QFC Data Protection Office imposes a reprimand and financial penalty on a QFC-licensed firm for infringements of the QFC Data Protection Regulations 2021

26 September 2024, Doha, Qatar: The QFC Data Protection Office (the "DPO") announced today that on 2 September 2024 it imposed a reprimand and financial penalty in the sum of US$150,000 on a QFC-licensed firm (the "Firm") for infringements of Article 8 (Principle 6), Article 9, Article 29(1)(B) and (D), and Article 31(1) of the QFC Data Protection Regulations 2021 ("the Regulations").

Summary of Decision Notice

Background:

In December 2022, a substantial data breach at the Firm led to the exposure of a considerable amount of personal data. The breach was caused by a threat actor gaining unauthorised access to the Firm's systems due to inadequate security measures and a lack of sufficient monitoring and oversight.

Key Findings:

Late Notification of the Personal Data Breach – Infringement of Article 31(1)

The Firm failed to notify the DPO of a personal data breach within the required 72-hour timeframe after becoming aware of it. The Firm's Data Processor was aware of the breach 13 days prior to notifying the Firm, resulting in a delayed Personal Data Breach Report by of at least 10 days.

The DPO notes that where a Data Processor becomes aware of a Personal Data Breach, it is obligated under Article 31(7) of the Regulations to notify the Data Controller 'without undue delay'. Where the Data Processor delays notification to the Firm, this does not absolve the Data Controller of its responsibilities under the Regulations. As the key decision-maker in Processing activities, the Data Controller determines the purposes and means of Processing, while the Data Processor acts on its behalf according to instructions. The Data Processor cannot be used as a means to evade compliance with the Regulations. Accordingly, the Firm was found to have contravened Article 31(1) of the Regulations.

Security of Processing and the Technical and Organisational Measures – Infringement of Article 29(1)(B) and (D)

The DPO found that the Firm did not sufficiently meet its obligations to protect the confidentiality, integrity, availability, and resilience of its processing systems and services, as required by Article 29(1)(B) of the Regulations. The Firm did not fully implement its established security measures and lacked adequate mechanisms for effective system monitoring.

Additionally, the Firm lacked adequate system logs, as there was insufficient retention and recording of activities. This limitation affected the Firm's ability to detect and investigate potential

security incidents. The Firm also did not conduct a comprehensive review of its information security and data protection practices to ensure their adequacy and effectiveness.

Integrity and Confidentiality of Processing – Infringement of Article 8 (Principle 6) and Article 9

The Firm failed to process personal data in a manner that ensured appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, as required by Article 8 (Principle 6). Additionally, the Firm was unable to demonstrate compliance with these principles, infringing Article 9. The Firm's lack of oversight mechanisms and failure to enforce its own security policies contributed to this failure.

Corrective Actions:

Reprimand: The Firm received a formal reprimand for its failures, particularly regarding incident response procedures and the implementation of adequate security measures. The DPO required the Firm to revise its technical and organisational measures to prevent future breaches and ensure timely notification in the event of any incidents.

Financial Penalty: A financial penalty of USD 150,000 has been imposed on the Firm. This penalty reflects the seriousness of the Firm's infringements and serves as a deterrent against similar lapses in the future.

Public censure:

In this instance, the DPO has elected not to issue a public censure against the Firm. This decision is based on the Firm's prompt and full cooperation with the investigation, its acknowledgment and acceptance of the DPO's findings, and the substantive steps taken to strengthen its data protection measures. As a result, the DPO has determined that a public censure would not further serve the public interest and would serve little purpose beyond inflicting additional punishment.

(Ends)

About the QFC Data Protection Office

The QFC Data Protection Office was established in 2021 under Article 32 of the QFC Data Protection Regulations 2021 by the Qatar Financial Centre Authority, in accordance with Article 6 of the QFC Law. The Data Protection Office's objectives, as outlined in Article 32(3), are to monitor, ensure, and enforce compliance with the Regulations; promote best practices among Data Controllers and Data Processors; and enhance public awareness and understanding of data protection within the QFC. The Data Protection Office has broad powers under Article 33, including investigative, corrective, and advisory functions, which include issuing orders, reprimands, and financial penalties.

Further details are available on the website www.qfc.qa.

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa