



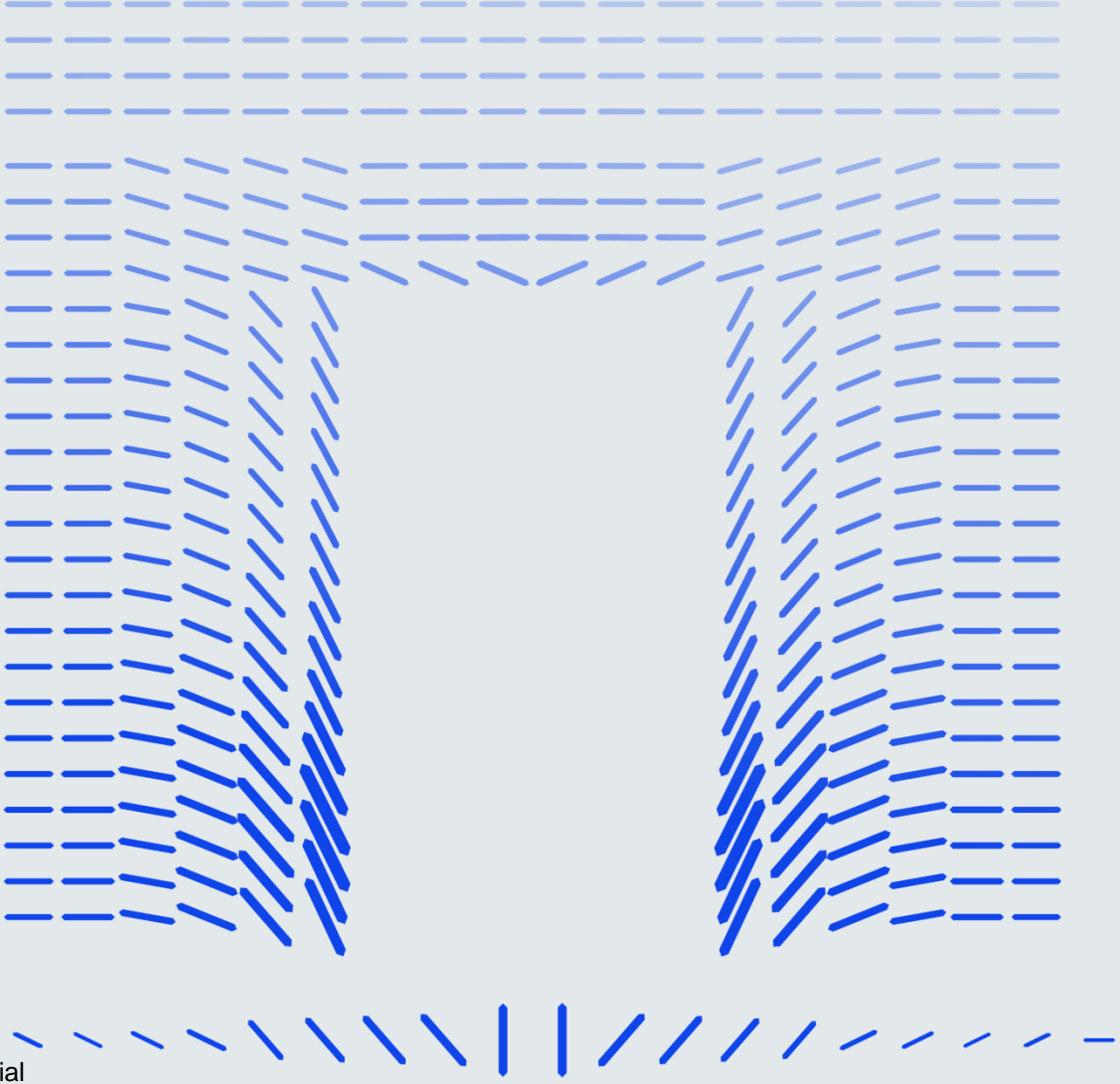
Dubai International
Financial Centre

Office of the Commissioner of Data Protection - UPDATE

Presented by
Lori Baker, DIFCA Director of Data Protection

30 June 2021

Confidential





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



02

THE DPO

General requirements

Reporting and Responsibilities

Articles 16 to 20 – The bulk of the accountability section of DP Law 2020 is about the DPO

DPOs have an independent role in an organization, acting in many ways like a “shadow regulator”

- **Review and monitor processes and policies**
- **Conduct training and share information about compliance requirements in the business**
- **Report to key stakeholders and senior management**
- **Conduct DPIAs and risk assessments**
- **Review contracts for DP obligations and flow downs**
- **Drive the culture of privacy in the business**
- **Act as a contact point for the Commissioner**

Article 16 – To Appoint or Not to Appoint

Designation of the DPO

(1) A Controller or Processor **may** elect to appoint a DPO that meets the requirements of Article 17.

(2) Notwithstanding Article 16(1), a DPO **shall** be appointed by:

- (a) DIFC Bodies, other than the Courts acting in their judicial capacity; and
- (b) a Controller or Processor performing [High Risk Processing Activities](#) on a systematic or regular basis.

(3) A Controller or Processor to which Article 16(2)(b) does not apply **may be required** to designate a DPO by the Commissioner.

Additional obligations:

- If no DPO, shall clearly allocate responsibility for oversight / compliance and provide details of the persons
- DPO role may be performed by a member of staff, an individual employed within the Group or by a third party
- Easily accessible from each entity in the Group.
- Must reside in the UAE unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis.

A [DPO appointment assessment tool](#) is available on the DP [guidance](#) website

Article 17 – It's about Independence

A DPO must:

- ✓ have the ability to fulfil the tasks set out in Article 18;
- ✓ (b) be able to perform his duties and tasks in an **independent manner...**;
- ✓ (c) have **direct access and report to senior management** of the Controller or Processor;
- ✓ (d) have **sufficient resources to perform his duties** in an effective, objective and independent manner;
and
- ✓ (e) have **timely and unrestricted access to information to carry out his duties and responsibilities** under the DP Law.

A DPO shall be transparent and cooperative with the Commissioner and shall notify the Commissioner of all relevant information within the Controller or Processor organisation, other than information that is subject to legal privilege or a conflicting obligation of non-disclosure under Applicable Law.

Subject to certain conditions, a DPO may hold other roles or titles within a Controller or Processor or within each such Group, and may fulfil additional tasks and duties.

Article 18 – It's about Accountability

Worth noting that the **CONTROLLER OR PROCESSOR** must ensure:

- ✓ its DPO is properly involved in a timely manner, on all issues relating to the protection of Personal Data and is given sufficient resources necessary to carry out the role;
- ✓ its DPO is free to act independently; and
- ✓ any additional tasks and duties fulfilled by its DPO, other than those required under the DP Law, do not result in a conflict of interest or otherwise prevent the proper performance of the role of the DPO.

A Data Subject may contact the DPO of a Controller or Processor with regard to all issues related to Processing of his Personal Data and to the exercise of his rights under this Law.

Articles 19 and 20 – What are the risks in your Personal Data processing and how will you handle them?

The DPO Annual Assessment is required **ONLY** of those organizations that have appointed DPO.

Can you do one anyway?

✓ Not officially, not in the DIFC Client Portal BUT... why not do it anyway?

Should you do one anyway?

✓ At the very least do **DPIAs on a regular basis** regarding departmental processing, project specific processing, as part of a policy requirement (retention, incident management, etc) or for general good health checks. There are many obligations to meet, ***with or without a DPO appointed.***

Obligations

Article 15	Requirement	References
	<p>Maintain a written record, which may be in electronic form, of Processing activities under its responsibility, which shall contain at least the following information:</p> <ul style="list-style-type: none"> (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). 	<p>procedures ROPA template (spreadsheet or other database)</p>
<p>Article 16 1</p>	<p>Requirement Appoint a DPO if required</p>	<p>References internal privacy policy online privacy policy / notification procedures</p>
<p>4</p>	<p>If not required, appoint a person responsible for DP compliance / communications with Commissioner's Office</p>	<p>internal privacy policy procedures</p>
<p>Article 20</p>	<p>DPO / entity to regularly conduct Data protection impact assessment, at least annually</p>	<p>internal privacy policy procedures</p>

Obligations (2)

<p>Article 22</p>	<p>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:</p> <p>(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</p> <p>Where a Controller is unable to ensure that Personal Data is securely and permanently deleted, anonymised, pseudonymised or securely encrypted, the Personal Data must be archived in a manner that ensures the data is put beyond further use</p> <p>Note: A22(4)(c) has certain requirements where AI is used</p>	<p>internal privacy policy procedures</p>
<p>Articles 23, 24 and 25</p>	<p>Sign appropriate written data processing agreements between your organization and any 3rd parties</p>	<p>contracts / agreements</p>
<p>Article 26</p>	<p>Ensure any privacy policies include a requirement that processing done in your organization is confidentially and only under specific instructions.</p> <p>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</p>	<p>internal privacy policy procedures</p>
<p>Article 26</p>	<p>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</p>	<p>internal privacy policy online privacy policy / notification to Commissioner record of processing activities contracts / agreements</p>
<p>Article 27</p>	<p>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</p>	<p>internal privacy policy online privacy policy / notification to Commissioner records of processing activities contracts / agreements</p>
<p>Article 29 and 30</p>	<p>Privacy notices (i.e., online privacy policy telling data subjects what you're doing with the PD collected)</p> <p>NOTE: Regarding emerging technology such as blockchain, Article 29(1)(h)(ix) has special requirements</p>	<p>internal privacy policy (article 31(3)) online privacy policy / notification procedures</p>
<p>Articles 32 to 40</p>	<p>Written policies that provides for data subjects rights contained in relevant articles</p>	<p>internal privacy policy online privacy policy / notification procedures</p>
<p>Articles 41 and 42</p>	<p>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 :</p> <p>-- notification of DP Commissioner -- where required, notification of data subject</p>	<p>internal privacy policy procedures</p>



03

Annual Assessment

Format

When, How, What?

Enforcement

DIFC Client Portal Service Request

Key points:

- ✓ Looks a lot like a DPIA, but much broader and more detailed
- ✓ Required in conjunction with Notification and / or License renewal
- ✓ First assessments are due at the first renewal date after July 1, 2021
- ✓ Commissioner will assess a sampling of these submissions and follow up with supervisory questions and comments as needed
- ✓ If you wish to ask us to assess your assessment, please let us know by email to commissioner@dp.difc.ae
- ✓ Different from a Notification because only DPO-appointed entities must complete this whereas ALL processing entities must notify
- ✓ Go to the DIFC Client Portal and search for the DPO Annual Assessment SR – it will only be available to DPO-appointed entities and only for 30 days before and after license renewal
- ✓ [Annual Assessment](#) guidance is available on the DIFC DP [guidance](#) website difc.ae

The Fines Print

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

Currently there are no fines for failure to complete the DPO Annual Assessment.

However... Failure to appoint a DPO or update your notification in a timely manner in accordance with the DP Law 2020 are contraventions of the DP Law and may be subject to an administrative fine in addition to any general fines

The Commissioner's Office understands that Covid-19 has had a considerable impact on DIFC businesses, and will be reasonable with respect to enforcement on a case by case basis for the time being.



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

Comprehensive Guides On Matters Related To Data Protection

Covid 19 FAQs	DOWNLOAD >
Complete Guide to Data Protection Notifications	DOWNLOAD >
Data Export Guidance	DOWNLOAD >
Data Subject Consent Guidance	DOWNLOAD >
Direct Marketing & Electronic Communications	DOWNLOAD >
DP Law 2020 Intro Sessions: Accountability, Supervision and Enforcement	DOWNLOAD >
DP Update for DIFC Law 2020 Introduction Session	DOWNLOAD >
DP Law 2020 Intro Sessions: Data Export and Sharing	DOWNLOAD >
Fines and Sanctions Guidance	DOWNLOAD >
Guide to Data Protection Law, DIFC Law No. 5 of 2020 and Data Protection Regulations	DOWNLOAD >
High Risk Processing Guidance	DOWNLOAD >
Individuals’ Rights to Access and Control DIFC Personal Data Processing	DOWNLOAD >
OECD: Privacy Online: Policy and Practical Guidance 21 January 2003	DOWNLOAD >
OECD: Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 21 December 2005	DOWNLOAD >
Security Breach Guidance	DOWNLOAD >

Data Protection Assessment Tools

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 DIFC entity. The information, which may be amended from time to time, does not constitute legal or any other type of advice and it is provided for information purposes only.

DP Assessment Tool – Applicability

CONDUCT ASSESSMENT

DP Assessment Tool – Data Protection Officers

CONDUCT ASSESSMENT

DP Assessment Tool - Data Export and Sharing

CONDUCT ASSESSMENT

DP Assessment Tool – High Risk Processing Activities

CONDUCT ASSESSMENT

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