DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to My Media World Ltd t/a Brand New Tube ('BNT') in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain alleged infringements of the UK GDPR.

Case Summary

It is our understanding that on or around 14 August 2022, an unauthorised third party gained access to BNT's systems and exfiltrated the personal data of 345,000 UK Data Subjects. BNT have been unable to determine the specific cause of the incident advising on separate occasions that a server misconfiguration and a DDoS attack were responsible for the access to their systems.

The nature of the data affected included the names, email addresses and passwords of 345,000 website users.

The proposed reprimand

The Commissioner has provisionally decided to issue a reprimand to BNT in respect of the following alleged infringements of the UK GDPR:

- Article 32 (1) which states:

  "taking 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

- Article 32 (1) (d) which states that organisations should have:

  "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing"

The reasons for the Commissioner's provisional findings are set out below.

- BNT were unable to provide evidence that they were conducting regular penetration testing or vulnerability scanning on their systems. They advised that a third party was responsible for

providing this service, but could not confirm when scans were last performed, or what their methodology or use was. NCSC guidance[1] recommends monthly vulnerability scans, and provides guidance on the type of scans on offer, including web application scans.

- BNT did not have appropriate organisational measures in place to ensure the confidentiality and integrity of their systems. BNT have not provided any evidence to show the technical security measures in place at the time of the incident, or that they were even aware what these measures were. BNT relied on the assurances of third parties and employees without proof of any contracts or oversight. Ultimately, BNT have failed to evidence how the personal data for which they were responsible was stored and protected. ICO guidance[2] provides a checklist for organisations to consider when implementing their technical security strategy, which includes recommendations that organisations ensure data processors also implement appropriate measures.

Provisional decision to issue a reprimand

Taking into account all the circumstances of this case, the Commissioner has provisionally decided to issue a reprimand to BNT in relation to the alleged infringements of Article 32 (1) and 32 (1) (d) of the UK GDPR set out above.

Further Action Recommended

The Commissioner recommends that BNT should take steps to ensure it is compliant with the UK GDPR. With particular reference to Article 32 (1) and 32 (1) (d) of the UK GDPR, the following steps are recommended:

1. In order to ensure compliance with Article 32 (1), BNT should ensure they have appropriate contracts in place with any third party providers which set out the roles and responsibilities of each party.

2. In order to ensure compliance with Article 32 (1), BNT should ensure they are keeping accurate records of their processing activities, and the security measures they are implementing.

3. In order to ensure compliance with Article 32 (1) (d). BNT should ensure they are carrying out regular scans and testing of their

[1] Vulnerability Scanning Tools and Services - NCSC.GOV.UK
[2] A guide to data security | ICO

environment, and are recording outcome and addressing any issues promptly.