Who's afraid of the Big Bad Wolf? UK data regulator huffs and puffs but most houses are still standing

Hans Allnutt
Partner
T: +44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com

Lara Maslowska
Associate
T: +44 (0) 20 7894 6389
lmaslowska@dacbeachcroft.com

Ten years ago, UK organisations were staring down the barrel of the GDPR which was promising astronomical levels of sanctions for cyber security and data protection breaches. With regulatory fines of up to 4% of annual worldwide turnover or EUR20 million, organisations who failed to meet the requirements of the GDPR could face punishing levels of financial penalties in the event of non-compliance. For those industries with thin profit margins, the prospect of having to handover 4% of turnover for their breach of the GDPR, would mean an existential threat.

Tom Draper, Managing Director of cyber insurer Coalition and twenty-year veteran of the cyber insurance market recalls:

> *"The introduction of GDPR was a game-changer in the demand for cyber insurance from the United States and into Europe. The previously unseen levels of fines for cyber security breaches focussed potential policyholders on these new risks and drove up enquiries for insurance cover, even though fines would only be insurable in certain circumstances."*

The same could be said for cyber and data privacy advocates. The world had embraced both the internet revolution and big data age, but organisational recognition of the responsibilities for securing connected data and privacy rights had not kept pace. The GDPR would finally place cyber security and data privacy risks at the very top of the corporate risk agenda.

Of course, from a regulatory and public policy perspective, the threat of fines and penalties was, and still is, presented as an unnecessary 'stick' because organisations should want to see compliance as the 'carrot'. Organisations should want to comply with the rules and requirements irrespective of the penalties for non-compliance. Such a perspective is a little more than rose-tinted: using a driving analogy, more responsible drivers will observe speed limits, but nothing keeps less responsible drivers within the law better than the prospect of a hefty fine.

Reality bites

The reality of GDPR fines in the UK is that they have arguably become somewhat of a damp squib, for reasons of frequency, quantum and enforceability. So much so that the UK Information Commissioner's Office (ICO) itself appears to have become reluctant to use the financial powers available to it.

It took the ICO over 18 months to issue the first GDPR fine, levying a sum of £275,000 against Doorstep Dispensaree on 20 December 2019 for leaving copies of sensitive patient data in an unsecure courtyard. The company appealed to the First-tier Tribunal who upheld the fine but reduced the amount to £94,000 on the basis that less data was involved than the ICO believed. Doorstep Dispensaree further appealed, unsuccessfully, to Upper Tribunal and Court of Appeal. The Court of Appeal dismissed this latest appeal in December 2024, and whilst the ICO was successful it was nonetheless caught up in over five years of litigation as a result of its first GDPR fine.

The UK's largest GDPR fine was issued to British Airways in relation to the attack they discovered in September 2018. Perhaps more notable than the fine itself was that it the ICO initially intended to levy a fine of £183.4m representing 1.5% of the business's 2017 global turnover. Following submissions from the business, the ICO reduced the fine to £20m in October 2020, a whopping 89% reduction.

At the date of writing, the ICO has issued 15 GDPR fines since the powers came into force. Of these, 4 fines have been made against publicly funded organisations that were unlikely to ever have appealed the ICO's decision. Of the remaining 11:

- Doorstep Dispensaree achieved a 66% reduction of the fine despite subsequent efforts to overturn the ICO decision being unsuccessful.
- British Airways achieved an 89% reduction of the fine at the submissions stage.
- Clearview AI Inc was fined £7.5m in May 2022 but successfully appealed the imposition of the fine at the First-tier Tribunal. The ICO was refused permission to appeal further, following which the ICO renewed its application for permission to appeal in October 2024.
- One further fine which remains under appeal at the First-tier Tribunal.

Of course, it would be remiss not to mention recent news from August 2024, when the ICO announced its provisional decision to issue a £6.09m fine to Advanced Computer Software Group Limited following a ransomware attack which impacted the personal information of over 80,000 people and resulted in disruption to critical services, such as NHS111.

This provisional decision represented the first enforcement action taken against a data processor.

We have published further thought leadership which includes analysis of the provisional decision in the Advanced case, including consideration of whether the outcome should be viewed as a one-off based on specific circumstances or the establishment of future enforcement trends against data processors. As matters stand, the final outcome in the Advanced case remains open.

Difficulty in issuing fines that stick is not new. Pre-GDPR decisions by the ICO have faced difficulty too. In 2020, the ICO issued a £500,000 fine against DSG Retail (the maximum level fine it was able to levy under the previous regime, Data Protection Act 1998). This was reduced to £250,000 by the First-tier Tribunal in 2022, and overturned entirely by the Upper Tribunal in September 2024 on the basis that payment card numbers were not personal data and therefore were outside the scope of the legislation.

Whilst we await the outcome of many of these appeals, the current status quo is that it is not uncommon for the ICO to get the law wrong when exercising its enforcement powers, arguably the most important of its legislative functions.

However, it is not only the sharp end of the arrow that has blunted, but the limited number of arrows that are being shot.

In the case of ransomware, arguably the most societally impactful type of cyber attack, the ICO's own statistics note that there have been over 3,500 ransomware incidents reported to them since the GDPR came into force. However, at the time of writing, only two ransomware attacks have resulted in GDPR fines (the Advanced fine remaining provisional at the time of writing).

Of course, quite rightly, not all notified ransomware attacks should result in a fine but from our own experience and publicly available information, those that have resulted in a fine are not too dissimilar to other breaches which have not been interrogated by the ICO.

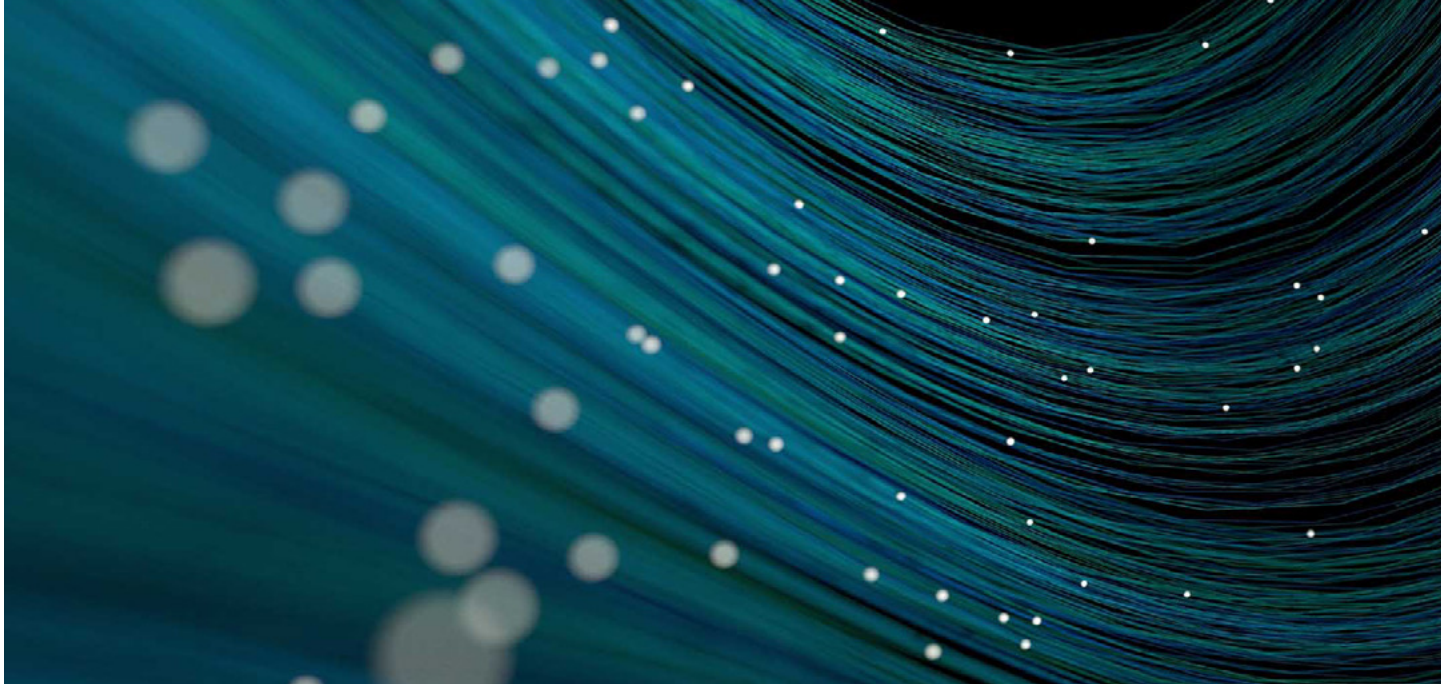
This upshot is a less than level playing field. When it comes to cyber security, one would expect that those who build their houses out of sticks ought to face the consequences when the Big Bad Wolf comes blowing, whereas those who have invested in bricks ought to reap the investment benefit and avoid regulatory scrutiny. Unfortunately, the statistics paint a different picture which even the ICO appears to acknowledge. John Edwards (the current Information Commissioner) told The Times on 18 November 2024 that he didn't feel that the ICO should be using fines to keep Big Tech companies in check:

> *"I don't believe that the quantum or volume of fines is a proxy for impact. You know, they get a lot of headlines. It's easy to compile league tables but I actually don't believe that that approach is necessarily the one that has the greatest impact… Now, if instead of [choosing alternatives], I fine Meta EUR10 billion for failing to do those things: a) they wouldn't make the changes that we've asked; b) they would take us to court and consume huge resources. And we would be in court for four, five or six years."*

This builds upon comments made at the ICO's annual Data Protection Practitioner's conference in October 2024 indicating a shift away from enforcement action taking many years to an approach that goes after 'quick wins':

> *"When I came here, I was seeing files come across my desk and getting briefed on enforcement matters and I would ask 'when did this happen' and the answer was usually four, five or more years ago and I said 'you know, this is not good enough, we cannot be delivering change in a fast paced digital environment and getting the lessons learnt if we are taking five years to investigate where things have gone wrong…..so we have to be more agile."*

Edwards went onto cite the £750,000 fine issued to the Police Service of Northern Ireland within 8 months of the breach, a breach where the PSNI was defenceless, published details of its entire workforce and where, we would suggest, the PSNI have a case to answer.



ICO's aversion to litigation

When one looks at the fines that have been appealed, they all relate to private sector organisations rather than the public sector. Where the ICO has been challenged, its original decisions have not had a good track record. It is not a strong look for a regulator to be found to have got the law wrong.

The picture that seems to be emerging is that, rather than blowing down the straw houses of those organisations that do not have appropriate security measures in place, the ICO is going after those organisations that are less likely to lawyer up and contest its actions.

Casual observers could understandably sympathise with a publicly funded regulator that is outgunned when it comes to legal spend. Indeed, the ICO argued for many years that it should be able to use some of the monetary penalties that it levied to fund its future legal bills of enforcement. In June 2022, the ICO reached an agreement with its government department to retain up to £7.5m of the fines levied per year in in order to fund its further litigation costs.

A Freedom of Information Act Request submitted to the ICO by one of our lawyers in a personal capacity reveals that the largely held expectation that the ICO would similarly 'tool up' itself with external lawyers in a bid to make its decisions stick has not come to pass.

It is notable that no funds were retained in relation to GDPR fines in either 2022/23 or 2023/24. This may be, in part, due to the ICO's inability to get the big fines to stick. As reported in the ICO's 2023/24 Annual Report, £25.9m in penalties were still uncollected of which £21.6m related to those under appeal.

The only retained funds relate to fines made under the Privacy & Electronic Communications Regulations, rather than the GDPR. These are typically fines that are levied for unlawful marketing and spam callers. £1.648m in 2022/23 and £3.895m in 2023/24 were retained respectively. These amounts are not insignificant and could provide a significant fighting fund for the ICO utilise by engaging its own external lawyers. However, instead, the majority of the funds have been used to pay for ICO staff costs, (£2.265m of the £3.895m in 2023/24 and £1.308m of the £1.648m in 2022/23). Of the £5.543m retained, therefore, roughly £2m has been spent on external legal costs with the remaining £3.5m being spent on internal ICO staff costs.

With the clear waning appetite of the ICO to issue large GDPR fines to big tech companies and a clear desire to avoid years of litigation, the status quo does not appear to be changing any time soon and the litigation fund could be a missed opportunity.
One answer for the ICO was to switch to an alternative strategy of naming and shaming through the use of reprimands, rather than fines. A reprimand is an alternative enforcement action which sees the ICO publicly finding a breach of GDPR with no financial consequences. A reprimand is not subject to the same appeal process that a final sanction would be, limiting the prospect of an appeal regarding the ICO's decision. Some commentators have described it as a 'watering down' of enforcement although one can see a meaningful strategy of regulatory statements that an organisation has come up short when otherwise there would be no sanction at all. However, when looking at the last 15 reprimands issued, almost all of them have been issued against public sector organisations - so it appears again to be the case that private sector enforcement has the ICO running scared.

No longer the poster child?

Fines under the GDPR were the poster child that promised to ensure that organisations invested in cyber security and privacy compliance. However, the statistical evidence and recent commentary suggests an ICO fine is not a realistic risk to UK organisations, save for in very limited circumstances. This is in contrast to the approach being taken by EU supervisory authorities and we consider this divergence in greater detail in our accompanying piece.

So, if regulatory enforcement is not the big bad wolf that is going to ensure that organisations take data protection and cyber security seriously, what might that be?

It is arguably other risk factors, such as litigation or actions taken by other regulators, that are keeping organisations in legal check.

Tom Draper's view is that, for a multinational conglomerate, it is EU competition and anti-trust regulators that present a greater fear at board level discussions:

> *"For large global companies, GDPR enforcement levels have been far lower than the penalties associated with EU tax policy or competition concerns."*

Beyond that and looking in particular across the Atlantic to the United States, the threat of class actions and volume litigation is generating concern. Numbers of cyber security, data breach and privacy related actions in the UK has grown significantly since the advent of GDPR. Whilst common law principles were already expanding, the GDPR simplified measures by entitling claimants to claim for their distress alone caused by a data breach.

There remains the prospect of compensation rights expanding further including whether damages are permissible for a simple breach of the GDPR and whether the burden of proof in demonstrating adequate security rests with the company rather than the data subject. Although it could be argued that the data breach claims landscape is trending in favour of defendants compared to the initial post-GDPR period, developments in these areas should be closely followed in the coming year. We have specifically discussed the data breach claim landscape heading into 2025 in our accompanying piece, including the significant litigation costs exposure that can accompany a data breach class action, and the risks associated with the use of the 'omnibus' claim form.

Full list of references available upon request