SLAUGHTER AND MAY/

March 2026

CYBER ENFORCEMENT – WHEN AN INCIDENT IS JUST THE TIP OF THE ICEBERG

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 144 (March 2026)

2025 revealed a shift in enforcement approach by the Information Commissioner's Office (**ICO**) when compared to the previous year. We saw a decrease in overall enforcement action, but a much higher proportion of those actions taken against organisations in the private sector and a significant focus on cyber and data security failings. This comes amid high-profile cyber-attacks against major UK retailers and manufacturers including M&S, Co-op and JLR, increased engagement by the government on cyber-resilience in corporate Britain as well as recent signs of renewed follow-on claims after breaches. It is clearer than ever that organisations must ensure robust security measures are in place and adapt their data handling, broader cyber-resilience, and management of contractual risk allocation accordingly.

2025 UK GDPR enforcement themes compared to 2024

What the figures say

In terms of GDPR fines, the ICO issued six monetary penalty notices, up from just two in 2024. These totalled over £20m of fines, with the highest fines issued against the *Capita Group* (**Capita**) (£14m), *Advanced Computer Software* (**Advanced**) (£3.07m), *23andMe* (£2.31m), *LastPass* (£1.23m), and *DPP Law* (£60k). Interestingly, these represented a higher proportion of the overall monetary penalties issued by the ICO than in 2024, demonstrating an increased focus on GDPR and data protection issues over e-privacy and marketing. The average amount fined also increased in 2025 – from around £380k in 2024 to just under £3m in 2025.

Learnings from the 2025 ICO fines

The key theme for GDPR fines in 2025 was security and integrity failings – all the fines mentioned above were issued following cyber-attacks. The only other GDPR fine the ICO issued was to a charity, *Birthlink*, in respect of the deletion of irreplaceable personal records relating to birth parents and family history. 2025 therefore provides numerous valuable lessons for controllers and processors.

Each case of course presented unique facts, but several common themes emerged:

- **Sensitivity and volume of the data.** The ICO's fines targeted cyber and data security breaches where the affected data was sensitive data (including special category data), and/or where it related to a large number of individuals. The compromised data in these cyber fines spanned genetic data, NHS patient health data, home entry details for individuals receiving care at home, special category data of pension scheme members and sensitive (and privileged) legal case data. In each case the ICO emphasised the potential harm to data subjects – and that "potential" harm is enough to form the basis for enforcement.

  In terms of volume, *Capita* had the highest number of affected individuals (approx. 6.7m) and *DPP Law* had the lowest (791), with the others ranging from between around 80,000 and 1.6m. However, even though *DPP Law* only involved 791 individuals, the ICO commented that this is not an insignificant number where highly sensitive data was involved (e.g. relating to court proceedings and legal advice to clients). This highlights the need to ensure data subject risk assessments are more nuanced (and less quantitative) going forward.

- **No second chances.** The ICO expects organisations to learn from past enforcement action - even more so when an issue has been highlighted in multiple penalty notices. For example, implementing multi-factor authentication (**MFA**) across the business should now be considered essential, as it was a factor in a number of the fines above, including *23andMe* and *Advanced*.

Other common security failures identified by the ICO included:

- insufficient network segmentation permitting threat actors to move laterally through networks and autonomously escalate their own privileges - in *Capita*, for example, the ICO found that, prior to the incident, Active Directory tiering (a storage management technique) was not in place despite there being "*clear longstanding guidance*" from Microsoft and NCSC on Active Directory tiering and Privileged Access Management;

- inadequate security monitoring and alert response leading to delays in breach detection. For example, the ICO found in *23andMe* that indicators of credential stuffing (automated cyberattack that inserts stolen usernames and passwords into the system's login fields) were not identified and messages from a potential threat actor were not prioritised appropriately. In *Capita*, despite there being controls to detect malware and issue subsequent alerts, appropriate measures were not in place to respond in time to "*prevent unnecessary and avoidable harm*"; and

- failure to secure legacy systems and manage vulnerabilities, particularly around patching and vulnerability scanning (an automated IT process that analyses computers, servers, and applications to identify missing security updates, bugs etc). The ICO is clear that it expects organisations to address known vulnerabilities (for example, patch vulnerabilities that were not updated in *Advanced*). Large organisations should also ensure that they share lessons across the business - for example, learnings gained from penetration testing in one part of *Capita's* organisation should have been shared internally.

The main lesson here is that organisations should keep a close eye on the detailed security measures the ICO has deemed inadequate in recent enforcement activity. They can then conduct audits to identify any similarities or equivalent issues within their own processes and practices and those of their key suppliers or processors. Unsurprisingly, known and avoidable vulnerabilities should be prioritised.

- **Technical expectations, standards and guidance.** The ICO has made clear that organisations should meet technical expectations through compliance with their own policies, guidance and industry standards (including ICO and NCSC guidance, OWASP and ISO 27001). For example, the ICO found in *LastPass* that, despite the organisation being a leading provider of password management services, it had failed to adhere to both ICO and NCSC guidance regarding employee use of personal devices to connect to essential networks, identifying that this was a key systems failure exploited by the threat actor.

- **Suppliers can be held liable for security failures.** The *Capita* and *Advanced* decisions demonstrate that, while enforcement action has traditionally been taken against the data controller, the ICO is prepared to enforce against processors directly. This reflects the reality that processors often have primary responsibility for securing the environments and systems they operate for corporate customers. That does not, however, mean that controllers are now off-the-hook. The decision in *DPP Law* demonstrates that controllers cannot delegate security responsibility to third-party suppliers, even where the supplier has created and maintained critical infrastructure components, and so controllers will need to maintain visibility and control over the access such suppliers have to sensitive personal data.

  Organisations should review their due diligence processes for new suppliers and monitor existing suppliers. This means processor contracts must be suitably robust including having appropriate audit rights.

- **How to handle ICO engagement and investigation.** As well as providing security advice, the fines provide useful guidance on how organisations can improve their position in the context of an ICO investigation following a cyber-incident. For example:

  - The ICO may take mitigating factors into account when making reductions to fines, but this is only likely to be available where an organisation demonstrates greater accountability overall. This includes proactively facilitating and assisting the ICO in its investigations. Steps like engaging third-party dark web monitoring services, setting up a dedicated call centre for affected individuals, engaging with other regulators (e.g. voluntarily informing the NCSC) and providing a 12-month Experian credit monitoring facility were also considered favourably in *Capita*.

  - Early admissions, voluntary settlement and agreement not to appeal were all steps that contributed to a discount in the *Advanced* fine. Perhaps learning from earlier cases which were challenged, the ICO's more focused approach to enforcement seems to be yielding results in

providing certainty both for the specific organisation penalised and businesses more generally looking for guidance.

Conversely, the notices also highlight behaviour the ICO will treat neutrally, or even negatively (thereby increasing fines). For example:

- The ICO was critical of the degree of cooperation in the *Capita* action on several grounds, including responses to Information Notices that could have been more detailed and failing to provide additional information requested by the ICO regarding civil claims.

- Cooperation with the ICO in its investigations was typically treated as a neutral factor.

- Larger, better-resourced organisations, particularly those where processing sensitive data is a core commercial activity, will bear more responsibility for securing personal data. Failure to do so is likely to be considered an aggravating factor by the ICO (as it was in, for example, *Capita, Advanced* and *23andMe*).

- Multiple extension requests, delaying key disclosure and incomplete or deficient reporting/responses can be considered aggravating factors in *23andMe*. However, the ICO may take 'exceptional circumstances' into account where this happens. For example, in *23andMe* the fact that they faced extreme financial and commercial challenges during the investigation meant the ICO treated these factors as neutral rather than aggravating factors.

- While not expressly mentioned in the 2025 fines, the ICO has previously been clear that paying ransoms to mitigate the risk to data subjects will not have a mitigatory effect. As well as advising against ransom payments more generally, the message for organisations is that the same funds would have been better invested in data and security infrastructure.

Looking ahead, the key lesson seems to be that the ICO is taking a more robust approach to the investigation process while being risk-focused on the substance of its investigations. This may include collaborative efforts across borders (as seen in their joint investigation with Canada's Privacy Commissioner in *23andMe*), which may result in better informed regulators and potentially more effective (and intrusive) investigation practices. With the ICO's enhanced investigatory powers under the Data (Use and Access) Act 2025 (**the DUA Act**) (see below), organisations should resource response preparation appropriately and be prepared to engage in interviews, including at the executive level. There will be increasing value in documenting data security decisions and having a clear reporting line for engagement with the ICO.

Outlook for 2026: convergence of ICO and UK Government cyber focus, and the potential return of follow-on damages claims

When looking ahead, organisations are not only facing a regulator ready to act decisively on cyber breaches – they are also navigating an escalating threat environment (the NCSC reported a 50% increase in highly significant cyber incidents in 2025 from 2024), strengthened ICO powers, and the possible return of mass-claims risk.

Strengthened ICO powers

The range of tools available to (and obligations on) the ICO is expanding:

- The Cyber Security and Resilience Bill (**CSRB**) will update the UK's current NIS regime, which is designed to protect the network and information systems of those in critical services. It will also expand the ICO's existing remit under the NIS regime and apply to a broader range of third-party providers including managed service providers. The ICO has voiced its support for the CSRB, but it is keen to have further engagement and guidance from the government. Alongside other initiatives, such as the Home Office consultation on ransomware last year, this is all showing a clear strategy from the government to strengthen the UK's cybersecurity resilience.

- In addition, the ICO has just gained enhanced powers under the DUA Act. These include requests for preparation of technical reports by approved persons (for example, independent third parties with the requisite expertise) and compelled witness interviews. It is, however, expected that the latter will be reserved for the more difficult cases, for example, where it is difficult to gather information through other means or if there is a refusal to attend a voluntary interview.

Mass claims risk?

The very recent decision in *Neil Spurgeon & Ors v Capita PLC* (**the Capita Ruling**) suggests that the decision in *Lloyd v Google* did not mark the end of mass claims following data incidents and enforcement activity. The Capita Ruling, while arguably only a preliminary ruling and not a guide to the merits of the underlying claim suggests that there may be a more workable (and funder attractive)

"follow-on" damages route. That said, there are still likely significant obstacles for mass breach claims in the UK. Individual assessment of damages may still be required by the Court in respect of each claimant, but the absence of a claimant-specific information does not seem to be enough to strike out such claims at an early stage.

Comment

The overall message for 2026 is that the potential fall-out from cyber incidents, whether regulatory, litigious or reputational, remains significant and organisations should prioritise cyber risk mitigation. However, from an ICO enforcement perspective the picture is perhaps a little more nuanced. The ICO is likely to continue prioritising cases where there is the greatest risk of harm but, as we have seen in a number of cases, is unlikely to take enforcement action where organisations can demonstrate genuine and reasonable efforts to comply. The ICO may also be finding it more challenging to enforce in other areas such as AI, in part due to governmental pressure and its new statutory duty to support innovation.

Having said that, to drive compliance the ICO must retain its position as a regulator with teeth. It was criticised by privacy lobbyists at the end of last year for shying away from enforcement activity in general, and in particular not formally investigating the Ministry of Defence in relation to the leaking of data relating to Afghans fleeing the Taliban.

Against this backdrop, cyber incidents that occur as a result of basic and preventable security failings or that involve large volumes of sensitive data (and possibly those under the CSRB in due course) are an easy target for enforcement action, and arguably harder to appeal. While a certain degree of cyber risk will always be present and unavoidable, the cost of handing 'easy wins' to the regulator (or circling litigation funders or claimants) is only going up.

CONTACT

RICHARD JEENS
PARTNER
T: 020 7090 5281
E: richard.jeens@slaughterandmay.com

WILLIAM DOYLE
ASSOCIATE
T: 020 7090 4736
E: william.doyle@slaughterandmay.com