Skadden

Cybersecurity and Data Privacy Update

April 1, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Aleksander J. Aleksiev
Associate / London
44.20.7519.7000
aleksander.aleksiev@skadden.com

Alex Smallwood
Associate / London
44.20.7519.7202
alex.smallwood@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

UK GDPR Regulator Fines Data Processor After Ransomware Attack

On 27 March 2025, the UK Information Commissioner's Office (ICO) issued a £3.07 million fine to an IT services provider following a ransomware attack in 2022 that affected the company's health care business.

The ransomware attack had significant consequences, including the theft of data about approximately 80,000 individuals (including health data for half of these), and outages affecting the National Health Service (NHS) 111 medical helpline and patient records systems.

Key Lessons

1. Companies need to get the cyber basics right.

The ICO found that the company failed to properly implement "fundamental cybersecurity principles" such as multifactor authentication (MFA), vulnerability scanning and patch management. These failures contributed to the ransomware incident because the threat actor was able to gain initial access to the company's systems through an account that did not have MFA enabled, and then exploit a two-year-old unpatched vulnerability to move through the company's IT environment.

The ICO and other General Data Protection Regulation (GDPR) regulators are generally sympathetic to ransomware victims who respond effectively to sophisticated attacks. However, these **regulators heavily scrutinise victims that fail to maintain basic cybersecurity practices or that poorly coordinate responses to a cybersecurity breach.**

- Companies should consider (i) gap-assessing their cybersecurity posture against the ICO's guide to data security, (ii) regularly reviewing incident response plans to ensure those are operating on the market and (iii) establishing models for and a practice of effective engagement with regulators and authorities.
- Companies should also conduct regular tabletop exercises to stress-test these plans, focusing on legal issues and regulatory engagement.

2. Extra care is needed when sensitive data is involved.

With limited resources, the ICO prioritises incidents involving sensitive data, such as medical information, and holds companies that process such data to a high standard. Companies that hold sensitive data should pay particular attention to their cybersecurity posture.

3. Proactive engagement with authorities is a mitigating factor for fines.

In assessing the fine in this case, the ICO considered the company's proactive and voluntary engagement with the UK government (including the National Cyber

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

Security Centre and the National Crime Agency) a significant mitigating factor.

- Companies should review their incident response plans to ensure that they support voluntary engagement with authorities — not just mandatory regulator notifications.

4. Data processors have responsibilities under the GDPR.

The company in this case acted as a data processor rather than a data controller in relation to the affected systems. **Even though data processors are subject to only a small subset of GDPR obligations, the decision serves as a reminder the GDPR regulators can and will enforce those obligations.**

5. The ICO considers data breaches "serious" offences and issues fines accordingly.

The ICO, applying its fining guidance, stated that the data breach had a "high degree of seriousness," and so required a significant fine. The authority ultimately issued a fine representing roughly 1% of the company's global revenue. Because the company was a relatively small entity, this amounted to only £3.07 million, but for larger organizations, 1% of global revenue would be a significant sum.