Case 201900212

Enforcement Order

Jacques Scott Group Ltd.

18 March 2021

EXECUTIVE SUMMARY

Jacques Scott Group Ltd. (JSG) suffered a ransomware attack that led to employees being denied access to the enterprise network and a number of critical systems. JSG notified the Office of the Ombudsman and the affected data subjects as required by law.

JSG's external IT service provider began an initial analysis, and decided to engage Deloitte and SigNus Technologies to investigate the breach and undertake mitigating action.

The ransomware attack affected various types of personal data of some 150 data subjects, including employees, shareholders and pension account members, but not their passwords or financial data. Because critical system logs were not available, a number of questions could not be answered, but the personal data is not thought to have been exfiltrated.

The Ombudsman found that JSG violated the seventh data protection principle of the Data Protection Law, 2017 (DPL), which requires data controllers to ensure that adequate technical and organizational measures are taken against unauthorized or unlawful processing.

The Ombudsman also found that JSG failed to incorporate certain mandatory provisions required by the DPL into the agreement with its data processor, which constitutes a separate violation of the seventh principle.

The Ombudsman recognized that JSG took appropriate steps to mitigate the effects of the ransomware, and adopted the recommendations made by Deloitte, as well as formulating a number of additional recommendations.

A. BACKGROUND

[redacted]

B. CONSIDERATION OF ISSUES

[redacted]

C. FINDINGS, RECOMMENDATIONS AND DECISIONS

Under section 45(1) of the DPL, for the reasons explained above, I make the following findings, recommendations and decisions:

- JSG did not comply with the seventh data protection principle, as it contravened paragraphs 3(b) and (c) of part 2 of schedule 1, since its agreement with the data processor, MCS, did not specify that the processor was to act only on instructions from the data controller, and that the data processor had to comply with obligations equivalent to those imposed on the data controller by the seventh data protection principle.
- JSG did not comply with the seventh data protection principle in paragraph 7, part 1 of schedule 1, since it did not take "appropriate technical and organizational measures ... against unauthorized or unlawful processing of personal data".
- Subsequent to the ransomware attack, JSG took appropriate steps to mitigate the consequences of the breach. The personal data in question does not appear to have been exfiltrated, and it appears that there have not been any serious or ongoing consequences for the data subjects whose data was involved.
- I require JSG to ensure that any current and future agreements with its data processors meet the requirements of paragraph 3 of part 2 of schedule 1, described immediately above.
- I support the recommendations made by Deloitte in the security and compromise assessment report and recommend that JSG execute them.
- In addition, I recommend that JSG take the following steps to prevent and/or detect any future ransomware attacks, including:

a) developing appropriate information security and related policies and procedures to ensure that business operations are conducted in line with the organization's information security governance and information risk profile;
b) providing cybersecurity awareness training to its employees at least annually to improve their ability to identify and prevent phishing and other malicious attacks, and conducting periodic phishing simulation tests;
c) providing training to its employees on established incident response policies and procedures, so that they are aware of what to do and who to report to in the event that they fall victim to a malicious attack or suspect one;
d) providing training to its employees on data handling practices once internal privacy policies and procedures are established to ensure ongoing compliance with the DPL;
e) enabling logs on all critical network devices to make sure that critical information for the investigation of any future cyberattacks is available;
f) ensuring that backups follow the 3-2-1 backup (or similar) strategy, by keeping three copies of the data, two of which should be stored on different media and one off-site;
g) implementing a leading endpoint protection platform that incorporates multiple layers of protection, as well as a UTM system that provides threat detection and prevention in real time;
h) implementing a patch management solution to ensure that operating systems and applications are kept up to date with the latest security patches;
i) implementing quarterly vulnerability assessments and annual penetration testing to identify security weaknesses in the information systems as part of a regular IT review and maintenance schedule.

[1] Under section 47, a person who has received an enforcement order under the DPL may, within 45 days of receipt and upon notice to the Ombudsman, seek judicial review of the order to the Grand Court.

Sandy Hermiston
Ombudsman