NOTIFYING THE COMMISSIONER OF DATA PROTECTION OF A PERSONAL DATA BREACH

Commissioner of Data Protection

DIFC

CONTENTS

1. Introduction

Personal Data Breaches may take many forms, both logical and physical. In recent years, the requirement to notify the relevant local data protection authority has been affirmed as a clear obligation. Breach notification requirements under the Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law") and potentially other applicable data protection laws and regulations similarly use terms such as "as soon as practicable" as per Articles 41(1) and 42(1) of the DP Law and Regulation 8 of the DIFC Data Protection Regulations, and others still set out a time-based requirement of 72 hours (including, for example the UK and EU General Data Protection Regulations) if the breach meets the criteria for reporting. Data processors are now also laden with breach notification obligations, in particular under Article 41(2) of the DP Law. Every DIFC registered entity that collects and maintains Personal Data must comply with these requirements.

Personal Data is defined in the DIFC DP Law as, "Any Data referring to an Identifiable Natural Person" and Special Category Data is defined as, "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person." Such data includes but is not limited to name, address, business or personal email address, business or personal phone numbers, geolocations, job title or other employee data, health and biometric data, religious affiliations or criminal history. In sum, Personal Data generally can be any information that when viewed together (or in some cases is so unique) clearly identifies a living individual. It could be data about clients, employees, suppliers, or family members, to name a few categories of Personal Data. The defined terms used herein have the same meaning as the defined terms in the DP Law.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the DIFC Commissioner of Data Protection (the **Commissioner**) either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

2. Scope

Due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance should be read in conjunction with those existing UK and EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

3. How to Report a Personal Data Breach

If your business is processing Personal Data or Special Category Data, and a breach occurs, please report it to the Commissioner of Data Protection Office. You may find it helpful to access the Personal Data Breach Reporting page of the DIFC website. There, you can:

- Complete the "Do I Need to Notify?" assessment, which will help you determine whether the breach is notifiable or not. It is only for guidance purposes. You may need to do a more detailed assessment or seek appropriate legal advice to properly determine whether to report a breach.

- If you have (already) determined that a privacy breach at your organisation is notifiable, or wish to notify us in any case, you may complete the 'Report a Breach' form on that page to go straight to breach reporting. If yours is a DIFC licensed entity or you are reporting on behalf of one, please supply the license number and a contact name. If not, please provide a way of contacting the person who reported the breach.

You may also report through the following methods if the above options are not available:

By Phone: +971 4 362 2222

By email: commissioner@dp.difc.ae

By Mail:
DIFC Commissioner of Data Protection
The Gate, Level 14
PO Box 74777
DIFC, Dubai, UAE

ROC Helpdesk: info@difc.ae (please clearly mark your submission as "PERSONAL DATA BREACH REPORT"

PLEASE NOTE: If you determine that you are (also) required under Article 42 to notify an individual Data Subject(s) whose personal data is involved in the breach, please do so separately as the Report a Breach form will not be shared with or reported to them by the Commissioner's Office.

4. What Should be Reported: A non-exhaustive checklist

Personal data breaches can include, but are not limited to:

- unauthorized third party access to systems and applications;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- lost or stolen devices; or
- alteration of personal data without permission or necessary instructions;

It is important to report all relevant details of the breach. This list could vary, as each breach is different. Generally, the main information to include is:

- Affected data subjects
- What personal data may have been stolen or lost
- Special categories of personal data that may have been in the data set
- How long it took to discover the breach
- What security measures were in place and how the breach occurred despite those measures
- How has it been or will it be mitigated, if possible
- What additional measures have been taken to secure the current database of personal data

Please include any other relevant information you think the Commissioner needs to know.

Special Issues – Regulation 8.4

Regulation 8.4 of the DIFC Data Protection Regulations was introduced to address the all too common situation of information in digital or other formats that may be left behind, lost or misplaced.

Inadvertently Obtained Personal Data

If an entity or person ("Party A") inadvertently comes into control or possession of data in either physical or electronic format (the "Inadvertently Obtained Information"), Party A must attempt to identify and notify the party or parties previously in control or possession

of such information ("Party B"). While Party A and Party B could be any operating entity, this situation normally involves a DIFC-based Landlord and the previously DIFC-licensed entity that formerly occupied offices or other space in the DIFC.

Impact on Party A

Party A would only be a temporary custodian of the personal information found as part of the Inadvertently Obtained Information, rather than a Controller in the commonly accepted sense. In other words, Party A would not have assumed liability and risk had Party B not left Personal Data behind, potentially constituting a breach and putting individuals at risk. Party A does have some level of responsibility, however, as there may be any number of scenarios under which information left behind could be more than simply a few names and email addresses. If a bank or other financial institution leaves such data behind, issues around impeding the prevention of financial crime may arise, for example. Regulation 8 therefore attempts to balance responsibility and liability of Party A when it happens upon Inadvertently Obtained Information. Regulations 8.4.2 through 8.4.6 set out obligations of Party A including:

- Notifying Party B that it left personal data behind in the Inadvertently Obtained Information dataset;

- Give Party B thirty (30) days to collect it;

- Where Party B is reachable, then:
    - expunging any such data from its records if Party B responds positively to Party A's notification; and

    - leaving the notification requirements of Articles 41 and 42 to Party B to follow up on, as necessary

- Where Party B is unreachable, unidentifiable or does not recover the Inadvertently Obtained Information within thirty (30) days, Party A shall:

    - notify the Commissioner about the Inadvertently Obtained Information, providing details of how it was obtained; and

    - Expunge such data from its own records.

Regarding Regulation 8.4.4, Party A may have to store the Inadvertently Obtained Information until such time it may be reasonable to destroy it. The decision to store or

destroy the information should be based on a data protection impact assessment that includes criteria accounting for the likelihood of the information containing personal data, the number of access requests or other interests in any such data that Party A is or becomes aware of, the potential sensitivity of the data, whether maintaining or destroying it constitutes High Risk Processing, and other subjective factors to be determined on a case by case basis.

Affected parties, including data protection officers or practitioners, or Data Subjects to which the personal data on the information belongs may also raise a complaint to the Commissioner regarding the mishandling of the information and any associated risks of it being left behind and collected by a third party. Likewise, such parties may wish to seek redress in the DIFC Courts to ensure relevant rights under applicable data protection laws or other relevant laws are reviewed for enforceability and, where necessary, enforced.

Where required by court order or other similar instrument that it comes to know of, Party A may be required to provide a copy of the Inadvertently Obtained Information to government or law enforcement authorities, in line with relevant government data sharing principles and guidelines, or as required by applicable laws, such as Article 28 of the DP Law.[1]

Unless Party A's actions meet the conditions of Regulation 8.4.6, Party A would not be liable in the way an ordinary Controller of Personal Data might, and may also be entitled to costs and other compensation to ensure the handling and eventual disposal of the Inadvertently Obtained Information does not leave them out of pocket.

Party A should not use or dispose of the information left behind for its own benefit, as this is often unethical and unfair to Party B, who may legitimately want this data back. It may be proprietary information, or simply valuable client and employee information that it did not intend to misplace.

Impact on Party B

Party B may be subject to recommended actions for proper retrieval or disposal of the Inadvertently Obtained Information, as well as sanctions and fines for breach of the DP Law or a direction to notify affected Data Subjects that a Personal Data Breach was committed involving their personal data. The Commissioner may order Party B to pay costs related to storage, access, assessment, disposal or other treatment of the contents, either directly or via court order. Party B may also be fined for failure to comply with the

[1] *DIFC or third party landlords should engage in an Article 28 assessment and review Article 28 guidance at such time. OECD guidelines on government access to personal data held by private sector entities may also have relevance.*

general principles of the DP Law, regarding the obligation to implement and maintain technical and organisational measures to protect Personal Data in accordance with Article 14(2).

Finally, the DIFC Commissioner's Office reiterates that *any* finder of this type of information, especially where it contains or may contain personal data, must be mindful of the rights of the both the Data Subject and the original Controller (in most cases, this will be Party B). Data protection principles, especially that of fair and lawful processing, should always be at the core of any third party's decision-making process or policies developed and implemented to address such circumstances.

5. What Happens When Reported?

The Commissioner may investigate a breach and may take enforcement action where required. A data subject may also report a breach or request an investigation, at which time the Commissioner will determine whether any follow up should be completed.

6. Applicable Laws and Regulations

Data Protection Law, DIFC Law No. 5 of 2020: the current governing data protection law of the Dubai International Financial Centre, supported by the DIFC Data Protection Regulations 2020.

There are several laws with breach reporting requirements that may apply in addition to the DIFC DP Law 2020, the most common for DIFC entities being those listed below, including but not limited to:

UK General Data Protection Regulation and the UK Data Protection Act 2018: The 'UK GDPR' sits alongside an amended version of the DPA 2018.

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring taking place in the UK of individual's behavior.

Remember as well that the European regulation, the EU GDPR may also apply.

General Data Protection Regulation (EU) 2016/679: the EU GDPR is the current governing data protection law of the European Union that has wide-reaching applicability and contains general requirements about Personal Data security breaches.

7. Applicability

The DIFC DP Law 2020 is always applicable in the DIFC to all DIFC entities and in some cases, those they do business with. Please see Article 6(3) of the DIFC DP Law 2020. The above-named laws may also be applicable in the DIFC and the GCC.

Other country's laws may also be applicable to your business, in cases where for example your parent company or group is based in another jurisdiction with data protection laws in place. Bear in mind that many, including the DIFC DP Law 2020, share similar principles and time-based actions.

Compliance with the DP Law and regulations is therefore critical to the operations of any business or other legal entity based in the DIFC. Administrative fines under such regulations can be very steep, and that's without considering the fines that may be imposed under the DP Law.

8. Questions and Comments

Please contact the DIFC Commissioner of Data Protection either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office for any clarifications or questions related to this document. You may also wish to refer to the DIFC Online Data Protection Policy.