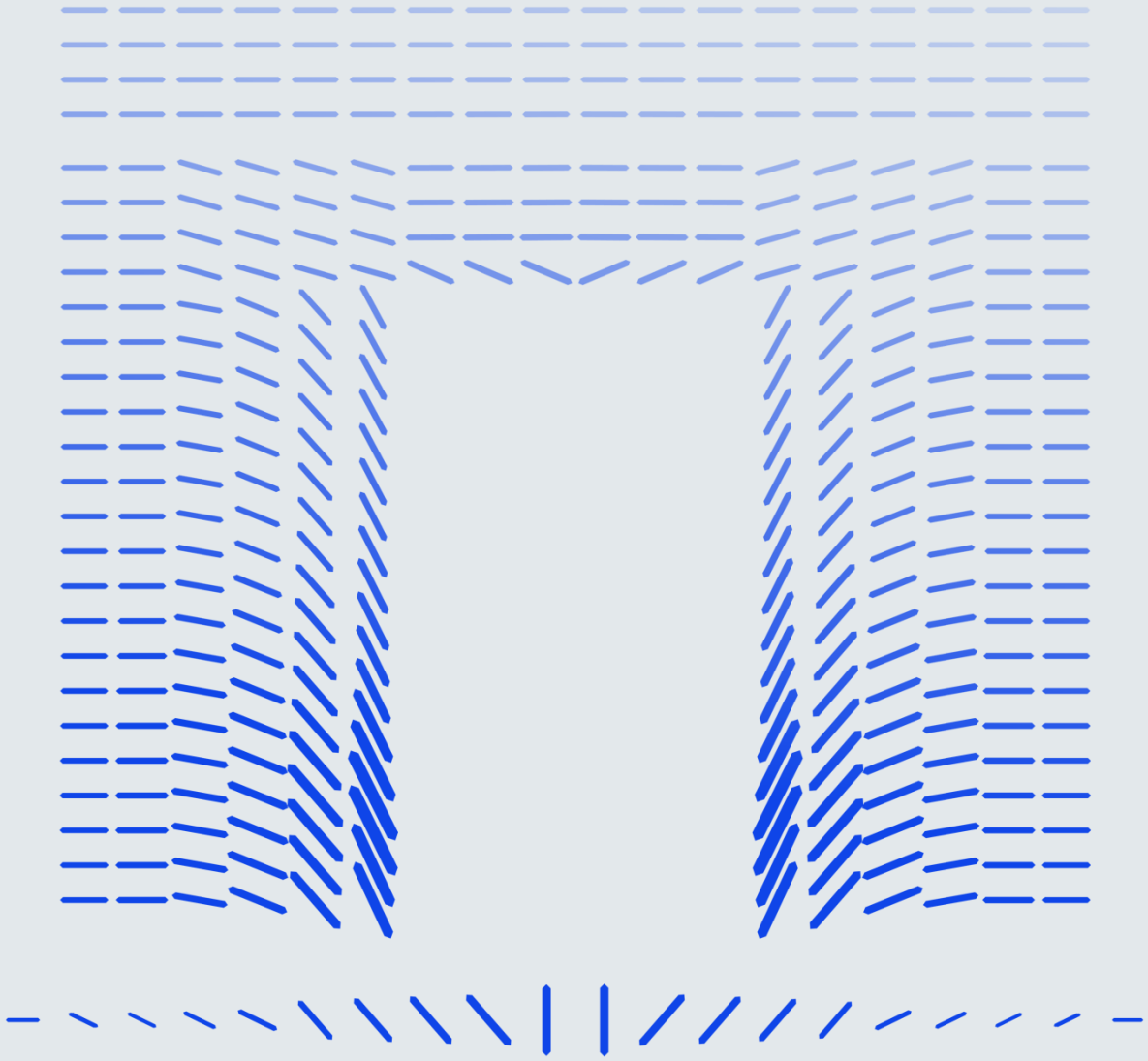
Dubai International Financial Centre

Office of the Commissioner of Data Protection - UPDATE

Presented by
Lori Baker, Director of Data Protection



20 August, 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	Notifications	Still required, however process for filing will be akin to setting up a compliance program tracked against the DP Law

02

Accountability & Notifications

Article 14 in Focus

Obligations

Guidance

Article 14

Part 2D - Accountability / General Requirements			
Article 14	**Requirement**	**Yes / No?**	**References**
1	Compliance program: based on data being processed, scale of processing, type		internal privacy policy online privacy policy / notification procedures
2	Technical and organizational measures: security, IT, training, comms, reporting, risk assessment		internal privacy policy online privacy policy / notification security policy training and communications (internal) procedures
3	Privacy by design / default: privacy is built in from the outset to all new processes and procedures		internal privacy policy procedures
4	Default online preferences: Where a Controller is offering online services through a platform, the default privacy preferences of the platform shall be set such that no more than the minimum Personal Data necessary to deliver or receive the relevant services is obtained or collected. Data Subject should be prompted to actively select his privacy preferences on first use and able to easily change such preferences.		procedures
5	Written data protection policy		internal privacy policy online privacy policy / notification
6	Codes of Conduct / Certification schemes (TBD - N/A for now)	N/A	N/A (for now)
7 / 8	Notification to Commissioner of Data Protection renewed on annual basis	Yes	procedures

Guide to DP Law 2020 and other resources

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 accountability enhancements.

The ICO in the UK provides excellent guidance as well, which the DIFC tracks to a large degree.

> *"**Why is accountability important?***
> *Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.*
>
> *Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage."*
>
> *~ UK Information Commissioner's Office*

03

Controller / Processor Obligations

Relevant articles

Obligations

Guidance

Controller / Processor – what is the difference?

Key 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

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	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

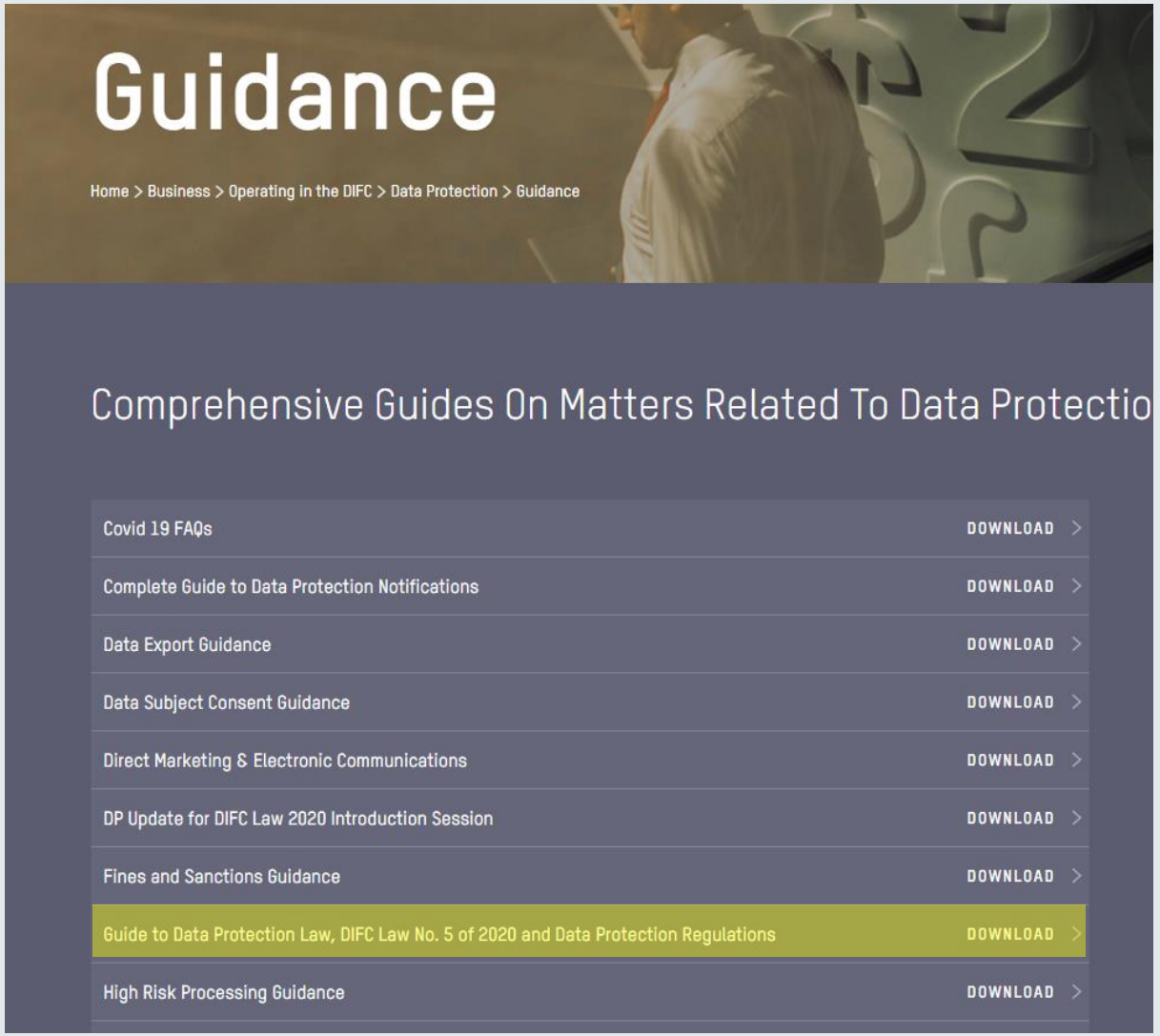
Obligations (2)

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 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 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

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



04

The Commissioner

What does the Office of the Commissioner do?

Supervision

Enforcement

Objectives, Powers and Functions

The objectives of the Commissioner of Data Protection in the DIFC are set out in Article 46(2):

46. Powers, functions and objectives of the Commissioner

(1) The Commissioner has such powers, duties and functions as conferred on him under this Law and any Regulation made under this Law and shall exercise such powers and perform such functions in pursuit of the objectives of this Law and the Regulations.

(2) In performing his functions and exercising his powers, the Commissioner shall pursue the following objectives:

(a) to monitor, ensure and enforce compliance with this Law;

(b) to promote good practices and observance of the requirements of this Law and the Regulations by a Controller or Processor; and

(c) to promote greater awareness and public understanding of data protection and the requirements of this Law and the Regulations in the DIFC.

The powers and functions of the Commissioner of Data Protection in the DIFC are set out in Article 46(3). They include taking complaints, investigating them where warranted, providing Regulations, supervision, enforcement and *above all* that each such power and function is carried out in an *independent manner.*

Supervision and Enforcement

One of the powers / functions of the Commissioner is to carry out inspections, aka **Supervision**.

•Meet with at least 2 DIFC entities per month, from all types and activities including DFSA regulated entities

•Review DP obligations and support by answering any questions

•Crucially, as the DIFC entity is often part of a broader organization or group of companies, it helps reinforce compliance with other similar laws such as the GDPR or the UK DPA 2018.

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

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.

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