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

14 November 2023

TO: GRS (Roadstone) Limited

OF: Unit 10, Goldsmith Way, Nuneaton, CV10 7RJ

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

The reprimand

The Commissioner has decided to issue a reprimand to GRS (Roadstone) Limited in respect of the following 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) (b) which states that an organisation should:

"ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"

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

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

The reason for the Commissioner's provisional findings are set out herein.

Information Commissioner's Office

The ICO exists to empower you through information.

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

GRS (Roadstone) Limited are an independent supplier of material to the construction industry. The group employs at least 800 people across 41 sites in the UK. They are a predominantly Business-2-Business operation, however they hold personal data on current and former employees.

It is our understanding that on 11 March 2022 a Threat Actor gained access to the GRS (Roadstone) Limited network, deployed Ransomware and exfiltrated data from the network. Part of the exfiltration included personal data for 2,022 UK Data Subjects and included names, addresses, National Insurance numbers, passports, driving licences, birth/marriage certificates, bank details, dates of birth and HR records. Within the HR records some limited special category data related to medical information was also exfiltrated as part of the incident.

GRS (Roadstone) Limited have determined the cause of the incident was via a Remote Desktop Service operated by a GRS (Roadstone) Limited subsidiary, S. Walsh & Son Limited. Once inside the network, the Threat Actor exploited a vulnerability on a print driver which allowed for an escalation of privileges, lateral movement across the network and the ability to deploy Ransomware and stage exfiltration of data.

Our investigation found infringements in relation to the security requirement of the UK GDPR and these are set out below.

- GRS (Roadstone) Limited were not ensuring the ongoing confidentiality of their systems as per Article 32 (1) (b).

When considering the risk posed to Data Subjects, the appropriate organisational measures were not in place. Specifically, the use of a Remote Desktop solution deployed by a subsidiary business (S. Walsh & Sons Limited), who were acquired by GRS (Roadstone) Limited in December 2017. At the time of the incident, some areas of the organisation utilised a Virtual Private Network and Multi Factor Authentication. The Remote Desktop solution which led to the incident did not have Multi Factor Authentication implemented. ICO Ransomware and data protection compliance specifically states *"You should not use single-factor authentication on internet facing services, such as remote access, if it can lead to access to personal data. Use multi-factor authentication, or other comparably secure access controls"*[1].

The acquisition of S. Walsh & Sons Limited took place four years and three months prior to the incident. GRS (Roadstone) Limited had the means and ability to deploy the technology, yet this was not undertaken.

[1] Ransomware and data protection compliance | ICO
[2] Vulnerability scanning tools and services - NCSC.GOV.UK

The lack of additional security measures in place on the Remote Desktop solution meant that with a single compromised credential, the Threat Actor was able to gain entry to the GRS (Roadstone) Limited network.

- GRS (Roadstone) Limited were not conducting security testing as per Article 32 (1) (d).

GRS (Roadstone) Limited were not conducting any formalised testing on their IT infrastructure prior to the incident. This included a lack of any vulnerability scanning or penetration testing. The group operates across 41 sites in the UK, which given the size and scale of the organisation there was a clear need for regular assessment of the IT infrastructure. Once inside the network, the Threat Actor escalated privileges and performed lateral movement by exploiting a documented Common Vulnerabilities and Exposure that had been published over two years before the incident. For this vulnerability there were relatively straightforward remedial steps which could have been taken. Had GRS (Roadstone) Limited conducted periodic vulnerability assessments of their network, this threat would almost certainly have been identified and the risk mitigated.

Both the ICO[1] and NCSC[2] have produced extensive guidance on vulnerability scanning. The NCSC recommend that it is conducted at least once every month.

Remedial steps taken by GRS (Roadstone) Limited

The Commissioner has also considered and welcomes the remedial steps taken by GRS (Roadstone) Limited in light of this incident. In particular, offering a credit monitoring service along with paying for new driving licences and passports to affected data subjects.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to GRS (Roadstone) Limited in relation to the infringements of articles of the UK GDPR set out above.

[1] Ransomware and data protection compliance | ICO
[2] Vulnerability scanning tools and services - NCSC.GOV.UK

Information Commissioner's Office

The ICO exists to empower you through information.

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

Actions taken by the Data Controller

Following the incident, GRS (Roadstone) Limited have taken a number of steps to improve the security posture of their IT infrastructure. These include:

- Deployment of vulnerability management tools
- Centralised logging
- Increased employee security awareness through additional training
- A significant increase in the number of applications requiring Multi Factor Authentication

Further action recommended

From a wider organisational perspective, there were several issues with policies and documents that were in place at the time of the incident.

- There was no Incident Response plan at the time of the incident. While not a mandatory document, when considering the *"state of the art, the costs of implementation and the nature, scope, context and purposes of processing"* this is something GRS (Roadstone) Limited could, and should have had available to support first responders. A draft of this document has been created by GRS (Roadstone) Limited, however it should now be implemented, tested and reviewed periodically.

- The Data Breach Policy makes multiple references to an appointed Data Protection Officer. It has been established that GRS (Roadstone) Limited do not in fact have an appointed Data Practitioner Officer; greater clarity around who and how breaches are handled should be clearly documented for all stakeholders related to the organisation.