28 January 2020

To: ADGM Registered Entities

OFFICE OF DATA PROTECTION CIRCULAR NO (1) OF 2020: Outcomes of Personal Data Breach Reporting Thematic Review

The purpose of this circular is to update you on the results of a personal data breach reporting thematic review, recently conducted by the Registration Authority's Office of Data Protection.

Under Section 9(5) of the ADGM Data Protection Regulations 2015, Data Controllers must notify the Registrar of personal data breaches not later than 72 hours after becoming aware of them.

Background

Between September and November 2019, the ADGM Office of Data Protection undertook a review of ADGM registered Data Controllers on the theme of data breach notifications as part of its participation in the 2019 Global Privacy Enforcement Network (GPEN) Privacy Sweep, as detailed in this circular.

GPEN and the Privacy Sweep

GPEN is a global network of privacy enforcement authorities established in 2010 to promote and support cooperation in cross-border enforcement of laws protecting privacy.

The GPEN Privacy Sweep is an annual initiative aimed at increasing awareness of privacy rights and responsibilities, encouraging compliance with privacy legislation and enhancing co-operation between international privacy enforcement authorities.

The 2019 GPEN Privacy Sweep

2019 marked the seventh edition of the annual Sweep and the theme was Data Breach Notifications.

Scope and Methodology

Data Breach Notifications

A personal data breach is any confirmed incident in which Personal Data has been lost, accessed and/or disclosed in an unauthorized fashion either accidentally or deliberately.

The Office of Data Protection's review, as part of the Sweep, focused on determining whether or not ADGM Data Controllers are aware of the data breach notification obligations in ADGM. The review also

assessed how well ADGM Data Controllers have implemented the practice of recording and reporting data breaches into their own internal privacy programs and policies.

Data breach reporting arrangements were assessed based on a framework consisting of the following five indicators:

1- Awareness of relevant data breach framework;
2- Internal procedures for handling data breaches;
3- Responding to data breaches;
4- Management; and
5- Preventing future breaches.

The approach to conducting the review involved four main steps:

1- Identifying the sectors and selecting the entities to review;
2- Creating a questionnaire;
3- Sending the questions and follow-up; and
4- Evaluating the responses.

A total of ten (10) ADGM Data Controllers were randomly selected for the review, consisting of seven (7) professional services entities and three (3) retail entities. The questionnaire was based on questions provided by GPEN, to ensure consistency of approach and comparability of findings globally.

Findings by Indicator

After sending, following up and receiving completed questionnaires from all the selected entities, the Office of Data Protection reviewed the responses. Below is the summary of the findings by indicator.

Indicator 1 - Awareness of data breach notification requirements in ADGM

All ten entities indicated that they are aware of ADGM's data breach reporting requirements. Looking in further detail, in relation to reporting mechanisms, six entities (60%) indicated that their reporting mechanisms reflect their awareness of the ADGM legal framework in relation to data breach notifications. Two entities (20%) indicated that they did not have reporting mechanisms.

Indicator 2 - Internal procedures for handling data breaches

This indicator covered whether or not Data Controllers have internal procedures for handling data breaches. Eight entities (80%) indicated that they do have internal breach handling procedures, while two entities (20%) responded that they do not have internal procedures in place.

Indicator 3 – Responding to data breaches

Data Controllers were asked whether they have policies and procedures for reporting breaches to relevant external parties (i.e. the individuals affected and the ADGM's Office of Data Protection).

Three entities (30%) confirmed that they do have such procedures in place, while two entities (20%) responded to being aware of only some aspects of what is required to report and to who. Five entities indicated that they have no reporting procedures in place.

Indicator 4 – Management

This indicator considered whether Data Controllers keep records of data breaches and whether they monitor their performance regarding data protection standards.

Three entities (30%) keep records of data breaches, while five entities responded that they have never had a data breach. Two entities (20%) responded that they do not keep records of data breaches.

Six entities (60%) responded that they monitor their performance regarding data protection standards. Four entities (40%) do not monitor their data protection standards' performance.

Indicator 5 – Preventing future breaches

Three entities (30%) responded that they take steps following a data breach to prevent future breaches. One entity responded that it does not have procedures for preventing future breaches while six entities failed to specify due to the number of Data Controllers indicating that they have never had a data breach.

Personal Data Breaches

Only one (1) Data Controller reported that it had had a data breach. Further, that entity indicated that it did not report the breach to the ADGM's Office of Data Protection (which is required under the Data Protection Regulations). All other Data Controllers indicated that they never had a data breach.

International Findings and Best Practices

The following findings and best practices are based on the overall combined results from the GPEN members that participated in the sweep:

1- Eighty-four percent (84%) of the entities across all sectors and jurisdictions had appointed a team or group responsible for managing data breaches, to whom breaches should be reported;
2- Around 45% of the entities surveyed indicated that they maintain up to date records of all data breaches or potential breaches;
3- Eighty-six (86%) of the entities had internal guidance in place to assist staff in recognising a breach or potential breach;
4- Some entities indicated that they discuss every personal data breach with the relevant DPA. This indicates that a greater understanding of the relevant legal framework and the establishment of internal policies would enable internal assessment to take place in the first instance;
5- To ensure regulatory standards in relation to data protection are met, some entities conduct monthly senior management reporting, quarterly information governance board meetings and periodic audits. Some respondents use external companies to conduct audits;
6- Some entities deliver staff training for specific risks such as phishing communications to help prevent future breaches; and
7- Other measures taken by entities to ensure compliance with mandatory data breach notification requirements are:

a. Staff training, implementing proper procedures, and designating someone to be responsible for handling data breaches;
b. Producing internal guidance and setting up internal awareness training for staff (either via e-learning or outsourced externally); and
c. External parties brought in to assist with entities to prepare for mandatory breach schemes and provide training.

Conclusion

The majority of Data Controllers in the review indicated that they are aware of the data breach reporting requirements in ADGM. However, when asked more detailed questions about data breach reporting arrangements, the responses often showed that entities did not have adequate arrangements in place to ensure compliance with the requirements and/or lacked sufficient understanding of the necessary arrangements regarding data breach reporting. In short, whilst entities indicated awareness, the findings suggest that there is a lack of full compliance with, and/or understanding of requirements.

Next Steps

All ADGM Data Controllers are expected to comply with the Data Protection Regulations 2015. Where a data breach occurs, entities are required to notify the Office of Data Protection through the RA online portal.

However, the Office of Data Protection recognizes the need for further education and awareness of data protection requirements, and is working to provide more guidance and outreach (including by issuing this Circular as well as setting up a dedicated data breach reporting webpage – see below).

The Office of Data Protection also carries out on site assessments to assess in further detail whether ADGM Data Controllers are complying with the ADGM Data Protection Regulations (including data breach requirements) and, where necessary, will take disciplinary action in respect of non-compliance.

Further Information

For further information and guidance on ADGM's data breach reporting requirements please go to the Registration Authority's dedicated data breach notifications webpage at: https://www.adgm.com/operating-in-adgm/office-of-data-protection/data-breach-notifications

Sincerely

4D
ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي
REGISTRATION AUTHORITY
سلطة التسجيل

Tim Land
Executive Director, Monitoring & Enforcement