Dubai International Financial Centre

Office of the Commissioner of Data Protection - UPDATE

Presented by

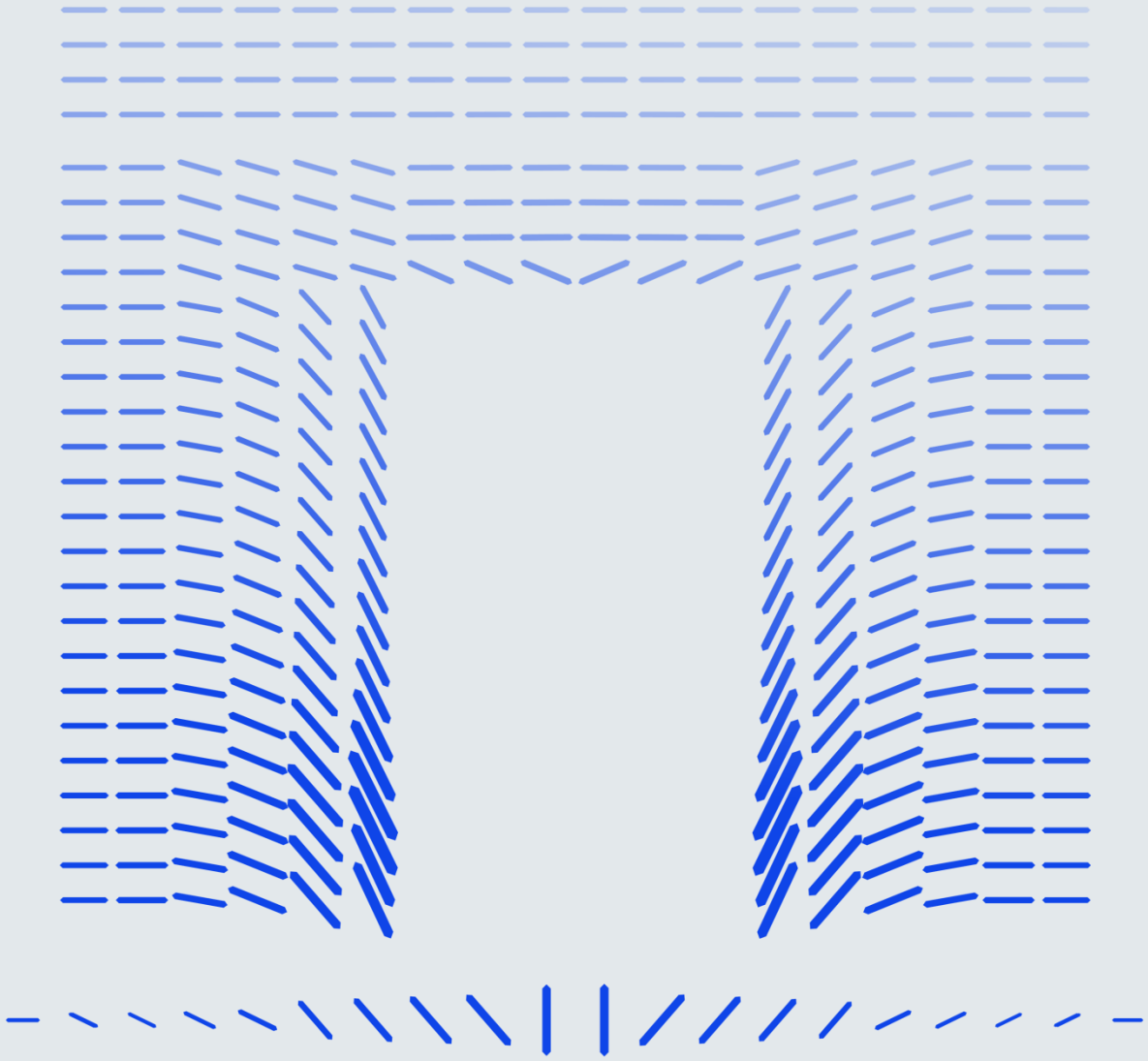
Lori Baker, DIFCA Director of Data Protection

Veena Dorairajan – DIFCA DPO

Ken Coghill – Assoc. Director, Operational Risk, DFSA

14 December 2020

Version: 2.4



01

Side by Side

DIFC DP Law 2007

DP Law 2020

Key updates

Data Protection in the DIFC – Side by Side

2007	2020	KEY UPDATES
Accountability	Accountability - Reinforced	Introduction of DPO and other controls such as prior consultation and processor provisions; enhanced Controller and Processor obligations.
Data Subjects Rights	Data Subjects Rights	Same rights, but aligned to absorb impact of emerging technology
Security breach reporting	Security breach reporting - Enhanced	The processor must now play a larger role in accountability overall and for breach reporting, and the data subject him or herself must be informed in certain cases
International Transfers	International Transfers - Realigned	Enhanced to align with current international adequacy standards, processors more accountable, additional mechanisms (i.e., BCRs) recognized
Data Protection Principles	Data Protection Principles	Same principles, but promotes concepts of structure, governance and risk-based approach to compliance (i.e., via PIAs, Codes, etc)
Notifications and applicability	Notifications and applicability	Still required, for all entities to notify one way or the other; applicability is set out in detail

Is it like the GDPR?

DIFC DP Law 2020 is based on not only the GDPR but other international DP Laws, as they all contain similar principles and components these days, and they feed each others best practices. But if you are curious…

Clyde & Co published an article that will help answer this question more specifically.

Regarding Security Breach Reporting… the DIFC Law is similar, but does not have a 72 hour requirement, for starters.

02

Security Breaches

General requirements

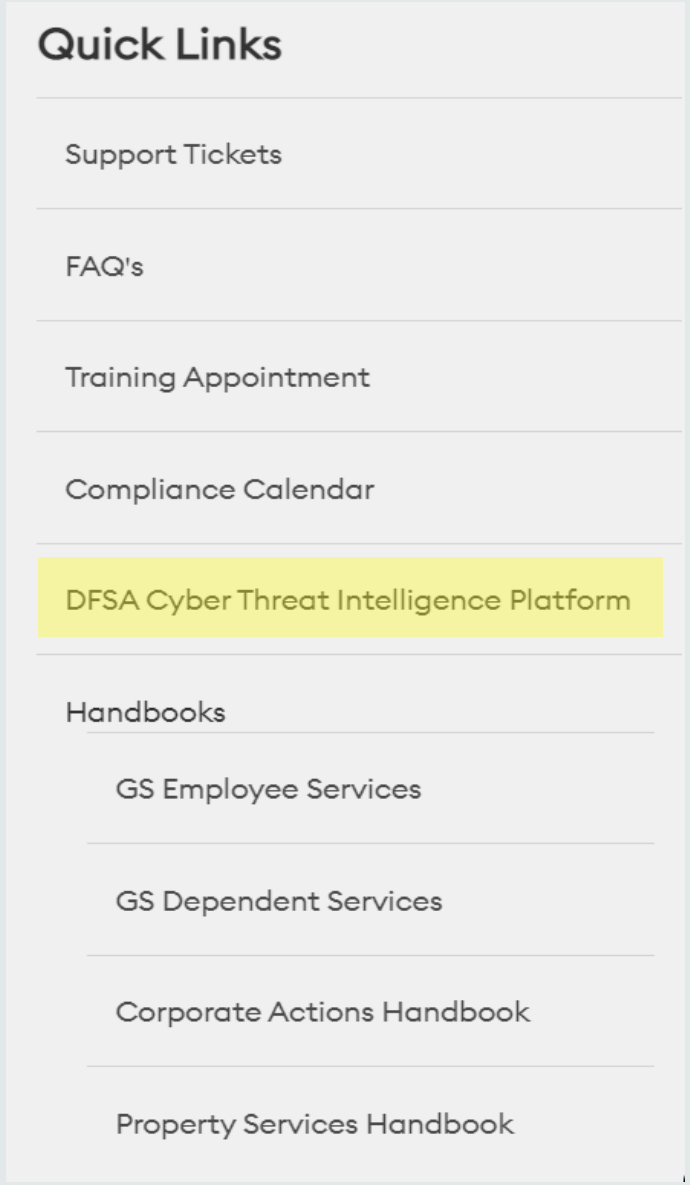
What to look out for

Article 9(1)(i) – Technical and Organisational Measures

Personal Data must be kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction or damage, *using appropriate technical or organisational measures (aka TOM)*

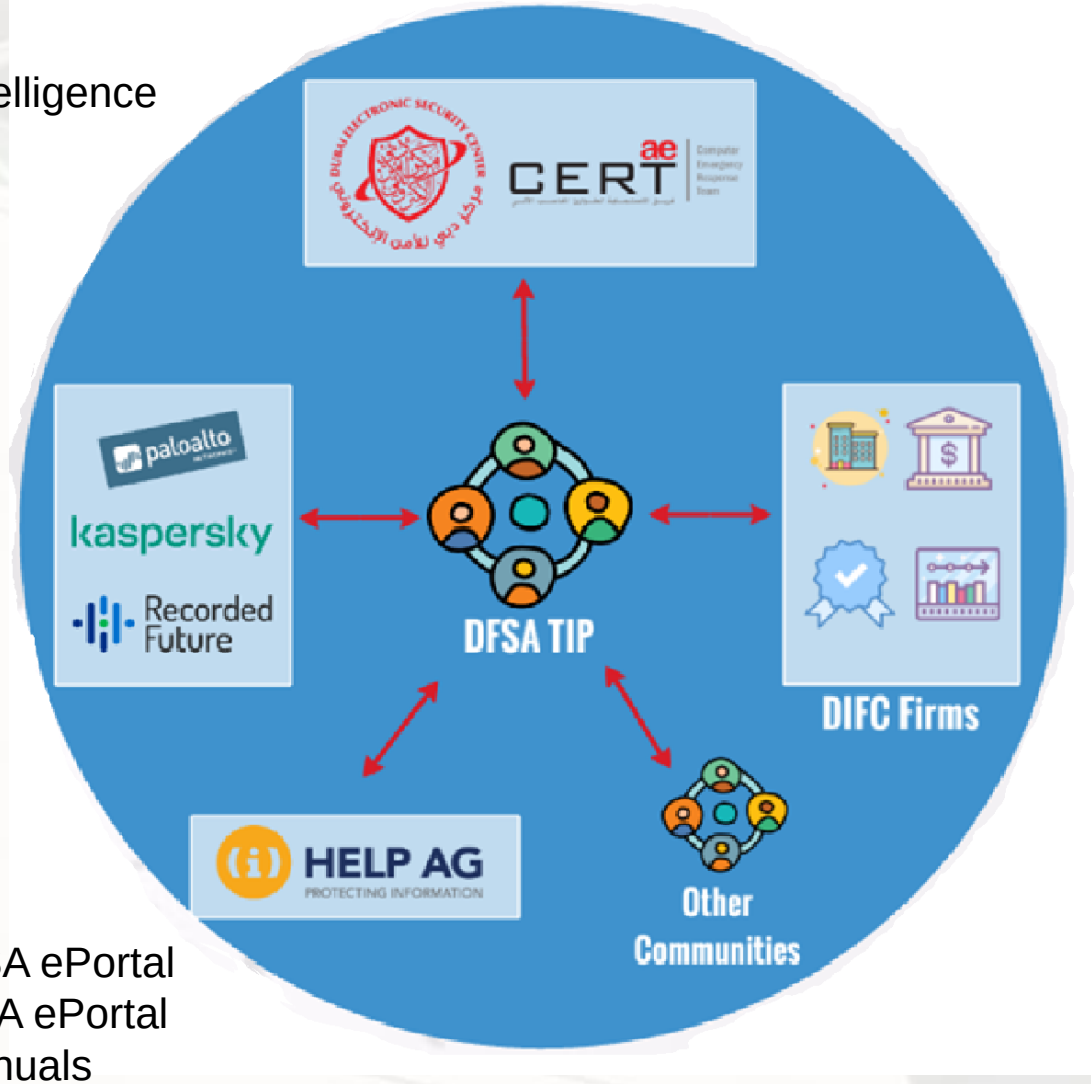
What TOM looks like:

- **Firewalls and IT security**
- **Security and IT information Training**
- **Phishing alert add ons**
- **ISMS policies and processes, certification**
- **External alert tools such as the DFSA Cyber Incident Platform**



DFSA Threat Intelligence Platform

- How it works
  - Mechanism for sharing cyber threat intelligence
  - 3rd party operational management
  - Government cybersecurity agencies
  - 3rd party cybersecurity experts
  - No participation fees
- Progress
  - Launched 21 January 2020
  - 150 + registered users
  - 160 new threats per week
  - Ransomware; phishing; targeting the finance sector and bank customers
- Queries
  - tip@dfsa.ae
- How to sign up
  - DFSA authorised firms access the DFSA ePortal
  - DIFC registered firms access the DIFCA ePortal
  - Terms and Conditions; guides; and manuals



Articles 41 and 42 – Security Breach Reporting to the Commissioner and / or the Data Subject

Article 41 says to report to the COMMISSIONER… "If there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy…"

Article 42 says to report to the DATA SUBJECT… "When a Personal Data Breach is likely to result in a high risk to the security or rights of a Data Subject…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."

NO mention of a specific window in which to report. Why?

What does breach reporting look like?

- clear and plain language the nature of the Personal Data Breach and contain at least the information provided for in Articles 41(4)(b) to (d)
- Where a communication to the individual Data Subjects referred to in Article 42(1) will involve disproportionate effort, a public communication or similar measure by the Controller whereby the Data Subjects are informed in an equally effective manner shall be sufficient

Guidance is available on the DP guidance website

03

Notifications Process

Forms & Fees

When, How, What?

Enforcement

Forms & Fees

Data Protection Notification

Failure by entities to notify the Commissioner of Data Protection ("Commissioner") in accordance with the Data Protection Law and Data Protection Regulations may result in the Commissioner imposing a fine in respect of the contravention as prescribed in Schedule 2 of the Data Protection Law. The data protection notification has to be submitted through the DIFC Client Portal. DIFC-registered entities are required to submit a data protection notification as per the process below:

NEW ENTITIES

The data protection notification is part of the registration/incorporation service request. Note that the DIFC Client Portal will not allow the user to submit the registration/incorporation service request without finalising the data protection notification.

DUTY TO NOTIFY CHANGES

If at any time during the year there are any changes to the registrable particulars, entities must submit a notification to the Commissioner through the DIFC Client Portal using the service request "Data Protection Notification".

DATA PROTECTION NOTIFICATION

The data protection notification renewal is part of the license renewal service request. Prior to submitting the license renewal service request, the user must first confirm if there are any changes to the registrable particulars notified in the manner described previously.

DIFC Client Portal - onboarding

NEW ENTITIES:

During onboarding, a new entity will complete the DP notification whether it (thinks it) Processes Personal Data… or not.

PLEASE DO NOT select that your entity **does not** Process Personal Data:

X If it is only newly established and "technically" doesn't have such data to Process – it has employees, clients, suppliers, etc., all of whom have PD

X To avoid paying the Notification fee – if you Process PD and do not notify, this is a breach of the DP Law and enforcement action can be taken.

A list of all new entities notifying that they do not Process PD is sent to the Commissioner's Office each week for review and a sample of those shared may be contacted for a discussion to understand and support any misunderstandings about DP Law 2020 or how / why to notify.

Notification gets recorded on the public register and may be considered a means of letting the world know on the most basic level how, what and where PD is dealt with by your entity.

KEY TAKEAWAY: *All new (and existing) entities should assess the risks of notifying (or not) based on a realistic, honest view of the PD your entity deals with, and take action accordingly. Document it and be able to justify the decision.*

DIFC Client Portal – existing entities

EXISTING ENTITIES:

Please go back to the DIFC Client Portal at some point soon, or certainly by confirmation statement time, to review your entity's DP notification whether it (thinks it) Processes Personal Data… or not.

PLEASE DO NOT select that your entity **does not** Process Personal Data:

X If it is recently established and "technically" doesn't have such data to Process yet.

X To avoid paying the Notification fee – if you Process PD and do not notify, this is a breach of the DP Law and enforcement action can be taken.

Go to the available Service Requests and select Data Protection. There are a number of new fields that will require adding new information to or even updating existing fields such as "data controller". It's in your interest to update sooner than later.

Notification gets recorded on the public register and acts as a means of letting the world know on the most basic level how, what and where PD is dealt with by your entity.

If you need assistance, please contact the **Registry Services helpdesk on** roc.helpdesk@difc.ae

DIFC DP Law 2020 Enforceable from October 1, 2020

Enforcement comes in when there are clear gaps or breaches of the DP Law 2020. It can range anywhere from directions and further investigations or reporting to other regulators (where strictly necessary), to imposing fines as set out in Article 62.

- General fines
- Administrative fines
- Guidance about fines and sanctions is available on the DP website

Failure to report a security breach in accordance with the DP Law 2020 is a contravention of the law and may be subject to an administrative fine in addition to any general fines for the breach itself.

The Commissioner's Office understands that the last 6 months have had a considerable impact on DIFC businesses, and will be reasonable with respect to enforcement on a case by case basis.

Plans for 2021 include automating additional enforcement activities, some with respect to a notifications review process and take action where necessary.

Any updates or changes will be communicated through normal channels

04

Helpful Resources

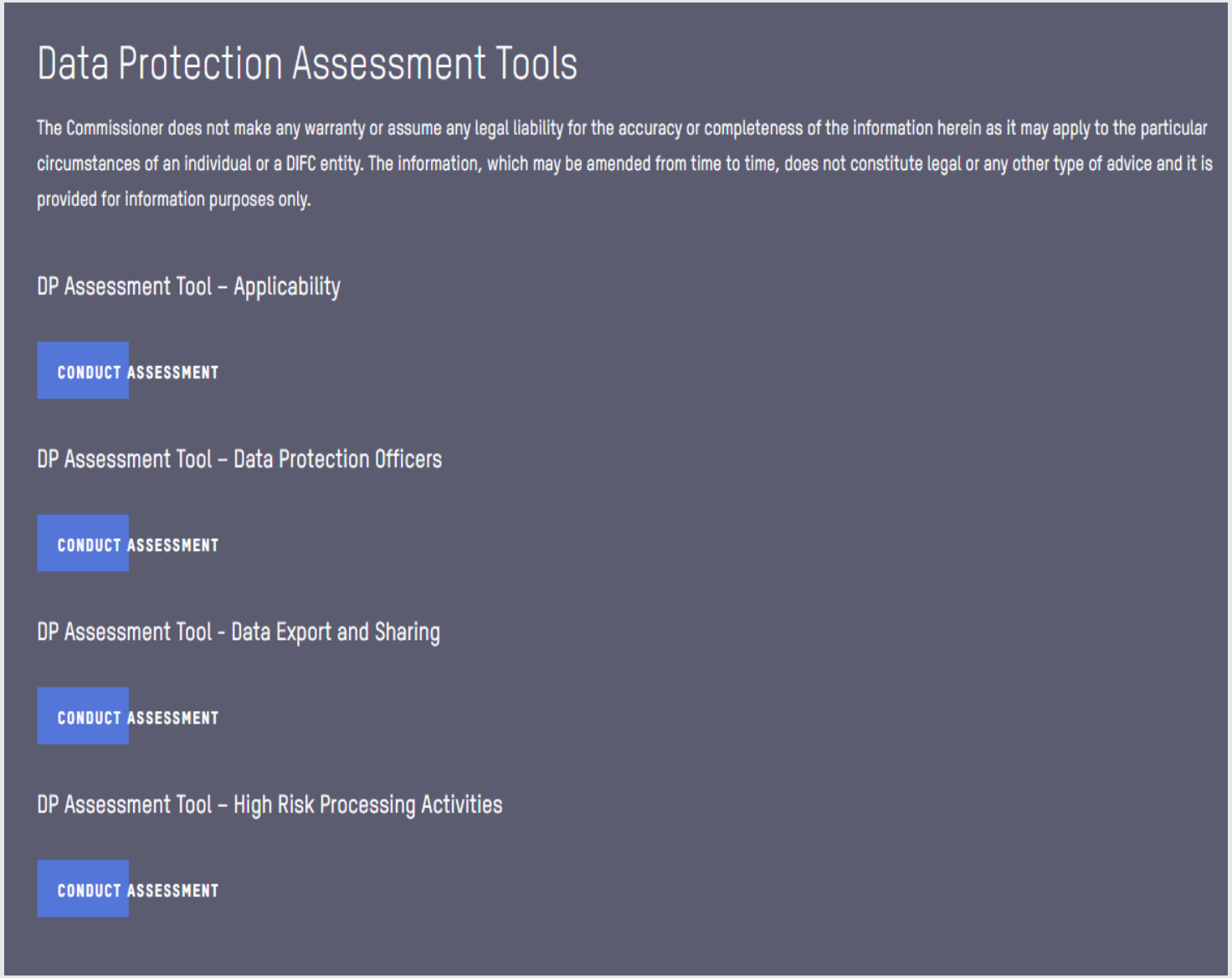
Guidance on DIFC DP Website

General Resources

DIFC DP Website

"Example Compliance Checklist & DPIA"

The Commissioner's Office has posted guidance and assessment tools on several key topic areas of the DIFC DP Law 2020



Other resources

FAQs page and the Guide to Data Protection Law No 5 of 2020 provide extensive information about compliance with the DP Law in general

There is also a set of 4 assessment tools as well: the Applicability Assessment tool, the DPO Assessment Tool , the Export Assessment Tool and the HRP Assessment Tool.

Finally, PWC created a **free** DIFC DP Law Maturity Assessment Tool that you may register for to review your compliance with the DP Law. It is available in both the onboarding process as well as the service request function in the Client Portal.

General Resources List

DIFC DP Website

DIFC DP Law 2020

DIFC DP Regulations

DIFC DP Guidance

DIFC DP FAQs

Clyde & Co article comparing GDPR with DIFC Law

PWC DP Maturity Tool

AML webinar – June 2020

DFSA Cyber Threat Intelligence Platform – press release Jan 2020

Dubai International Financial Centre

Thank You

For more information regarding this presentation, kindly contact:

commissioner@dp.difc.ae