DIFC DATA PROTECTION GUIDANCE

Commissioner of Data Protection

NOTIFYING THE COMMISSIONER OF DATA PROTECTION OF A SECURITY BREACH

Contents

1. Introduction

Security 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, rather than an assessment left solely to the entity involved in a breach. 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 others still set out a time-based requirement of 72 hours (including, for example the EU General Data Protection Regulation) 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.

All capitalized terms have the same meaning as the defined terms in the DP Law.

2. How to Report a Security Breach

If your business is processing Personal Data or Sensitive Personal Data, and a breach occurs, please report it to the Commissioner of Data Protection Office as follows:

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: roc.helpdesk@difc.ae

3. What Should be Reported

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

- unauthorised 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

This list is not exhaustive. Please include any other relevant information you think the Commissioner needs to know.

4. What Happens Once Reported?

The Commissioner of Data Protection may investigate a breach if deemed necessary, 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.

5. 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.

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

e-Privacy Directive / Regulations: the Privacy and Electronic Communications Directive 2002/58/EC, which has been enacted in all EU Member States (i.e., in the UK it is embodied in the Privacy in Electronic Communications Regulations 2003), and is undergoing transformation into a new, updated EU regulation

that will align with the GDPR. In other words, the e-PR can be thought of as a specialised subset of rules that fall under the overall privacy framework established by the GDPR.

6. Applicability

All of the above-named laws may be applicable in the DIFC and the GCC. The DP Law is directly applicable to any business registered in the DIFC.

The GDPR has a very broad reach with respect to its applicability. In short, broadly, an entity with links to an EU establishment, including processing Personal Data in Europe, and / or that entity providing access to a website that allows it offer goods or services to, or to monitor, target or track the interests and preferences of an EU data subject, allow for the GDPR to apply to the entity's Personal Data processing operations. The security breach requirements of the GDPR therefore apply as well. Further, the e-Privacy Directive / Regulation incorporates breach notification requirements. Still other country's laws may also be applicable to your business, bearing in mind again that many share similar principles and time-based actions.

Compliance with these 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.

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.