Reference: ADGM/RA/ODP/LET/028

To: VentureRock Global Limited (000009138)

Address: Bubble Number B03, 11th floor ADGM
Al Sarab Tower
ADGM Square
Al Maryah Island
Abu Dhabi
United Arab Emirates

Date: **23rd of June 2023**

ABU DHABI GLOBAL MARKET

DATA PROTECTION REGULATIONS 2021

DIRECTION ISSUED UNDER SECTION 54(1)

1. DIRECTION

1.1 The Commissioner of Data Protection (the "**Commissioner**") of the Abu Dhabi Global Market ("**ADGM**"), in accordance with Section 54(1) of the Data Protection Regulations 2021 (the "**DPR 2021**"), has decided to serve VentureRock Global Limited ("**VentureRock**") with a Direction ("**Direction**") under Sections 50(5)(b) and (d) of the DPR 2021 for failure to comply with the DPR 2021.

1.2 This Direction explains the Commissioner's decision.

2. LEGAL FRAMEWORK

2.1 The DPR 2021 governs the Processing of Personal Data by Controllers established in ADGM.

2.2 Section 62(1) provides the following key definitions in the DPR 2021:

a. '*Establishment'* means any authority, body corporate, branch, representative office, institution entity, or project established, registered or licensed to operate or conduct any activity within the ADGM or exempt from being registered or licensed under the laws of the ADGM;

b. *'Personal Data'* means any information relating to a Data Subject.

c. *'Data Subject'* means an identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

d. *'Controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; and

e. *'Processing'* means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.3 Extracts of DPR 2021 referred to in this Direction are attached in Annex 2. A complete copy of the DPR 2021 is accessible on the ADGM website.

3. VENTUREROCK GLOBAL LIMITED

3.1 VentureRock was incorporated and licenced to operate in ADGM on 14 February 2023.

3.2 VentureRock has applied pursuant to Section 27 of the Financial Services and Markets Regulations 2015 to be granted a Financial Services Permission to conduct the following Regulated Activities in or from the ADGM:

a) *Advising on Investments or Credit;*
b) *Arranging Deals in Investments; and*
c) *Managing a Collective Investment Fund.*

3.3 On 16 December 2022, VentureRock received an In-Principal Approval ("**IPA**") letter from the ADGM Financial Services Regulatory Authority ("**FSRA**") to conduct the abovementioned activities subject to VentureRock fulfilling certain conditions to FSRA's satisfaction listed out in the IPA.

3.4 As of 14 February 2023, VentureRock is a Controller, as defined in Section 62(1) of the DPR 2021, in respect of the Processing of Personal Data.

4. FACTS AND MATTERS RELIED UPON

4.1 On 20 February 2023 at 12:08 pm, ADGM's Office of Data Protection ("**ODP**") was notified by ADGM Information Security of a malicious phishing email originating from the email address of an individual at VentureRock (the **"Incident**"). The email subject was titled '[redacted]'. The email had been sent to ADGM employees.

4.2 The email was sent by '[redacted]' on 20 February at 07:34 am.

4.3 The email account of '[redacted]' belongs to [redacted]. [redacted] ADGM company [redacted] VentureRock.

4.4 On 20 February 2023 at 12:55 pm, the ODP emailed [redacted] informing [redacted] of the breach and requesting [redacted] to complete the breach notification form. The ODP provided [redacted] a deadline of 24 February 2023.

4.5 On 21 February 2023, [redacted] responded and attached the breach notification form. The breach notification form did not provide any sufficient or useful information.

4.6 On 2 March 2023, the ODP sent a follow-up email to [redacted] informing [redacted] of the lack of detail and requested VentureRock to provide an investigation, analysis or report into the Incident by 17 March 2023. The investigation, analysis, or report should assess several issues related to the Incident, and particular focus on key facts and safeguards.

4.7 On 17 March 2023, the ODP received a response from [redacted], which included an attachment of an updated breach notification form. The updated breach notification was again lacking sufficient detail or analysis of the Incident and did not include any reports or analysis of the Incident.

4.8 On 28 March 2023, the Commissioner issued VentureRock with an Order under section 50(1)(a) of the DPR 2021 requiring VentureRock to conduct an assessment. In particular, Order No.1 of 2023 required the VentureRock to provide the ODP within 40 days following the date of the Order with a detailed technical investigation report into the Incident which addresses the following questions:

I. details regarding how this incident occurred including a timeline.
II. the logs regarding the unauthorised access (i.e. I.Ps, date/time, services, session duration).
III. analysis of the services accessed by a malicious third party (i.e. Outlook, O365, OneDrive).
IV. analysis of the personal data placed held in account [redacted] (i.e. emails addresses, passports, financial information, docs etc.).
V. details regarding steps taken to contain or remediate this incident.
VI. a copy of relevant policies and procedures in place at the time of the incident.
VII. description of technical measures implemented prior to this incident.
VIII. remedial measures are taken to mitigate reoccurrence.
IX. information about relevant training and awareness of the risk of phishing.

4.9 In deciding whether to serve VentureRock with the Order, the Commissioner considered VentureRock's disinclination to provide the information sought and its necessity for the performance of the Commissioner's duties and functions to investigate VentureRock's compliance with the DPR 2021.

4.10 A preliminary consideration based on the information at hand indicated that all information and content held in the account of '[redacted]' was at risk and could have been viewed, accessed or exfiltrated. However, further information including logs was required to determine key facts and the technical measures and controls in place at VentureRock at the time of the Incident.

4.11 On 8 May 2023, [redacted] submitted to the ODP an Independent Assessment Report [redacted] dated 11 April 2023 (the "**Report**") of an assessment of the Incident conducted on 11 April 2023 by [redacted] (the **"Assessment"**).

5. FINDINGS FROM THE ASSESSMENT

5.1 The Assessment was performed on a MacBook Pro 16-inch 2019. The device appeared to be the personal device of [redacted], which was also used for [redacted] role at VentureRock. The Microsoft O365 application was registered under the [redacted] domain.

5.2 The Assessment explored the ODP questions in paragraph 4.8 above. The Report also provided some useful information for the Commissioner with regards to the facts and controls in place at the time of the Incident. In particular, it is noted that:

i) the cause of the Incident was an unauthorized access to [redacted]'s mailbox. The report highlighted that the attacker *"…had direct access to the mailbox to be able to send phishing emails to all contacts registered in the client's mailbox".*

ii) the likely cause of the malicious access was *"…account hijacking by credential harvesting through free Wi-Fi provided at the airport lounge during a trip to Abu Dhabi and Doha".* The Report highlights that this likely occurred between trips dated 11 February 2023.

iii) No data logs were retained before March 12, 2023 regarding the unauthorized access due to "…*the nature of the account*". VentureRocks admin team had provided a message trace route file within the period of the Incident, where two suspicious IP addresses were identified to send the phishing emails.

iv) On the analysis of the services accessed by a malicious third party, the Report highlighted that *"…all mails received after the incident were being redirected to the folder 'Conversation History'"* adding that *"…the fact that a new rule exists in the mailbox is proof that the attacker had gained access to the client's mailbox history".*

v) No policies and procedures were in place at VentureRock at the time of the Incident.

vi) The only technical measures implemented prior to this Incident were the use of a 'free' AVG antivirus licence. This was not effective for mitigating against this Incident.

vii) No two-factor authentication of measures implemented with Microsoft services.

viii) The remedial measures taken post-incident to mitigate reoccurrence include:

- Strict use of safe network access in public
- Secure Microsoft Outlook account with password policy and 2 Factor Authentication
- Inclusion of a Chief Information Security Officer (CISO) to develop and implement information security programs
- Reviewal of security policies implemented within the application
- Cyber Awareness Training with EC-Council

5.3 The findings and recommendations presented in the Report highlighted that VentureRock had not implemented appropriate technical and organisational measures.

6. CONTRAVENTIONS

6.1 The Commissioner finds that VentureRock did not comply with the following provisions of the DPR 2021:

6.2 Security Principle

6.2.1 Under Section 4(1)(f) of the DPR 2021, personal data must 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."*

6.2.2 Sections 30(1) of 30(2) state that:

> *(1) 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 of natural persons, the Controller and the Processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:*
>
> *(a) the Pseudonymisation and encryption of Personal Data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;*
>
> *(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.*
>
> *(2) In assessing the appropriate level of security the Controller and Processor must take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.*

6.2.3 The Report highlights that prior to the Incident, the Controller did not have in place any policy or procedure for handling such incidents or mitigating consequences for Personal Data in the event of a security breach.

6.2.4 The Report also identified that the only technical measure in place prior to the Incident was the use of free antivirus tool provided by AVG. The Assessment report highlights that the Controller had not ensured any of the following controls and measures:

- *Regular backups of data on all professional devices, and storage on dedicated servers to prevent data loss*
- *Automatic check, download and installation of updates of OSs, Antivirus software and other apps on all professional devices on a regular basis*
- *Connection safe network on all professional and personal devices used for work*
- *A proper password policy and implementation of related safeguards such as authentication*
- *Awareness training for the employees*

6.2.5 Furthermore, the Report attributed "*human error from poor cybersecurity practices"* as a root cause of the Incident. The lack of proper training, awareness, and appropriate policies/procedures were key factors concluding that the "…*incident could have been avoided if basic cyber hygiene had been followed*."

6.2.6 It is also noted that VentureRock engaged the independent assessors 21 days following the Incident, and 15 days following Order 01-2023. During this time, VentureRock undertook a number of mitigation steps which removed historic data. This action made it difficult for the assessors to obtain some information regarding the Incident.

6.2.7 It is clear from the Incident and the Report that email addresses and the content of the Microsoft Office account were accessible by the malicious third party. The creation of a rule and the redirection of emails is sufficient proof that the third party had gained access to [redacted]'s mailbox including its content.

6.2.8 The Commissioner also finds that VentureRock did not have in place appropriate technical measures for ensuring that the personal data held in his Microsoft O365 account were safeguarded against unauthorized or unlawful access. This was evident by the findings from the Independent Assessor. In particular, the lack of basic measures which could have prevented this Incident from occurring.

6.2.9 VentureRock also did not have in place appropriate organisational measures. In particular, VentureRock did not have in place any data protection policies or procedures in relation to its Processing activities as well as a lack of appropriate training. In addition, there was no process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

6.2.10 Pursuant to Sections 22(1) and (2) of the DPR 2021 it is the duty of the data Controller to implement appropriate technical and organisational measures and appropriate data protection policies to all personal data in respect of which he is the Controller. The Commissioner is of the view that VentureRock did not implement appropriate technical and organisational measures.

6.3 Lack of Cooperation

6.3.1 Section 29 of the DPR 2021 states that *"The Controller and the Processor must cooperate, on request, with the Commissioner of Data Protection in the performance of their duties and functions."*

6.3.2 During the course of the investigation, VentureRock did not provide any meaningful information when requested to do so by the ODP. [redacted] was given opportunities to cooperate and provide sufficient information from initial contact on 20 February 2023.

6.3.3 The Commissioner had to serve VentureRock with an Order to compel the provision of information.

6.3.4 The Commissioner is satisfied that VentureRock did not comply with Section 29 of the DPR 2021.

7. DIRECTION

7.1 The Commissioner has decided to serve VentureRock with a Direction under section 50(5)(b) of the DPR 2021 reprimanding VentureRock for its failure to comply with Sections 4(1)(f), 22(1), 22(2), 29, 30(1), 30(2) of the DPR 2021.

7.2 The Commissioner has decided to serve VentureRock with a Direction under 50(5)(d) of the DPR 2021 requiring VentureRock to ensure the implementation of the measures listed in **Annex 1**.

7.3 The Commissioner considers that the proposed measures set out in this Direction are both necessary and proportionate to improve the Data Controller's compliance with the DPR 2021, by implementing appropriate technical and organisational measures to ensure an adequate level of security appropriate to the risk to the integrity, availability and resilience of its OSs, devices, applications, systems, and data processing operations within VentureRock.

7.4 The Direction supports the ODP regulatory objectives including to:

a. upholding the privacy related rights afforded to individuals under DPR 2021;
b. promoting compliance; and
c. deterring other Controllers from committing similar contraventions.

7.5 In deciding to take the measures set out in this Direction, the Commissioner has considered

- the options available to him under the DPR 2021;
- VentureRock's lack of technical and organisational measures;
- VentureRock'slack of appropriate data protection and security policies and procedures;
- VentureRock'slack of proper training and awareness of the risk of phishing; and
- VentureRock'sdisinclination to fully cooperate with the ODP in the course of Incident investigation

7.6 The Commissioner has taken into account the following mitigating features of this case:

- VentureRock was a newly established entity with the ADGM at the time of the Incident;
- VentureRock took a number of remedial steps to mitigate the Incident;
- VentureRock appears to have notified most of the affected contacts to disregard the email;
- There is no evidence of individuals suffering any damage or distress in this case;
- There is no indication or evidence that VentureRock deliberately contravened the DPR 2021; and
- The Commissioner is satisfied that VentureRock has taken the initiative to review its policies and has committed to implementing measures listed in the Report.

8. PROCEDURAL MATTERS

8.1 Pursuant to Section 54(4) VentureRock may ask the Commissioner to review the Direction within 21 days of receiving this Direction. The Commissioner may receive further submissions and amend or discontinue the Direction.

8.2 The Commissioner may publish this Direction at its discretion.

ABU DHABI
GLOBAL MARKET

Dated the 23 of June 2023

Signed:

Sami Mohammed
Commissioner of Data Protection
Office of Data Protection

ANNEX 1

1. Within **four months** following the date of this Direction provide the Office of Data Protection with an update on the technical and organisational measures implemented by VentureRock following the Incident.

   The measures must consider policies and/or procedures which addresses:

   i) backups on all work related devices.

   ii) updates and patches.

   iii) using public wifi and remote working.

   iv) password management.

   v) training and awareness.

2. If any of the measures set out above cannot be implemented, an explanation or justification is required. The measures set out above shall be taken in addition to, or in line with, the recommendations placed in the Report, as listed in section 6.

ANNEX 2

Extracts of DPR 2021 referred to in this Direction

Section 4(1)(f)
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.

Section 22(1) and (2)
(1) Taking into account the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights of natural persons, the Controller must:

(a) implement appropriate technical and organisational measures to ensure and to be able to demonstrate that Processing is performed in accordance with these Regulations; and

(b) review and update those measures where necessary.

(2) Where proportionate in relation to Processing activities, the measures referred to in section 22(1) must include the implementation of appropriate data protection policies by the Controller.

Section 29
The Controller and the Processor must cooperate, on request, with the Commissioner of Data Protection in the performance of their duties and functions

Section 30(1) and (2)
(1) 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 of natural persons, the Controller and the Processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

(a) the Pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

(2) In assessing the appropriate level of security the Controller and Processor must take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

Section 54(1)
If the Commissioner of Data Protection is satisfied, after duly conducting all reasonable and necessary inspections and investigations, that a Controller or Processor has contravened or is contravening these Regulations or any rules made under these Regulations, the Commissioner of Data Protection may issue a direction requiring the Controller or Processor to do any of the measures referred to in sections 50(5)(a) to 50(5)(h) and section 50(5)(j) (a 'Direction').