



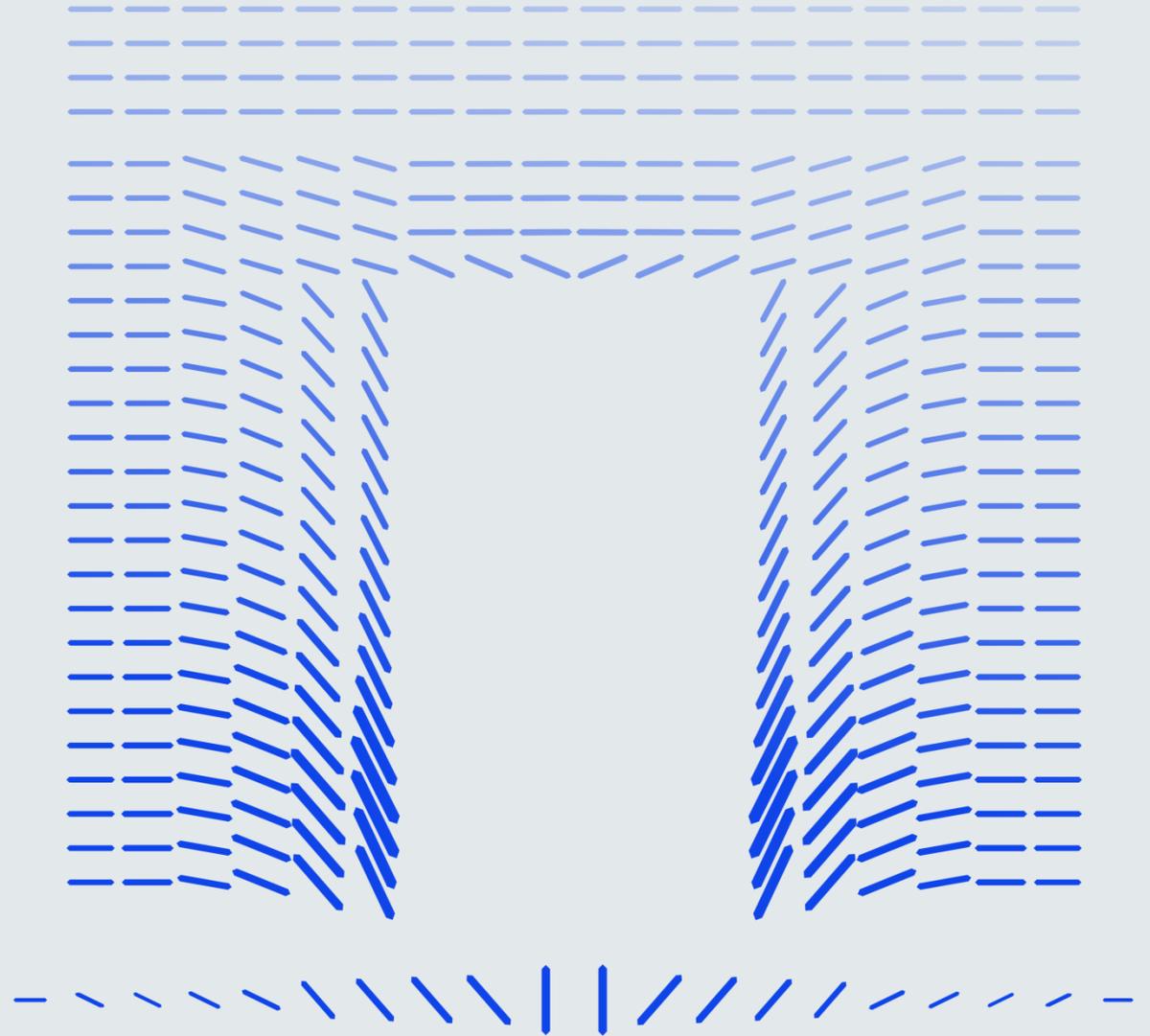
Dubai International
Financial Centre

Office of the Commissioner of Data Protection - UPDATE

Presented by
Lori Baker, Director of Data Protection

1 September, 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



02

Notifications & Applicability

Articles 6 and 14 in Focus

Obligations

Guidance & Resources

Articles 6 & 14

DP Law 2020 Part 2 - General Requirements		
Article 6	Requirement	References
(3)(a)	Applies to all DIFC entities (not only financial services)	
(3)(b)	Applies to entities not incorporated in DIFC but that have stable arrangements <i>in the context of its Processing activity in the DIFC (and not in a Third Country), including transfers of Personal Data out of the DIFC.</i>	contracts, business relationships, other arrangements
Article 14	Requirement	References
7 / 8	Notification to Commissioner of Data Protection renewed on annual basis	procedures

Two pronged “test”:

Stable arrangements

Considered by the Court of Justice of the [European Union \(CJEU\) in the Weltimmo case](#), the CJEU ruled that "any real and effective activity – even a minimal one" – through "stable arrangements" in the EEA may be sufficient to qualify as to serve as an establishment (of a relationship, gateway or platform for Processing into the jurisdiction) under (European) data protection law. The threshold for “stable arrangements” can be quite low, and that in some cases a single employee or agent with a sufficient degree of stability of operations would satisfy the test. This is what was in mind when drafting this clause.

Context of Processing Activity

Determine whether the processing activities "*are carried out in the context of the activities of an [entity]*". Hand in hand with stable arrangements is the concept of the "*inextricable link*", again first set out in European DP Law. While to be fair and transparent, this concept in DIFC remains to be tested in the courts as the DP Law 2020 is new, as is the concept. However, “context” of activities can include revenue-raising activities within the DIFC that relate to the processing of Personal Data taking place outside the DIFC, which may indicate that the processing is carried out "*in the context of the activities of*" the DIFC relationship or platform.

Whether such arrangements and context exists is an assessment which organisations need to carry out on a case by case basis. The key is to implement appropriate controls on whatever scale they deem necessary (if any), which is best practice for any business anyway.

DIFC DP Website

The Commissioner’s Office has [posted guidance](#) and assessment tools on several key topic areas of the DIFC DP Law 2020

[“Example Compliance Checklist & DPIA”](#)

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 >

Please review the [guidance](#) page of the Commissioner’s DP website on DIFC.ae

The [Guide to Data Protection Law No 5 of 2020](#) provides extensive information about compliance with the law in general and applicability examples.

The Commissioner’s Office has posted a set of assessment tools as well, one of which is the [Applicability Assessment](#) tool.

Other resources

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



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

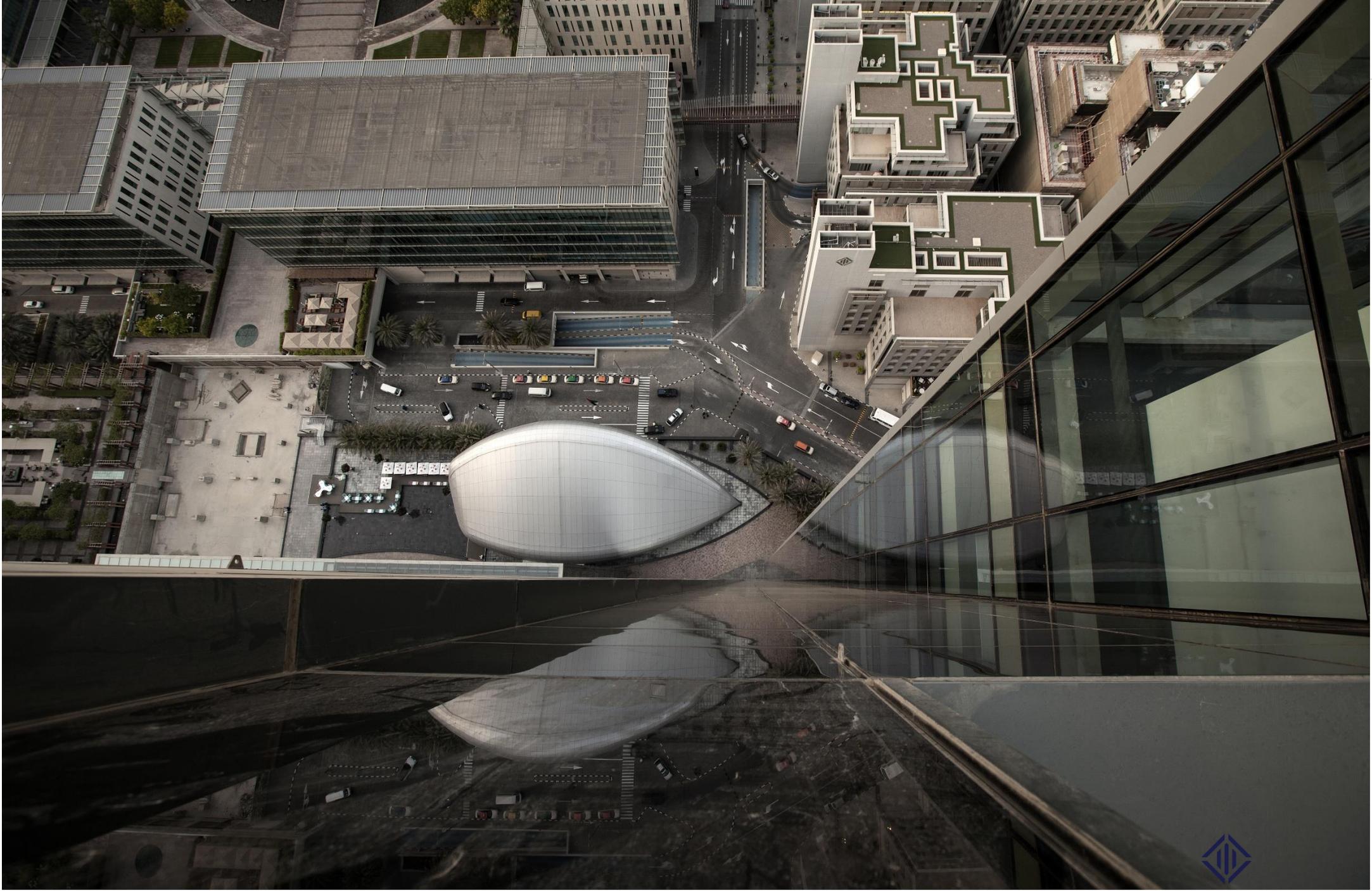
MOST IMPORTANT: BUILD A CULTURE OF PRIVACY IN THE BUSINESS

Relevant Articles

Article 15	Requirement	References
	<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>
Article 16	Requirement	References
1	Appoint a DPO if required (and then see Articles 17 to 19 inclusive)	<p>internal privacy policy online privacy policy / notification procedures</p>
4	If not required, appoint a person responsible for DP compliance / communications with Commissioner's Office	<p>internal privacy policy procedures</p>
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)	<p>internal privacy policy procedures</p>

Obligations (2)

Article 22	<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 (in accordance with Article 22(3) and accounting for Article 22(4))</p>	internal privacy policy procedures
Articles 23, 24 and 25	Sign appropriate written data processing agreements between your organization and any 3rd parties	contracts / agreements
Article 26	<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>internal privacy policy online privacy policy / notification notification to Commissioner record of processing activities contracts / agreements</p>
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	<p>internal privacy policy online privacy policy / notification notification to Commissioner records of processing activities contracts / agreements</p>
Article 29 and 30	Privacy notices (i.e., online privacy policy telling data subjects what you're doing with the PD collected)	<p>internal privacy policy (article 31(3)) online privacy policy / notification procedures</p>
Articles 32 to 40	Written policies that provides for data subjects rights contained in relevant articles	<p>internal privacy policy online privacy policy / notification procedures</p>
Articles 41 and 42	<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>	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