DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

9 August 2023

TO: [redacted]

OF: [redacted]

The Information Commissioner (the Commissioner) issues a reprimand to [redacted] 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 [redacted] in respect of the following infringements of the UK GDPR:

- Article 5(1)(f) which states "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

- Article 32(1)(b) 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, including inter alia as appropriate: (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"

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

Case Summary

It is our understanding that on 8 December 2020, [redacted], an online source for cybersecurity news and independent research, contacted [redacted] and advised it had gained access to [redacted] The email was automatically sent to a junk folder. [redacted] subsequently contacted [redacted] to advise it was able to access [redacted] data. [redacted] contacted [redacted] on 4 January 2021 to inform them of this issue and [redacted] shut down the [redacted] on 5 January 2021.

During the course of an internal investigation, [redacted] determined the [redacted] was accessed for the first time in three years, two weeks prior to the system penetration by [redacted] [redacted] believed the [redacted] was configured in error when the account was accessed by a [redacted] employee on 18 November 2020. [redacted] further stated it was likely this triggered the weakness in the system and allowed the data to be accessed. [redacted] acknowledged there was a risk the data had been accessed by a third party for malicious purposes. It also stated it could not be ruled out because the data logs were only held for a limited time, and it was no longer possible to access this information.

Within the affected [redacted] [redacted] stored approximately 12,000 records relating to 3,000 workers. The personal data consisted of a variety of different data sets, including names, addresses, dates of birth, passports, ID documents and National Insurance numbers.

Our consideration of this case

We have investigated whether [redacted] has complied with the requirements of data protection legislation. Our investigation has identified the following points in relation to the security requirements of the UK GDPR:

• [redacted] misconfigured its [redacted] storage container to be publicly accessible and the data was consequently exposed to open access without any requirement to authenticate. [redacted] was unable to categorically state who configured the [redacted] to be publicly accessible, but believed the [redacted] configuration was altered in error when the account was accessed by an employee on 18 November 2020. Public access to the [redacted] was not removed until 5 January 2021.
• There are no additional costs to set a [redacted] to public or private. It is a configuration setting where the customer chooses how it is set.

• [redacted] acknowledged the volume and content of the data, which included basic identifiers, ID documents and financial details, would lead to a high risk if the data had been accessed by a malicious actor.
• Guidance was available from [redacted] and the National Cyber Security Centre ('NCSC') at the time of the incident which highlighted the importance of cloud configuration, logging, identity management and access controls.

Mitigating factors

During the course of our investigation, we have noted that [redacted] directly notified data subjects of the security incident and published an information notice on its website.

Remedial steps taken by [redacted]

The Commissioner has also considered and welcomes the remedial steps taken by [redacted] in light of this incident. In particular:

• [redacted] took action to remove open access to the [redacted] on 5 January 2021 and deleted all data held in the storage container on 7 January 2021, having moved the data to hard storage.
• [redacted] undertook a full review of all internal data processing processes, policies and procedures and provided training to staff to minimise the risk of a recurrence.

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 [redacted] in relation to the infringements of Article 5(1)(f) and Article 32(1)(b) of the UK GDPR set out above.

Recommendations

In line with Article 5(1)(f) and Article 32(1)(b) of the UK GDPR, The Commissioner routinely recommends the following steps:

1. Periodically audit the configuration of cloud services as part of a wider security assessment. The NCSC's guidance on risk management includes practical advice on security governance and how to align the security activities to the objectives of the

organisation. The NCSC has also published specific cloud security guidance which outlines principles surrounding identification, authentication and operational security.

2. Ensure appropriate identity and access controls are in place to allow secure access to systems processing (including the storage of) personal data. Access rights should be reviewed regularly and revoked when no longer required. The NCSC has published guidance on identity and access management which suggests the development of appropriate policies and processes and authentication methods proportionate to the risk.

3. Appropriate event logging and security monitoring should be maintained to trace access to personal data and quickly identify if a security incident occurs. This can be supported by the NCSC's guidance on logging and monitoring in its '10 Steps to Cyber Security'.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely,

[redacted]
Lead Technical Investigations Officer
Information Commissioner's Office
[redacted]