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

18 October 2023

TO: Gap Personnel Holdings Limited

OF: Pulford House, Bell Meadow Business Park, Park Lane, Pulford, Chester, England, CH4 9EP

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

The reprimand

The Commissioner has decided to issue a reprimand to Gap 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 organisations should:

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

- 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 findings are set out below.

Case Summary / Background

Gap, is a recruitment company who provide an employment service for temporary and permanent contracts in multiple sectors such as Construction, IT, Science, Healthcare, Human Resources, Sales, Finance.

It is the Commissioner's understanding that an unauthorised third party gained access to Gap's systems twice within a 12-month timeframe. Both incidents resulted in personal data being exfiltrated from a database within Gap's system.

First Incident

Unauthorised access was first gained on or around 13 March 2022 (the "March incident"). The affected database contained personal data for 13,720 UK Data Subjects. The database included both fully and partially completed records meaning that not all categories of data were present for all data subjects, but variously included names, addresses, email addresses, telephone numbers, dates of birth and right to work. For 5,364 UK Data Subjects the data also included bank account numbers.

Gap were unable to determine the specific cause of the March incident but believe it is likely that the threat actor leveraged an unsecure script (PHP file) and performed an SQL injection attack.

In response to the March incident, Gap kept the affected system live and carried out remedial measures which included [redacted]

Second Incident

However, on or around 16 August 2022 the same threat actor gained unauthorised access to Gap's system again (the "August incident"). At this time, the affected database contained personal data for 4,421 UK Data Subjects. The database included both fully and partially completed records

meaning that not all categories of data were present for all data subjects, but variously included names, addresses, email addresses, telephone numbers, dates of birth and right to work. For 1,506 UK Data Subjects the data also included bank account numbers.

Gap have been unable to determine the specific cause of the August incident, however it believes that the August incident was the result of an SQL injection attack on a different webpage to that used to access the database in the March incident. Gap stated that the vulnerability they believe allowed unauthorised access in March had been patched and tested on 26 April 2022.

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

Article 32(1)(b)

- Gap were not ensuring the ongoing confidentiality, integrity and resilience of their systems as per Article 32 (1) (b). Gap did not have the appropriate technical and organisational measures in place to ensure the level of security appropriate to risk.

  At the time of the incident there were a number of vulnerabilities present, which Gap had previously been made aware of. There are four specific vulnerabilities which we found to have contributed to the breach for the following reasons:

  i. Unsupported version of MySQL

     At the time of both incidents, Gap were using MySQL version 5.6. This version had received no support after February 2021. Gap were aware the version was out of support but explained that updating the MySQL version could stop the system from working, so they knowingly continued with the 'out of support' version and decided to replace the system instead. While the out of support version may not have directly led to the execution of an SQL injection attack, it shows a wider lack of adherence to good practice around patch management in the security landscape.

ii. Unsupported PHP version

At the time of both incidents Gap were using PHP version 7.1. This version received its last update in October 2019. Gap decided not to update the PHP version due to the legacy coding not being compatible with the recent versions of PHP. Updating the coding would have taken significant work on a system Gap were planning to replace. As outlined in (i), this highlights a lack of awareness in relation to patch management and the risks associated with securing personal data.

iii. Poorly written PHP code

The poorly written coding is relevant to input validation because this directly relates to whether the data inputted by a user onto a system is or isn't acceptable. It would be expected that a system capturing personal details would validate input data; both to prevent SQL injection attacks and also ensure the integrity of data entered by the user.

iv. Insufficient logging

Gap did have system logging in place at the time of both incidents, however the logging was insufficient which meant analysis of the attack was limited. A strategy for recording events on a system is good practice and would help in the analysis of an attack on a system.

The software vulnerabilities, along with the lack of appropriate logging and monitoring system, limited Gap's ability to effectively detect and quickly mitigate security incidents. The NCSC[1] guidance recommends organisations implement logging and monitoring to effectively identify the source and the extent of compromise.

The commissioner has taken into consideration the nature and risk of processing, the state of the art and the cost of implementation, and

[1] Logging and protective monitoring - NCSC.GOV.UK

understands that Gap intended to replace the affected system, and have since introduced this. Gap cited Covid for the reason for the delay.

Article 32(1)(d)

- Gap were not conducting security testing as per Article 32 (1) (d). [redacted] The NCSC[2] recommends organisations perform vulnerability scans at least once every month, and provides guidance on the type of scans available, including web application scans.

Article 32(1)

- Gap did not have the correct organisational measures in place to ensure a level of security appropriate to the risk as per Article 32 (1). Gap did not have an active patching policy in place at the time of the incident. This demonstrated failings in the organisation's wider obligations under the UK GDPR.

Remedial steps taken by Gap

The Commissioner has also considered and welcomes the remedial steps taken by Gap in light of this incident. In particular Gap's prompt notification to Data Subjects of the March incident in April 2022, which included a link to NCSC data breach guidance for individuals[3], and provided them with direct contact information to discuss the incident in more detail. Also, in October 2022 Gap implemented a new system with security measures and regular penetration testing, alongside introducing additional policies including data retention, patching and vulnerability management.

Moving forward in line with Article 32 (1) of the UK GDPR, Gap should ensure they maintain appropriate technical and organisational measures to detect and respond to incidents promptly.

Decision to issue a reprimand

[2] Vulnerability Scanning Tools and Services - NCSC.GOV.UK
[3] Data breaches: guidance for individuals and families - NCSC.GOV.UK

Taking into account all the circumstances of this case, including the remedial steps, and the representations made by Gap, the Commissioner has decided to issue a reprimand to Gap in relation to the alleged infringements of articles of the UK GDPR set out above.

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