote public trust and confidence in the processing of personal data.***

As well as the principal objective, the Information Commissioner must also have regard to 'other matters' such as promoting innovation, competition, safeguarding public and national security, children's interests, and the importance of dealing with criminal offences.

Against this backdrop, sections 95 and 102 of the DUAA introduces reporting requirements on the Commissioner:

1. **To prepare and publish an annual analysis of the Commissioner's performance using key performance indicators.**
2. **To prepare and publish an annual report on UK GDPR investigations including details on the number of investigations undertaken during the reporting period, the acts or omissions compelling the investigations, any enforcement powers exercised, the duration of investigations and details of the types of outcomes.**

Of course, the ICO already issues Annual Reports as discussed above, but the new reporting requirements are a change from purely operational reporting to strategic accountability. It should be noted that the DUAA removed provisions previously contained in the Data Protection and Digital Information Bill. This would have had the Information Commissioner consider a statement issued by the relevant Secretary of State, which would have outlined the government's strategic priorities with respect to data protection.

That proposal raised concerns about the independence of the ICO both in the UK and EU; unsurprisingly the proposal was withdrawn. Nonetheless, the requirements on the Commissioner to prepare performance and investigation reports may impact the enforcement approach going forward.

More detailed public reporting may make the ICO's regulatory priorities and sector-specific concerns more transparent for organisations. The requirements on the Information Commissioner to take account of 'other matters' may also mean that enforcement focus may shift towards areas such as children's privacy and industries with a high level of innovation such as AI.

At present, fines for breaches of the UK GDPR have, arguably, lost much of their impact due to how infrequently they are imposed, the amounts involved, and challenges with enforcement. The ICO still appears hesitant to fully exercise its authority to issue financial penalties against both public sector bodies and private companies.

It is unclear if the DUAA reporting requirements will affect the ICO's approach. Overall, the remit of the Information Commissioner to consider economic factors such as innovation and competition, alongside its traditional focus on data protection with an undercurrent of its own public reputation, suggests there will continue to be a nuanced regulatory approach from the ICO.