SLAUGHTER AND MAY/

MANAGING CYBER RISKS

KEY LESSONS FROM RECENT LITIGATION AND ENFORCEMENT ACTION

This morning, the Information Commissioner's Office (**ICO**) announced that it had fined Interserve Group Limited (**Interserve**) £4,400,000 for breaches of the UK GDPR which came to light following a May 2020 cyberattack. This is the fifth enforcement decision from the ICO since Commissioner John Edwards took office at the start of the year and, taken with recent decisions in data-related litigation, there are clear lessons emerging as to how the ICO and the courts expect organisations to handle cyber and data risk.

First, the Interserve decision makes clear that the ICO expects all organisations to stay on top of cyber security standards and practices, even if they are a B2B business and even if they are facing financial challenges. The ICO emphasised that it expects organisations to take account of relevant industry standards of good practice, including the ISO27000 and NIST series, and publicly available guidance, expressly referencing guidance from the National Cyber Security Centre and the ICO itself.

Second, while the cyberattack affected numerous companies within the Interserve Group, the ICO found that Interserve, as the parent company, was ultimately responsible for making decisions on data protection and information security and therefore it received the MPN. This is consistent with enforcement against other large groups, such as BA and Marriott. It is essential that organisations are clear about where and how these decisions are made and who owns cyber and data risks – and that they can evidence this to the ICO if challenged or transaction counterparties (e.g. in an M&A scenario).

Third, the decision again demonstrates the importance of acting quickly to remediate and investigate any data incident. The ICO acknowledged the extensive remedial efforts made by Interserve to address the impact of the cyberattack and the action it took to mitigate the risk of harm to data subjects and provided a substantial reduction in the penalty ultimately imposed as a result. These remediation efforts also enabled Interserve to operate its business without substantial interruption as a result of the cyberattack and to subsequently carry out a series of significant M&A transactions without undue impact.

The detailed investigation undertaken by Interserve and its advisers allowed Interserve to present clear facts to the ICO from the outset, not only in relation to how the incident happened and what data was affected but also how it addressed the risk of harm. Carrying out a detailed investigation also means organisations can effectively challenge the ICO's findings if required and is critical to any appeal against an ICO fine, as evidenced by the reductions obtained by DSG Retail Ltd and Doorstep Dispensaree Ltd before the First Tier Tribunal.

Somewhat unusually the ICO has said that no reductions to the fine were made on account of Interserve's representations - and the public enforcement decision does not offer the usual discount for prompt payment seen in the ICO's guidance and other decisions. Our experience, however, is that proactive engagement with the ICO in the course of its investigation increases the likelihood of the ICO arriving at a reasonable starting point for any penalty and ensuring that appropriate reductions are made during the fine setting process itself (not just once the draft notice of intent arrives).

Fourth, unfortunately, the Interserve decision also makes clear that there is limited ability to change the past and prior data incidents (and any unaddressed remediation efforts from such incident) will be taken into account as aggravating factors. This is consistent with other decisions (and the ICO's draft enforcement guidelines) and shows the ICO is increasingly focused on organisations having the right governance and management systems in place to safeguard data. In that regard, the Commissioner has stated (somewhat forcefully) that he considers the biggest cyber risk to be complacency within an organisation and has warned that organisations will face fines if they fail to monitor for suspicious activity on an ongoing basis, act on warnings, update software and train their staff.

Consistent with broader trends in data-related litigation where the courts in England and Wales (and indeed in Europe) have shown a marked reluctance to award substantial compensation for non-material damages in data breach cases, there does appear to be comparatively less regulatory focus on the impact on individual data subjects.[1] Nonetheless, with cyberattacks on the rise and organisations handling more data than ever before, it is essential that organisations can

[1] See for instance the UK Supreme Court decision in *Lloyd v Google* or the recent EC Advocate General opinion in *UI v Österreichische Post AG*.

demonstrate that they have considered relevant guidance on data and cyber risk, how that applies to their business and documented key decisions taken to safeguard data.

Slaughter and May advised Interserve on its response to the cyberattack and the subsequent ICO investigation.

CONTACTS

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

ROSS O'MAHONY
ASSOCIATE
T: 020 7090 3856
E: ross.OMahony@SlaughterandMay.com