The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 ico.org.uk

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

23 August 2023

TO: Gloucester City Council

OF: Civic Suite

North Warehouse

The Docks

Gloucester

GL1 2EP

The Information Commissioner (the Commissioner) issues a reprimand to Gloucester City Council in accordance with Article 58(2)(b) of the UK General Data Protection Regulation ('UK GDPR') in respect of certain infringements of the UK GDPR.

The Reprimand

The Commissioner has decided to issue a reprimand to Gloucester City Council in respect of the following infringements of the UK GDPR:

- Article 32(1)(b) which states that organisations must have appropriate technical and organisational measures in place, appropriate to the risk of their processing, including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- Article 32(1)(c) which states that organisations must have appropriate technical and organisational measures in place,

appropriate to the risk of their processing, including the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

- Article 32(1)(d) which states that organisations must have appropriate technical and organisational measures in place, appropriate to the risk of their processing, including 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 findings are set out below.

Lack of appropriate logging and monitoring systems

As noted in the post-incident forensic report, Gloucester City Council did not have a centralised logging system or SIEM in place. This significantly restricted Gloucester City Council's ability to effectively monitor and respond to security incidents, detect anomalous activities, and identify potential threats.

Implementing technical and organisational measures to detect and respond to incidents is a key aspect of cyber security, and there is significant guidance available on logging and monitoring best practice. For example, the NCSC provides guidance on logging and monitoring systems, stating that "Collecting logs is essential to understand how your systems are being used and is the foundation of security (or protective) monitoring. In the event of a concern or potential security incident, good logging practices will allow you to retrospectively look at what has happened and understand the impact of the incident. Security monitoring takes this further and involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling organisations to detect events that could be deemed as a security incident, and respond accordingly in order to minimise the impact". As part of this guidance, the NCSC recommend that organisations should

"Consider which logs [they] want to draw into a centralised location for analysis"

Additionally, following the ransomware attack, it became apparent that the threat actor had successfully deleted logs, erasing crucial evidence and hindering both Gloucester City Council's investigation and remediation of the incident. This also prevented early detection of the incident through the log review process that Gloucester City Council had in place with a third party supplier. Industry standards and best practice cover the requirement that logs be protected from tampering – for example the NCSC recommends that organisations should "Protect [their] logs from tampering so that is it hard for an attacker to hide their tracks and you can be confident that they accurately represent what has happened". GCC failed to prevent such tampering and, when combined with the lack of centralised logging systems or appropriate log review processes, this hindered Gloucester City Council's ability to detect and recover from this incident.

The Commissioner considers that a SIEM, or an alternative measure that would have improved Gloucester City Council's ability to effectively detect and quickly mitigate security incidents, along with appropriate considerations on how to protect logs from tampering would have been appropriate security measures for Gloucester City Council to implement proportionate to the risk of their processing activity.

Failure to implement measures and test, assess and evaluate the effectiveness of security technical and organisational measures for ensuring the security of processing.

During the post-incident response, the Commissioner considers that Gloucester City Council did not restore access to personal data, or the systems that stored personal data, in a timely manner. Additionally, Gloucester City Council were unable to determine the data subjects at risk of harm from the incident in order to notify them.

During our investigation, it was noted that the process Gloucester City Council followed to access and review impacted data – in order to determine what categories of personal data had been compromised and which data subjects were at risk – was reliant on ad-hoc systems and

processes through, for example, downloading data through the home WiFi networks of Gloucester City Council employees. There is limited evidence to suggest that Gloucester City Council had appropriate technical or organisational measures in place to respond to the incident, restore impacted data and identify risks to specific data subjects.

Article 32(1)(C) of the UK GDPR states that organisations should have appropriate measures in place to restore access to personal data in the event of an incident. Article 32(1)(d) further suggests that measures should be regularly tested to evaluate the effectiveness of such measures, and Recital 87 of the UK GDPR provides additional context into considerations the Commissioner makes on the notification to data subjects, stating "It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject". In this incident, Gloucester City Council did not recover access to personal data in a timely manner, were unable to determine which individual data subjects were at risk as a result of the incident, and did not demonstrate an appropriate process to identify and analyse impacted data in order to aid in these areas of their incident response.

During the investigation, it was considered whether Gloucester City Council had an appropriate incident response process documented, along with appropriate information and asset classification documents that would have aided in the identification and recovery of impacted personal data. Whilst evidence was provided to show that some documentation and processes were in place in this regard, correspondence from Gloucester City Council on 25 May 2022 stated that the methodologies they had in place – whilst sufficient for smaller breaches – were not sufficient for this incident.

Considering the 25 May 2022 correspondence and the ad-hoc incident response and data analysis process observed during our investigation, the Commissioner considers that Gloucester City Council did not appropriately implement technical and organisational measures that would have aided in the recovery of personal data and mitigation of risks to data subjects. We further note that this had a knock-on effect on Gloucester City Council's Article 34 compliance, requiring notification of data subjects without undue delay, and was a contributing factor in Gloucester City

Council not issuing Article 34 notifications until 17 months after their initial breach report to the Information Commissioner's Office.

Mitigating factors

In the course of our investigation we have additionally noted that:

- Gloucester City Council did have backup systems in place. Backup systems are recognised as a key technical measure to aid in the timely recovery of access to personal data, and the Commissioner considers Gloucester City Council's backups as evidence that Gloucester City Council were taking steps to comply with Article 32(1)(c). However, these backups were not utilised in favour of a full rebuild of Gloucester City Council's systems – which significantly impacted the timeline for recovery of access to personal data.

- The initial attack vector for this incident was a phishing email received from a legitimate third-party email address. No specific vulnerabilities, either through outdated systems or otherwise, were found to have contributed to the threat actor gaining initial access to Gloucester City Council's systems.

- Gloucester City Council did have some systems in place for gathering and reviewing logs, for example through regular reviews from a third-party supplier of logs generated by Gloucester City Council's systems. Whilst this has been considered as evidence that Gloucester City Council took some steps to comply with Article 32(1)(b), the logging and monitoring systems were not considered to be adequate or proportionate to the risk of Gloucester City Council's processing.

Remedial steps

The Commissioner has also considered and welcomes the remedial steps taken by Gloucester City Council in the light of this incident. In particular, the implementation of a SIEM following the incident to improve Gloucester City Council's Article 32(1)(b) compliance and the other

security hardening measures that have been undertaken, such as those outlined in Gloucester City Council's correspondence to the Information Commissioner's Office dated 14 March 2023.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to Gloucester City Council in relation to the infringements of Article 32 of the UKGDPR set out above.

Further Action Recommended

The Commissioner recommends that Gloucester City Council take certain steps to ensure its compliance with UK GDPR. With particular reference to Article 32 of the UK GDPR, the following steps are recommended:

1. In order to improve compliance with Article 32(1)(d) of the UK GDPR, ensure that Gloucester City Council's technical and organisational measures – including those introduced as postincident remedial measures – are regularly tested and there is a documented process in place for evaluating, and improving, the effectiveness of these measures

2. Perform a full review of Gloucester City Council's backup and disaster recovery measures. Including both technical and organisational measures in place to restore access to personal data, understand what personal data has been impacted during an incident and demonstrate compliance with Article 32(1)(c) if a future incident occurs. Any processes already in place should be reviewed to ensure they are sufficient in large incidents that pose a risk to data subjects through confidentiality, availability or integrity issues. Processes to test recovery systems and evaluate their effectiveness should also be considered and implemented where appropriate.

3. Review Gloucester City Council's records of processing and asset registers to ensure there is a concrete understanding of what personal data is being processed, which systems store personal data and the risks posed by a breach of confidentiality, integrity or availability for the personal data being processed. This should aim to ensure, in the event of a future incident, Gloucester City Council can quickly and confidently understand what personal data is at risk given the impacted systems and aid in Article 32(1)(c) and Article 34 compliance

Thank you for your co-operation and assistance during the course of our investigation. We now consider the matter closed.

Yours sincerely,

[redacted]

Principal Cyber Investigation Officer

Information Commissioner's Office

[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

We prioritise our investigations according to the likely impact of our actions, including considering the risks, harm and opportunities to improve compliance; alignment with our strategic priorities, including considering whether we are best placed to act or should work in collaboration with others; the likelihood of successful regulatory outcomes consistent with achieving our aims; and the resources we will require to achieve those outcomes.

As such, we aim to complete all our investigations as quickly as possible, and will keep you updated on how we are doing. Our target is to complete 95% of our investigations within 365 days. We report on our progress on our website at: Our performance | ICO

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/aboutthe-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice