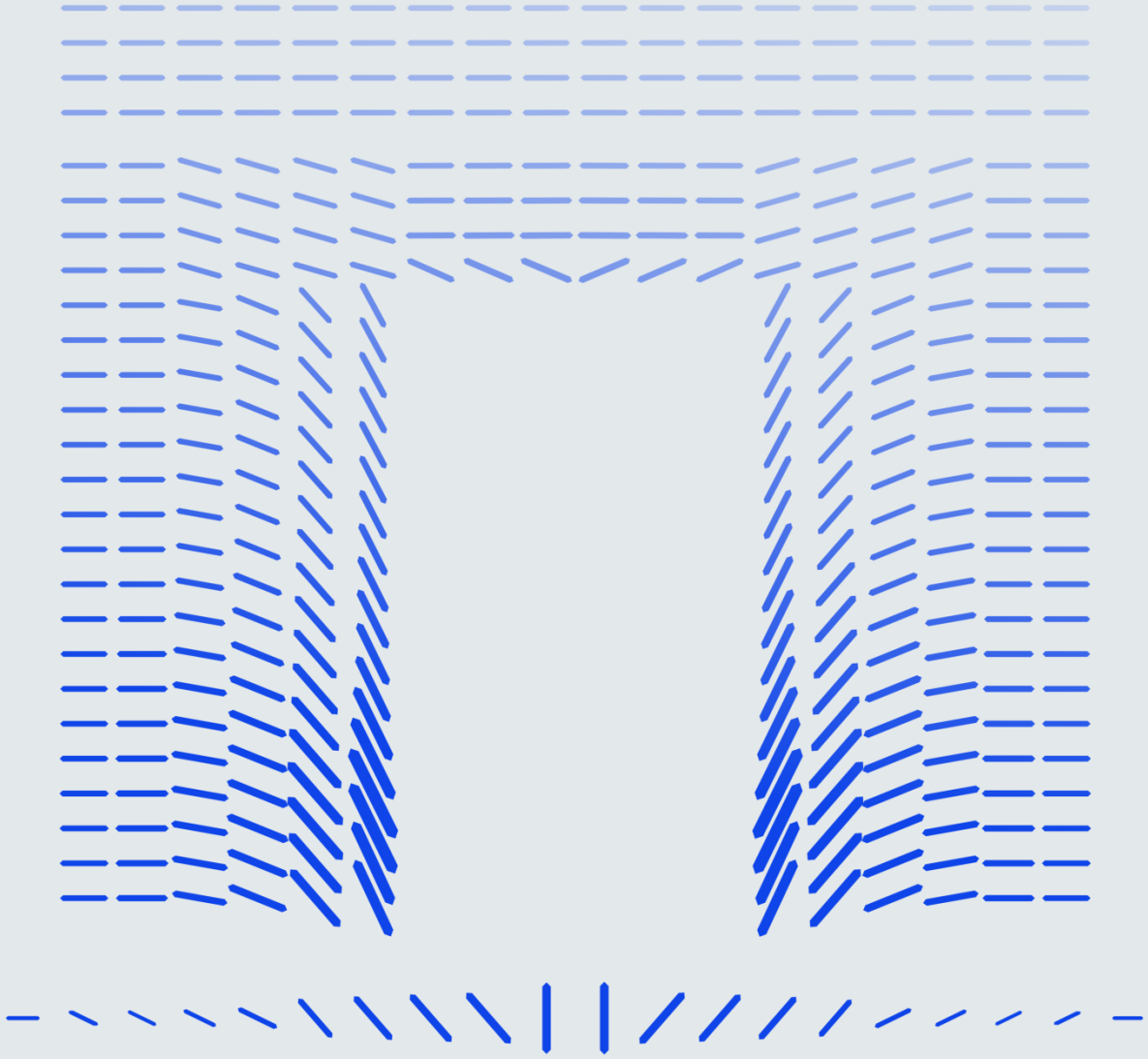
Dubai International Financial Centre

Office of the Commissioner of Data Protection - UPDATE

Presented by
Lori Baker, Director of Data Protection &
Dino Wilkinson, Partner, Clyde & Co.

1 October 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.

02

FAQs

Links to DIFC DP Page

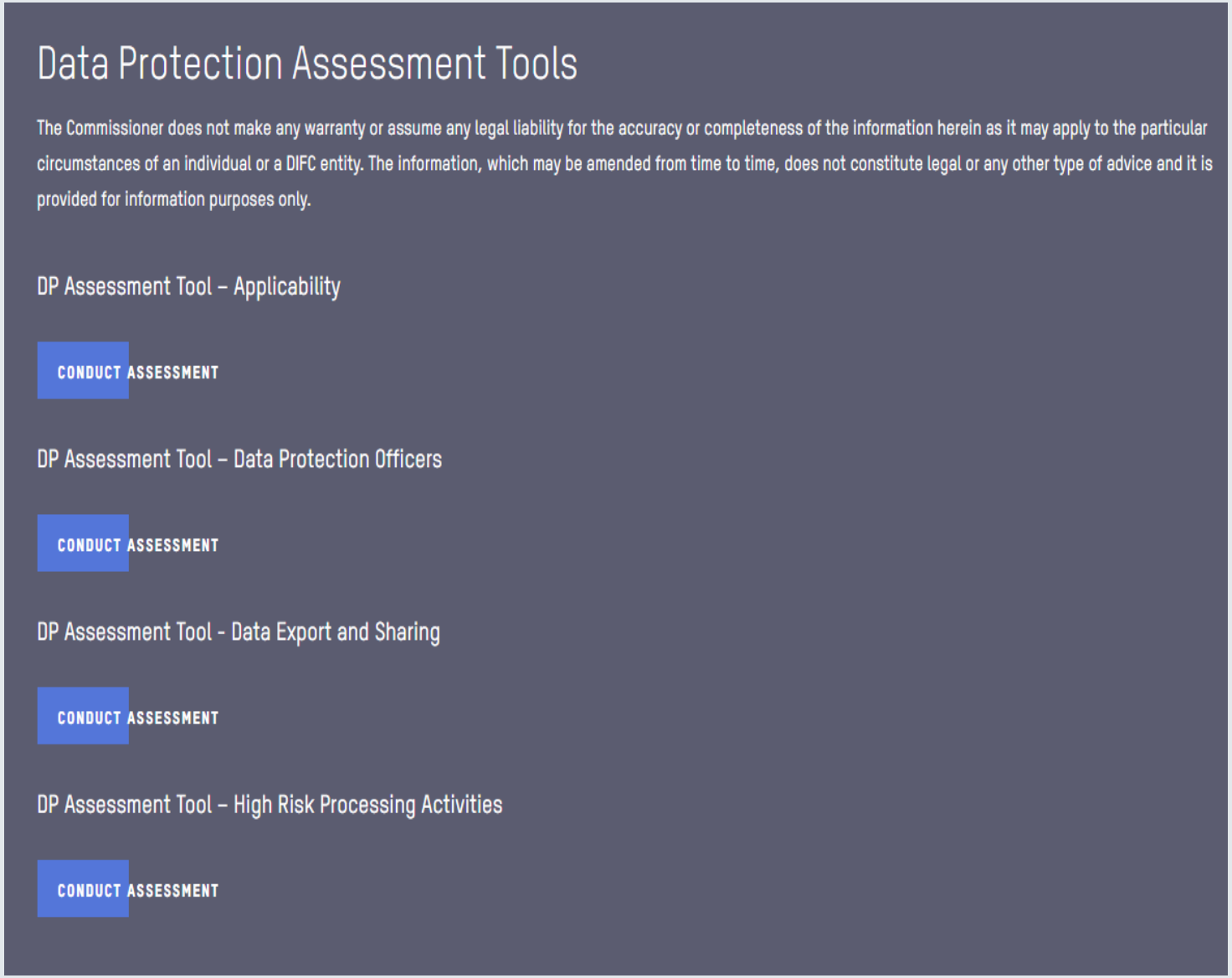
MYTHBUSTING!!

Questions submitted by DIFC clients

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.

COMPLIANCE, NOTIFICATIONS, AND FINES

1. When is the "deadline for compliance" and will there be any extension?

DP Law 2020 is an update of the old law with a few new requirements and clarifications. Theoretically, all entities should have complied previously, and the new requirements have been available for 4 months to implement. We will not therefore provide any extension because compliance is an on-going obligation.

The October 1st date is not a deadline for compliance as such. It is the date from which the Commissioner can take enforcement action such as imposing fines, etc. Articles 14(7) and (8) of the DP Law 2020 state that the notification must be made and must be current (updated regularly). The Data Protection Regulations at Section 3.1.3 require that the notification is made within 14 days of beginning processing of personal data. All relevant sections of the notification must be completed (including ensuring compliance with any obligations set out therein) and associated fees (if any) must be paid to make the update. So at any time through the year, if / when something about DP processing operations changes, the notification must be updated – not just now or "by October 1st".

2. Will fines be issued immediately?

NO - we will take immediate action after October 1 primarily with regard to recognisably serious breaches of the DP Law or those brought directly to our attention, and then make assessments on an ongoing basis regarding any other types of breaches.

3. Do we have to notify either way? *Yes – notify whether you do or don't process personal data.*

4. What happens if my notification is pending in the Portal? *It will be considered in due course. Again, Oct.1 is not a deadline.*

5. What happens if my company is still under formation or doesn't have customers yet? Do I have to notify?

You should notify anyway during onboarding, and if you anticipate having customers or indeed already have employees or shareholders, etc., you are, even on a small scale, processing personal data and will have to assess the risk of filing one way or another. If you document your decision and can justify it, the Commissioner's Office is willing to consider your views but will provide recommendations and take action accordingly.

Supervision and Interpretation

6. How is DP compliance monitored in DIFC? / What is the key approach DIFC is following to identify the non-compliance with Law?

The Commissioner's Office conducts routine scheduled and voluntary inspections.

7. What is the Annual Assessment and when is it due?

The AA is due the first renewal date after July 1, 2021. There is nothing to do now, unless you would like to have a look at the manual form in order to prepare. The form that will be submitted will be automated. It is not the same as the notification, although they do contain similar information. The AA will require more details and is only to be submitted if a DPO is appointed. A DPO must only be appointed as set out in Article 16(2) and (3). ***DIFCA's DPO is VEENA DORAIRAJAN***

8. Do we HAVE to use a CSP or third party consultant to administer our compliance with the DP Law 2020?

Absolutely not.

9. Our data is publicly available, is that the same thing as processing personal data?

Any type of data, public or private, can be personal data. What matters is whether a living individual can be identified from it.

10. What are the Regulations for and what do they say?

The Data Protection Regulations are another important part of implementing the DP Law 2020. They provide specific timelines and instructions about certain topics.

Legal-ese

11. What about transfers to the US in light of Schrems II – are additional safeguards required?

Additional safeguards are always required when transferring out of the DIFC to a non-adequate jurisdiction.

12. Is consent required for the processing of data under the DP Law 2020?

There is extensive guidance on consent on the DIFC DP Guidance page – short answer is no, not always

13. Are companies considered data subjects under the DIFC Data Protection Law or can only individual persons be designated as such?

No – in a few places, yes, but not in DIFC under the current DP Law.

14. What about direct marketing? Is that allowed?

It is but it must be communicated that it will take place using any PD that is collected in simple terms. Please see the direct marketing guidance available on the DIFC DP Guidance page.

15. AML Due Diligence? Which law wins? *Depends on the circumstances, but generally, DP controls should be maintained to the extent possible. See "Substantial Public Interests"…*

16. What is the most important change to take note of?

How long is a piece of thread… ? Accountability for all entities is a biggie…

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

Article on Banking secrecy vs DP Laws (EU / UK view, but relevant)

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.

With the recent digital onboarding enhancements in the portal, you'll notice a difference to the DP section.

Since July 1, 2020, the DP section of the portal covers off your business's compliance with essentially each part of the DP Law 2020

The idea is to ensure that at a bare minimum, through your notification registration with the Commissioner's office, you will have the skeleton basis of a DP compliance program

This will be enhanced as well as we receive feedback about the operation of DP Law 2020

Notifications, payment of and objection to fines and all other matters should be managed through the DIFC client portal as before.

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

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

Review: Key Obligations

Obligations

Relevant articles

Guidance

Key obligations

Primary updates:

- Records of processing activities
- Appointment of DPO / Annual Assessment
- DPIA
- Cessation of Processing procedures
- Data Processing Agreements
- Contractual obligations reflecting:
  - data subjects rights; and
  - additional controls around international data transfers
- Data breach response and notification procedures

MOST IMPORTANT: BUILD A CULTURE OF PRIVACY IN THE BUSINESS

Relevant Articles

Article 15	Requirement	References
	Maintain a written record, which may be in electronic form, of Processing activities under its responsibility, which shall contain at least the following information: (a) name and contact details of the Controller, its appointed DPO, where applicable, and Joint Controller, if any; (b) the purpose(s) of the Processing; (c) a description of the categories of Data Subjects; (d) a description of the categories of Personal Data; (e) categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in Third Countries and International Organisations; (f) where applicable, the identification of the Third Country or International Organisation that the Personal Data has or will be transferred to and, in the case of transfers under Article 27, the documentation of suitable safeguards; (g) where possible, the time limits for erasure of the different categories of Personal Data; and (h) where possible, a general description of the technical and organisational security measures referred to in Article 14(2).	procedures ROPA template (spreadsheet or other database)
Article 16	Requirement	References
1	Appoint a DPO if required (and then see Articles 17 to 19 inclusive)	internal privacy policy online privacy policy / notification procedures
4	If not required, appoint a person responsible for DP compliance / communications with Commissioner's Office	internal privacy policy procedures
Article 20	DPO / entity to regularly conduct Data protection impact assessments when necessary, i.e., HRP (required); or at the start of a new project / updating existing operations (best practice)	internal privacy policy procedures

Obligations (2)

Article 22	Where the basis for processing under Article 10 changes for any reason, processes are in place for ensuring one of the following actions is taken with respect to the Personal Data: (a) securely and permanently deleted; (b) anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released; (c) pseudonymised; (d) securely encrypted; or Where a Controller is unable to ensure that Personal Data is securely and permanently deleted, anonymised, pseudonynmised or securely encrypted, the Personal Data must be archived in a manner that ensures the data is put beyond further use (in accordance with Article 22(3) and accounting for Article 22(4)	internal privacy policy procedures
Articles 23, 24 and 25	Sign appropriate written data processing agreements between your organization and any 3rd parties	contracts / agreements
	Ensure any privacy policies include a requirement that processing done in your organization is confidentially and only under specific instructions.	internal privacy policy procedures
Article 26	Determine where and personal data is transferred for processing outside of the DIFC. If adequate jurisdiction, no further action is required but update notification to Commissioner	internal privacy policy online privacy policy / notification to Commissioner record of processing activities contracts / agreements
Article 27	Determine where and personal data is transferred for processing outside of the DIFC. If not an adequate jurisdiction, ensure one of the requirements in Article 27(1)(a to c) is met. Also update notification to Commissioner	internal privacy policy online privacy policy / notification to Commissioner records of processing activities contracts / agreements
Article 29 and 30	Privacy notices (i.e., online privacy policy telling data subjects what you're doing with the PD collected)	internal privacy policy (article 31(3)) online privacy policy / notification procedures
Articles 32 to 40	Written policies that provides for data subjects rights contained in relevant articles	internal privacy policy online privacy policy / notification procedures
Articles 41 and 42	Written policy and / or incident management procedure that provides for steps to take when a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed occurs (aka a Personal Data Breach) that accounts for : -- notification of DP Commissioner -- where required, notification of data subject	internal privacy policy procedures

As always, questions for the Commissioner's Office are welcome

If you would like to take advantage of the consultation period for processing that your organization is considering, or want to engage in a voluntary supervisory visit, please let us know

Review your business’s DP status currently and prepare to update as needed both within your organization and on the portal to align with the DP Law 2020

Dubai International Financial Centre

Thank You

For more information regarding this presentation, kindly contact:

commissioner@dp.difc.ae