GUIDANCE ON RETENTION AND STORAGE OF PERSONAL DATA

Commissioner of Data Protection

CONTENTS

1. Introduction

The Dubai International Financial Centre and/or its affiliates and entities (collectively "DIFC", "DIFCA") values individuals' security and privacy. DIFC has its own Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law"), and may for certain types of Personal Data processing also apply the laws from other jurisdictions.

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. Purpose of this Guidance

Compliance with the DP Law requires good records management, data governance and data security. Article 9 sets out the privacy principle that organisations should only keep data that is "relevant and limited to what is necessary in relation to the purposes described in Article 9(1)(c)." Article 14 requires compliance policies and procedures, including technical and organisational measures, that provide a foundation for proper access to, storage or and dissemination of Personal Data.

In complying with Article 14, your organisation should seek to identify the minimum amount of Personal Data it is required to hold in order to properly fulfil the purpose for which it was collected, accounting for other legal requirements as well that may necessitate storing this data. This will be a question of fact in each case. Where an organisation holds the Personal Data of several individuals but only requires the Personal Data of a few of those individuals to fulfil a specific processing purpose or purposes, it is possible that the amount of Personal Data the relevant entity holds is "excessive". This is an assessment each organisation needs to make, document and review on a regular basis.

Any Personal Data held that is not required to fulfil the purpose should be deleted, archived or put beyond further use. It is not acceptable to hold Personal Data on the basis that the Personal Data may be useful in the future without knowing how it will be used. This situation needs to be distinguished from holding Personal Data in the case of a particular foreseeable contingency which may never occur. For example, where an employer holds an employee's health information for emergency situations, maintaining data for this purpose may be permitted, based on a clear, well-documented and well-reasoned assessment.

Entities that retain and store Personal Data should continually monitor compliance with the retention provisions which have obvious links with the other provisions in the DP Law. Changes in circumstances or failure to keep Personal Data up to date may mean that the Personal Data that was originally adequate becomes inadequate. If Personal Data is kept for longer than necessary then it may be both irrelevant and excessive. In most cases, relevant entities should be able to remedy possible breaches of the DP Law 2020 by the erasure or addition of particular items of Personal Data.

Please note that there is no prescribed time limit for retaining data under the DIFC DP Law 2020 or under many other data protection laws. Again, it is an assessment the company itself must make and a policy that documents the approach is highly recommended.

4. Records filing and location

Put minimum standards in place for the creation of records and effective mechanisms to locate and retrieve records.

Playbook:

- Create and maintain policies and procedures to ensure that you appropriately classify, title and index new records in a way that facilitates management, retrieval and disposal.
- Identify where you use manual and electronic record-keeping systems and maintain a central log or information asset register.
- Ensure that your organisation has a proper document versioning and management system in place and that all records are indexed at all times, including the ability to track movement (authorized and unauthorized) of data, and data loss prevention and notification measures.
- Archive and index records stored off-site with unique references to enable accurate retrieval and subsequent tracking.

5. Security

Ensure appropriate security measures are in place to protect data that is in transit, including incoming or outgoing data (import and export of data to and from other organisations).

Playbook:

- Include in any organisational privacy policy and training information about the rules protecting the internal and external transfer of records by post, fax and electronically.

- Minimise data transferred off-site and keep it secure in transit.

- Use an appropriate form of transport for offsite data storage (for example secure courier, encryption, secure file transfer protocol (SFTP) or Virtual Private Network (VPN)) and check that the information has been received.

- Put agreements in place with any third parties used to transfer business information between your organisation and third parties.

6. Quality Assurance

Implement procedures to make sure that records containing Personal Data are accurate, adequate and not excessive.

Playbook:

- Conduct regular quality impact reviews of Personal Data to make sure they are accurate, adequate and not excessive.

  Accuracy is key as processing out of date information could result in life-changing results when data is part of automated decision-making, or even in an emergency situation or cases of fraud that may cause significant harm to individuals relying on services that require processing this information. It is of course up to the individual as well to provide accurate data and keep it up to date. Generally, however, if your business regularly processes Personal Data and specifically if it offers services that need accurate data to properly provide them, doing a quality audit of the accuracy of the data is essential. Records containing Personal Data (whether active or archived) should be refined periodically to assure that it is adequate and to reduce the risks of inaccuracies and excessive retention.

  But what is an “adequate” or “not excessive” amount of Personal Data?

  The term “adequate” in this context aligns with the principles of minimisation, meaning that the Personal Data your business processes is enough to fulfil the purposes for which it is collected and processed. “Not Excessive” may be a bit clearer, but there are important legal concepts that underpin this term that a business must understand. It means that only as much data as is reasonable or necessary to complete a task is maintained for as long as needed, that the risk of harm in processing that data is mitigated, and overall retention is proportionate to the requirement. An impact assessment is usually a good way to determine whether your business is processing the “right” amount of data. The balance of the amount of data businesses believe they need and how much they actually need may be

surprising, especially as most controllers and processors are conditioned to collect as much as possible – often for what they think are regulatory requirements. Perhaps other regulations require collection of a significant amount of data, and any impact assessment should be made through this lens.

- Train your teams about data quality issues following data quality checks or audits to prevent recurrence, assess risks and fill quality gaps.

  The key issue in training is often around helping staff understand what they can and cannot delete from inboxes, shared drives, share with others, and how and when to request accurate information. Training around carrying out a realistic, pragmatic audit of data geared to objective compliance with the DP Law is essential as well.

7. Retention

Create a retention schedule that sufficiently outlines storage periods for all Personal Data, which you review regularly.

Playbook:

- Build a retention schedule based on business needs with reference to statutory requirements and other principles (for example employment, tax, or health law requirements).

- Provide complete information in the schedule including full coverage of all relevant categories, and how disposal decisions should be processed in line with the schedule.

- Ensure that retention, privacy or security champions (someone responsible, in a formal program, perhaps) support staff information about adherence to the schedule.

- Review it regularly.

- Regularly review retained data to identify opportunities for minimisation, pseudonymisation or anonymisation; document any such decisions in the schedule.

8. Destruction

Implement methods of deletion and destruction of records that are appropriate to prevent disclosure of Personal Data prior to, during or after disposal. Review whether a "legal holds" process should be implemented for certain data managed by key stakeholders.

Playbook:

- For paper documents, use locked waste bins for records containing Personal Data, and implement either in-house or if possible, secure third party cross shredding or incineration is in place.
- For information held on electronic company-issued devices, wiping, degaussing or secure destruction of hardware (shredding) is in place. Align similar measures with a bring your own device policy (if any; please see below for further guidance).
- Securely hold, collect or send away confidential waste awaiting destruction, preferably in a secured location for waste to be collected daily if possible or until collected for disposal internally or by a third party.
- Where third parties are contracted to dispose of Personal Data, obtain appropriate assurances of secure data disposal, for example through audit checks and destruction certificates.
- Maintain a log of all equipment and confidential waste sent for disposal or destruction.
- Create a secure storage area for equipment awaiting disposal or on "legal hold", meaning they cannot be wiped or formatted for purposes of litigation, or other regulatory requirements (please see below for further guidance).

9. Mobile devices, home or remote working and removable media

You have appropriate mechanisms in place to manage the security risks of using mobile devices, home or remote working and removable media.

Playbook:

- You have a mobile device and a home/remote working policy that demonstrates how your organisation will manage the associated security risks.
- You have protections in place to avoid the unauthorised access to or disclosure of the information processed by mobile devices, for example, encryption and remote wiping capabilities.
- You implement security measures to protect information processed when home or remote working, for example VPN and two-factor authentication.
- Where you have a business need to store Personal Data on removable media, you minimise Personal Data and your organisation implements a software solution that can set permissions or restrictions for individual devices as well as an entire class of devices.
- Your organisation uses the most up-to-date version of its remote access solution. You are able to support and update devices remotely.
- You do not allow equipment, information or software to be taken off-site without prior authorisation and you have a log of all mobile devices and removable media used and who they are allocated to.

10. Secure areas

You secure physical business locations to prevent unauthorised access, damage and interference to Personal Data.

Playbook:

- You protect secure areas (areas that contain either sensitive or critical information) by appropriate entry controls such as doors and locks, alarms, security lighting or CCTV.
- You have visitor protocols in place such as signing-in procedures, name badges and escorted access.
- You implement additional protection against external and environmental threats in secure areas such as server rooms.

- Office equipment is appropriately placed and protected to reduce the risks from environmental threats and opportunities for unauthorised access.
- You securely store paper records and control access to them.
- You operate a clear desk policy across your organisation where Personal Data is processed.
- You have regular clear desk 'sweeps' or checks and issues are fed back appropriately
- You operate a 'clear screen' policy across your organisation where Personal Data is processed.

11. Business continuity, disaster recovery and back-ups

You have plans to deal with serious disruption, and you back up key systems, applications and data to protect against loss of Personal Data.

Playbook:

- You have a risk-based Business Continuity Plan to manage disruption and a Disaster Recovery Plan to manage disasters, which identify records that are critical to the continued functioning of the organisation.
- You take back-up copies of electronic information, software and systems (and ideally store them off-site).
- The frequency of backups reflects the sensitivity and importance of the data.
- You regularly test back-ups and recovery processes to ensure they remain fit for purpose.

12. Other useful tools for good document and data retention governance

Information asset register

Maintain an asset register that records assets, systems and applications used for processing or storing Personal Data across the organisation.

Acceptable software use policy

Identify, document and implement rules for the acceptable use of software (systems or applications) processing or storing information.

Access control

Limit access to Personal Data to authorised staff only and regularly review users' access rights.

Unauthorised access

You prevent unauthorised access to systems and applications, for example by passwords, technical vulnerability management and malware prevention tools.

Accountability

Have you considered the effectiveness of your accountability measures?

- Can staff find the above policies and procedures?
- Are they aware of the main contents?
- Are staff aware of the retention schedule?
- Do they adhere to it?
- Could staff explain what their responsibilities are and how they carry them out effectively?
- Would a sample set of devices have appropriate encryption?
- Could you demonstrate appropriate access arrangements for home or remote working?
- Are staff working from home or remotely aware of the authorisation requirements?
- Are printer/fax areas secure?
- Do staff follow protocols and are they clearly communicated?
- Would we see appropriate environmental controls in your secure areas?
- Would a tour of your offices reveal an effective clear desk policy?
- Are screens left unlocked?
- Do staff know how to classify and structure records appropriately?
- Is the asset register kept up to date?
- Have there been any issues locating records?
- Do staff know how to send emails or information by post or fax securely?
- Have they been using appropriate forms of transport?

If you are still unsure what to do, please review the Guide to Data Protection Law and the Assessment Tools available on the Guidance page of the DIFC DP website.

13. 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.