Personal data breaches in the Dubai International Financial Centre

Charlotte Sutcliffe - Associate - Digital & Data
- Dubai International Financial Centre

The Dubai International Financial Centre ('DIFC') has issued a new DIFC Data Protection Law, DIFC Law No. 5 of 2020 ('DIFC Data Protection Law'). The DIFC Data Protection Law replaces the previous DIFC data protection law, DIFC Law No. 1 of 2007.

Modelled on Europe's General Data Protection Regulation ('GDPR'), the DIFC Data Protection Law provides enhanced standards and controls for the processing and movement of personal data by controllers and processors, and protects the fundamental rights of data subjects. One purpose of the DIFC Data Protection Law is to protect the fundamental rights of data subjects, including how such rights apply to the protection of personal data in emerging technologies.

In this article, we explore the obligations on 'controllers' (i.e. entities that control the processing of personal data) and 'processors' (i.e. entities that process personal data under the direction of a controller) to notify the DIFC Data Protection Commissioner, and affected data subjects, in the event of personal data breach incidents.

Guarding against personal data breaches

Guidance issued by the Commissioner of Data Protection sets out that controllers and processors should consider the following matters with regards to enhancing information security and protecting against personal data breaches:

- what are the biggest areas for security breach or unauthorised data access or loss?
- are physical security measures considered in information security policies?
- how are the staff trained about breaches, reporting, and incident management?
- is there an incident management policy?

Controllers and processors should prepare an incident response plan to ensure the correct procedures are followed to reduce the risk of personal data breaches, and to know what to do if a breach incident occurs. The incident response plan should be aligned to the personal data breach requirements in the DIFC Data Protection Law.

Controllers and processors should ensure they provide specific DIFC Data Protection Law training to personnel, including training focussed on data breach incidents. Such training will assist personnel in recognising data breach incidents, which can take a variety of forms, ranging from inadvertently sending an email to the wrong recipient through to sophisticated hacking events.

Notification to the DIFC Commissioner of Data

Protection

The DIFC Data Protection Law sets out that if there is a personal data breach that compromises a data subject's confidentiality, security or privacy, the controller involved shall, "as soon as practicable" in the circumstances, notify the personal data breach to the DIFC Commissioner of Data Protection. If a processor discovers a personal data breach, the processor is required to notify the relevant controller without undue delay.

The notification to the Commissioner should:

- describe the nature of the personal data breach, including (where possible) the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the Data Protection Officer (where applicable) or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken, or proposed to be taken, by the controller to address the personal data breach, including (where appropriate measures to mitigate its possible adverse effects).

Notification to data subjects

When a personal data breach is likely to result in a high risk to the security or rights of a data subject, the controller shall communicate the personal data breach to an affected data subject as soon as practicable in the circumstances. If there is an immediate risk of damage to the data subject, the controller shall promptly communicate with the affected data subject in clear and plain language containing the following information (at the least):

- the nature of the personal data breach;
- the name and contact details of the Data Protection Officer (where applicable) or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures taken, or proposed to be taken, by the controller to address the personal data breach, including (where appropriate, measures to mitigate its possible adverse effects.

The Commissioner has the option to communicate the personal data breach to the data subjects where there is a high risk to the security or rights of the data subjects involved, or otherwise direct the controller to make a public communication disclosing that the personal data breach has occurred.

Comparison to the GDPR position

The DIFC position in relation to personal data breach notification obligations is similar to the GDPR approach, but there are some distinct differences:

- **Breach notification to the Commissioner**: Whereas the DIFC Data Protection Law requires notification to the DIFC Commissioner as "as soon as practicable", the GDPR imposes a stricter timeframe of reporting a breach to the supervisory authority within 72 hours after becoming aware of such breach.
- **Breach notification to data subjects**: Both the GDPR and the DIFC Data Protection Law require

breach notification to data subjects in certain circumstances. While the DIFC Data Protection Law requires disclosure where the breach is likely to result in a "high risk to the security or rights of a data subject", the GDPR requires disclosure to the data subject where the Personal Data Breach is likely to result in "a high risk to the rights and freedoms of natural persons". Note that whilst data subjects are "identified or identifiable natural persons", natural persons do not necessarily have to be identified.
    - Whilst the DIFC Data Protection Law requires disclosure to the data subject as soon as practicable in the circumstances, the GDPR requires the communication of the Personal Data Breach to the data subject "without undue delay". Arguably, "without undue delay" conveys more of a sense of urgency than "as soon as practicable", which suggests that whilst notification should be done soon, it can be delayed until practicable.
    - Whilst the GDPR creates an exemption for the data subject notification requirement (where the controller has implemented appropriate technical and organisational measures, and the controller has taken subsequent measures which ensure that the high risk to the rights of data subjects is no longer likely to materialise), the DIFC Data Protection Law does not include such an exemption. While this could be read as indicating the duty to communicate the breach to the data subject is absolute under the DIFC Data Protection Law, consideration also needs to be given to the threshold question of whether the breach is likely to result in a "high risk to the security or rights of a data subject".
- **Fines**: Under the GDPR, fines can exceed 20 million euros or up to 4 per cent of an entity's global turnover. When calculating fines for breaches of the DIFC Data Protection Law, there is no reference to the percentage of an entity's worldwide turnover. The DIFC Data Protection Law imposes a fine of up to US$50,000 for failing to notify a data breach to either the Commissioner or to the data subject.

Conclusion

Controllers and processors subject to the DIFC Data Protection Law must ensure they are across all obligations with respect to data breach notification obligations, including with regard to notifications to the Commissioner of Data Protection and to affected data subjects. Besides the risk of fines and claims for damages, failure to act appropriately in addressing data breach incidents can also result in reputational damage.

For more information, please contact Martin Hayward (m.hayward@tamimi.com) or Charlotte Sutcliffe (c.sutcliffe@tamimi.com).