Processor liability: the winds of change or an isolated storm?

Christopher Air
Partner
T: +44 (0) 161 934 3167
cair@dacbeachcroft.com

Susanna Read
Senior Associate
T: +44 (0) 117 918 2334
sread@dacbeachcroft.com

Last year, for the very first time, the UK Information Commissioner's Office (ICO) indicated its intention to take serious enforcement action against a processor. The fact that this comes some six years after the implementation of the GDPR is itself of note. Back in May 2018, processors found themselves with direct obligations under data protection law for the first time. At that time, there was a general sense that this would change the liability landscape.

However, since then, processors in the UK could have been forgiven for increasingly assuming that, unless they went rogue or otherwise acted completely against a controller's instructions, they were almost immune from enforcement action being pursued directly by the ICO. It seemed that the previous status quo of the buck stopping with the controller was largely maintained.

Across the EU however, enforcement actions against processors are not unprecedented by any means. For instance, in 2022 a Romanian regulator ANS PCDP (or the National Supervisory Authority for the Processing of Personal Data) fined Wens Experience SRL (a processor) for appointing a sub-processor without requisite permission from its controller, which was a direct breach of the processor's obligation under paragraph 2 of Art 28 of the EU General Data Protection Regulation (EU GDPR). The fine itself was only for EUR1,500, however. There have been other instances, including in Italy for example – but generally such action constitutes a very small portion of overall supervisory authority enforcement – with well over 90% of enforcement action being taken against controllers.

In 2024, for the first time, the ICO indicated its intention to consider taking serious enforcement action against a data processor. This action theoretically represents a marked sea change, not only in terms of enforcement measures against data processors, but also potentially the ICO's general regulatory approach, as substantiated by our accompanying piece on the regulator's overall enforcement strategy.

In August 2024, the ICO announced its provisional decision to issue a £6.09m fine to processor Advanced Computer Software Group Ltd ('Advanced'). Advanced is a software provider which delivers solutions to NHS and social care organisations. In August 2022 it suffered a ransomware attack, which impacted the personal data of 82,946 individuals and resulted in disruption to critical services, such as NHS 111. The personal data exfiltrated by hackers included phone numbers and medical records, as well as details of how to gain entry to the homes of 890 individuals who were receiving care at home. On the face of it, this incident sounds like any other security breach related attack and there was nothing to suggest that Advanced was acting outside of its role as a processor, or directly refusing to comply with the instructions of its controller customers. Indeed, this appears to be a fairly standard security failure by the processor – so why have Advanced been singled out and is this fair, given that processors have historically been let off the hook for more egregious breaches?

It is important to note that this is the ICO's provisional decision, not a definitive finding on liability nor the amount of any penalty. Nonetheless, it is worth pausing to reflect on the significance of this announcement and consider what direction the ICO may take as regards to future enforcement action against processors.

Is the Advanced provisional decision a sign of things to come? Will 2025 be the year in which we see the ICO increasingly taking enforcement action against processors? Or is this an anomaly based on a set of specific facts?

The winds of change?

Several commentators are now expecting the Advanced case to mark the start of a new approach by the ICO, clamping down on inexcusable basic security failings in supply chains affecting critical industries such as the NHS.

Zero tolerance approach to no multi-factor authentication

As readers will be aware, processors have a number of direct obligations under the UK GDPR, including:

- to only process personal data under a binding contract and in accordance with a controller's instructions, unless otherwise required by law; and
- to implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

The second requirement, stemming from Article 32 UK GDPR, is the key security obligation on processors. This is intentionally non-prescriptive – the ICO's own guidance on data security is non-exhaustive – specifically because the requirement is for organisations to keep pace with technological threats and other developments and put in place measures which are proportionate to and take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

In a statement regarding the Advanced matter, John Edwards (the UK Information Commissioner) stated:

> *"For an organisation trusted to handle a significant volume of sensitive and special category data, we have provisionally found serious failings in its approach to information security prior to this incident. Despite already installing measures on its corporate systems, our provisional finding is that Advanced failed to keep its healthcare systems secure. We expect all organisations to take fundamental steps to secure their systems, such as regularly checking for vulnerabilities, implementing multi-factor authentication and keeping systems up to date with the latest security patches."*

It is notable that Advanced were criticised for failing to put in place basic security measures, such as multi-factor authentication (MFA) to protect their systems and data. The National Cyber Security Centre and ICO have published various guidance notes, highlighting the importance of MFA for some time now. The above is a clear statement from Edwards, indicating that the ICO will no longer show sympathy to those who ignore its guidance or fail to ensure the most basic of security measures.

We therefore anticipate that the ICO will increasingly be adopting a tougher stance on supply chain participants (processors and sub-processors) who fail to put in place basic security measures, particularly where such failings jeopardise special category data in the supply chain for many controller customers in critically important sectors.

It is unclear whether Advanced were contractually required to use MFA, or whether the ICO expected this more as industry standard – either way, as it was delivering IT solutions to many NHS and social care customers, and therefore handling not only large amounts of personal data, but special category data, MFA should have been in place as standard.

Gavin Wood, CEO at CyberLab said that:

"Multi-Factor Authentication (MFA) is non-negotiable in any business cybersecurity program. It effectively prevents phishing, social engineering, and credential-based attacks. Using MFA can block over 99% of account compromise attempts, making it essential for safeguarding your data and business.

At CyberLab, we recommend activating phishing-resistant Multi-Factor Authentication to add an extra layer of security. It requires multiple verification methods to access your organisation's systems, reducing the risk of unauthorised access even if passwords are compromised."

Wider focus on supply chain risks

It is worth also considering whether wider factors will increasingly influence the ICO's stance – in particular, the need to evolve UK cyber security laws. There is a sense that the UK is in danger of lagging behind in terms of cyber legislation and needs to adopt a tougher enforcement approach, particularly in terms of supply chain vulnerabilities in critical sectors. The Advanced incident, and others like it (for example, Capita in March 2024, and Synnovis in June 2024) were all attacks on the supply chains underpinning critical parts of the UK economy.

This issue is particularly relevant when compared to legislation being implemented in the EU which aims to strengthen operational resilience in Member States, such as the:

- NIS2 Directive which strengthens the power of regulators, as well as imposes requirements relating to supply chain security, accountability of company management for risk-management compliance and incident reporting obligations; and
- Digital Operational Resilience Act which focusses on digital operational resilience of financial services industry organisations and their IT supply chains.

As we have noted in our other pieces in this collection, these are two important pieces of legislation aimed at bolstering cyber security and resilience across key sectors. The UK has not adopted these laws, but the new Labour government has announced its new Cyber Security and Resilience Bill, which aims to plug the gaps in terms of vulnerabilities across key sectors and recognises that supply chains are critically important in protecting the UK from further attacks. At the time of writing, we understand that the new Bill will be placed before Parliament at some point in 2025 and will amend the existing Network and Information Systems Regulation 2018 by:

- expanding the remit of the regulation to protect more digital services and supply chains;
- putting regulators on a strong footing to ensure essential cyber safety measures are being implemented; and
- mandating increased incident reporting to give government better data on cyber-attacks.

Similar attacks likely to involve similar action

The Synnovis incident on 3 June 2024, involved another ransomware cyber-attack against an IT supplier. Synnovis is an organisation providing services to the NHS, specifically relating to pathology services using blood samples. The immediate headlines from the Synnovis attack highlighted the concerning impact on patients, including 119 cases of patient harm arising from the attack, including at least five cases of moderate harm. NHS policy defines 'moderate harm' as including affecting the success of treatment but not meeting the criteria for reduced life expectancy or accelerated disability. Focus was also directed at suggestions that the hackers had stolen patient data.

Beverley Bryant (Chief Digital Information Officer at Guy's and St Thomas' NHS Foundation Trust and King's College Hospitals NHS Foundation Trust) described the three months of disruption after the cyber-attack as *"unbelievable"*. She noted that if MFA had been in place "the cyber-attack may not have happened." It therefore appears, in a similar fact pattern to the Advanced cyber-attack, a lack of MFA may be a critical vulnerability.

In the immediate aftermath of the Synnovis attack, the ICO published a short statement stating it was *"making enquiries"* into the matter; we anticipate that Synnovis may well be in the ICO's cross hairs in a similar fashion to Advanced.

An isolated storm?

A security failure, in particular, a failure to put in place MFA, is not just a failure by a processor to comply with its security obligations under Article 32 of the UK GDPR, it is also a failure by the relevant controller to comply with the same obligations, as well as the security principle under Article 5. Furthermore, controllers are required to ensure that when appointing processors:

> ***"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."***

Therefore, controllers are required to perform suitable due diligence on their processors, to ensure that their data will be in safe hands. This is not just a one-off obligation that occurs before the processor is appointed, but a continuous process requiring consistent review and assessment throughout the duration of the relationship between the relevant controller and processor. For instance, controllers have rights to audit their processors to determine ongoing compliance. In reality however, audit rights are rarely exercised – which raises a question regarding the accuracy, frequency and completeness of the information controllers receive from their processors, and how diligently this is proactively monitored, particularly once the procurement process is complete and the IT systems have gone live.

One must ask, why did none of those controllers notice the basic failure by Advanced and potentially Synnovis to put in place MFA – either through due diligence, reporting, regular reviews or audits? As mentioned above, there is nothing to suggest at this stage that Advanced and Synnovis were deliberately acting against the instructions of their respective controllers.

In a supply chain attack, where the supplier provides IT solutions to dozens or even hundreds of large corporate customers, particularly across critically important industries such as financial services, healthcare, logistics, transport or defence, the supplier is not only vulnerable to attack due to its pivotal role but will also be potentially more likely to fall under the spotlight by the regulator if something goes wrong under their watch.

So, one does wonder whether in practice, it is sometimes more convenient for a regulator to act against a single processor for the failure, rather than collectively taking enforcement action against dozens of controllers, despite them being equally culpable? On the face of it, this approach is appealing for a number of varying reasons. For instance, with limited resources at its disposal – attempting to take enforcement action against dozens of controllers could prove administratively and financially very challenging for the regulator. Conversely, with all of the affected controllers' fingers of blame metaphorically pointing at their processor, it appears to be a more direct and straightforward approach to target the single processor entity.

What can we expect to see in the future?

In our view, it is unlikely that the Advanced case marks a major shift in position from the ICO in terms of targeting processors.

That is not to say that we won't see serious enforcement action taken against processors in the future – but rather, such cases will focus on protecting critical sectors, holding processors in strategically important supply chains to account and clamping down on basic security failings such as a lack of MFA.

Regardless of the outcome for Advanced, this wake-up call will see a change in dynamic when it comes to negotiating liability and indemnity clauses in contracts between controllers and processors. Since 2018, when the GDPR came into force, we have seen the balance of bargaining power still with the controllers, who often insist on being indemnified by their processor suppliers and typically seek a super cap on liability or unlimited liability for data breaches (and the position is not always mutual). With growing recognition that processors could themselves face regulatory fines, this will likely result in processors revisiting their standard position, negotiating such clauses with renewed vigour and concern.

We will be watching with eagerness to see how the Advanced decision unfolds (as well as possible details of the investigations into Synnovis and Capita) and further analysis and legal opinion on these developments will follow.

Full list of references available upon request