Office of the Commissioner of Data Protection

DIFC

Notifications Guidance: Process, Requirements and Step by Step Explanations

Date: November 2022

The future is here.

01

DIFC

DP Law 2020

DP Law 2020 – Enacted May 2020, Effective July 2020, Enforceable from October 1, 2020

02

Ethical Data Management

In focus – Articles 6 and 14 requirements and obligations

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 ***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.***	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*". "Context" 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.

Obligations

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 assessment, at least annually	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 NOTE: A22(4)(c) has certain requirements where AI is used	internal privacy policy procedures
Articles 23, 24, 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 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) NOTE: Regarding emerging technology such as blockchain, Article 29(1)(h)(ix) has special requirements	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

Accountability

What does Accountability mean?

Please review the guidance page of the Commissioner's DP website on DIFC.ae for useful resources about the Law and Accountability.

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

Notifications Process

Why are Notifications required and where does it say so in the DP Law and Regulations?

What is a notification?

A notification is a way of telling the Commissioner and the general public what the entity's processing activities are and how they comply with the DP Law.

NOTIFICATIONS MUST BE UP TO DATE

Why is it necessary to notify when an entity processes Personal Data?

- *It is required for accountability of the entity, to be transparent, and to ensure the entity itself is aware of and tracks its own compliance obligations.*
- *More importantly, it helps the entity build a culture of compliance, privacy and security within the organization.*
- *This isn't just to avoid fines, but to really understand and respect that the Personal Data it processes belongs to individual persons, who are entitled to that right to privacy and to determine how their information and profile is managed.*

What parts of the DP Law and Regulations tell us about notification requirements?

Article 14(7) and (8) of the DP Law state that notifications are required and must be up to date. Section 3 of the DP Regulations states the timing requirements and what must be provided.

Steps for Completing the DP Notification

How do I complete a notification in the DIFC Client Portal?

Log into the portal, and if you are **onboarding** as a **new entity**, please complete the DP section as directed.

For an **existing company** updating its notification, please select the DP Notification service request. Notifications guidance is available as well.

Some things to consider before notifying:

- ✓ **Do I engage in High Risk Processing and if so, who will be my DPO?** Helpful tools are available on the guidance site for both HRP and DPO appointments.
- ✓ **Where does the data I collect go?** Think about suppliers or other third parties that might access it (Art. 15), or other parts of your company in another country that you may email or send it to for storage (Art. 27). Please see the Data Export tool for support.
- ✓ **What would any people whose data I process reasonably expect me to do with their data or why I need it?** It's only fair to be clear about how and why you collect / process data, but you can't email everyone that might think about sharing their data with your business. So you need a privacy notice / policy (Art. 29/30), privacy clauses in your contracts (Art. 23/24/25/28) (including employment contracts) and a policy to support individuals exercising their rights to request access to / updating of their Personal Data (Art. 14, 32 to 40). Tools are available to help you understand the requirements for responding to access requests.

Process flow – Overview

The Notification process during ***Onboarding*** happens in ***TWO*** stages

Stage 1: Select the **purpose of the notification**, i.e., to tell the Commissioner that your entity **does / will** or **does not / will not** process Personal Data. To help you understand the concept of processing and the notification requirement, please run this useful, simple notification assessment tool.

At this time, your entity probably doesn't do any processing, but think about whether it will do so in the future, i.e.:

- taking orders from customers for delivery or taking payments
- having employees whose information you must process for visas, payroll and health insurance
- using names and email addresses for marketing purposes or promotions
- using data from website visits (through cookies and IP addresses) to gather analytics and build customer profiles
- supplier information for running your business

If you indicate that you **do not Process** Personal Data, further questions will appear regarding whether you have employees, suppliers or customers, and additional information may be required to justify your selection.

Our team will review your submission and if rejected, you will have to re-complete your initial notification.

Stage 2: From the time your initial onboarding review is accepted, you will have 6 months to complete the rest of the notification. You will be asked to provide additional details about your company's Processing activities.

Guidance and FAQs about notifications is available on the DIFC DP website. This notification assessment tool may help you make this decision as well.

If you still have questions about Data Protection obligations and compliance in DIFC, please contact commissioner@dp.difc.ae . IF you have questions about the DIFC Client Portal and any technical issues with completing your notification, please contact the Registry Services Help Desk.

All information collected in this form is processed in accordance with the DIFC Online Data Protection Policy.

The process for updating an existing notification essentially follows the same process flow regarding any notification that an entity does not Process PD.

Process flow of Stage 1

PURPOSE OF NOTIFICATION

Corresponds to Article 14(7) and (8) of the DP Law and Section 3.1.1 of the DP Regulations

For the purposes of Articles 14(7) and 14(8) of the Law, a Controller or Processor must notify the Commissioner of the following Personal Data Processing operations.

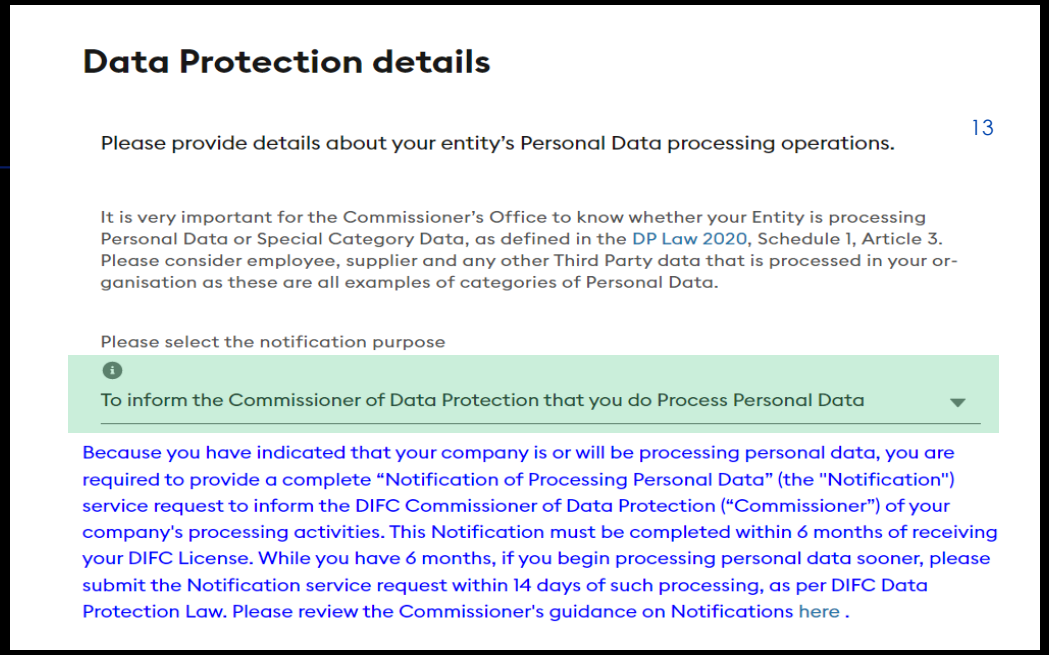
PLEASE NOTE:

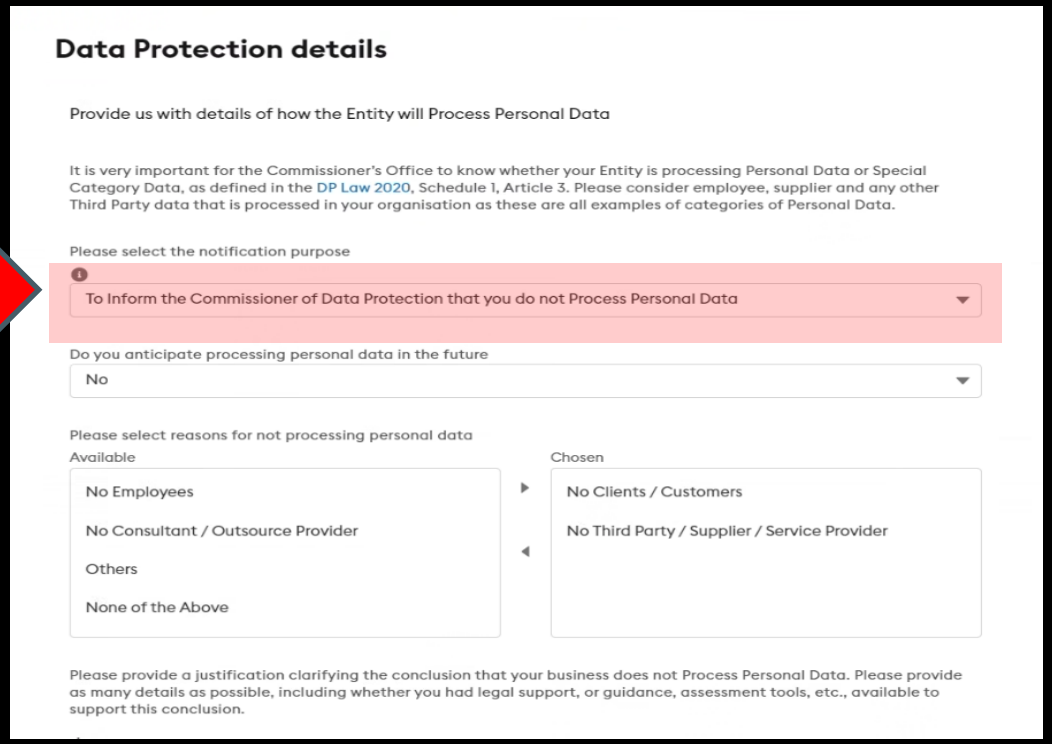
If your entity submits that it *does not process* Personal Data, a reason must be given. An action is created in the Client Portal for the Commissioner's Office to review this type of response.

"DO NOT PROCESS"

Please note that DO NOT PROCESS responses may possibly be rejected on initial assessment by Commissioner's Office, and you may be contacted to discuss your reasons for your selection. If it is rejected, you must indicate that your entity DOES process Personal Data and pay any associated fees for notification.

Only prescribed companies and pure holding companies are currently excluded from this step of the process.





Process flow of Stage 2 / Updating Notification

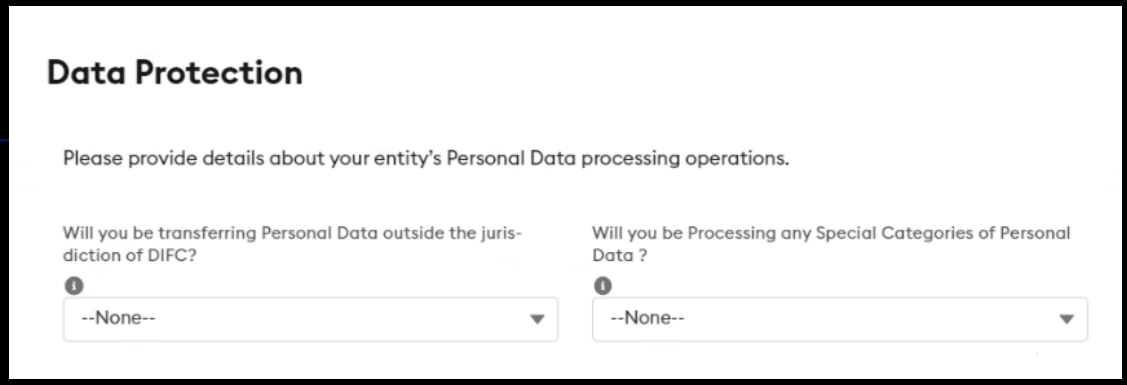
PURPOSE OF NOTIFICATION

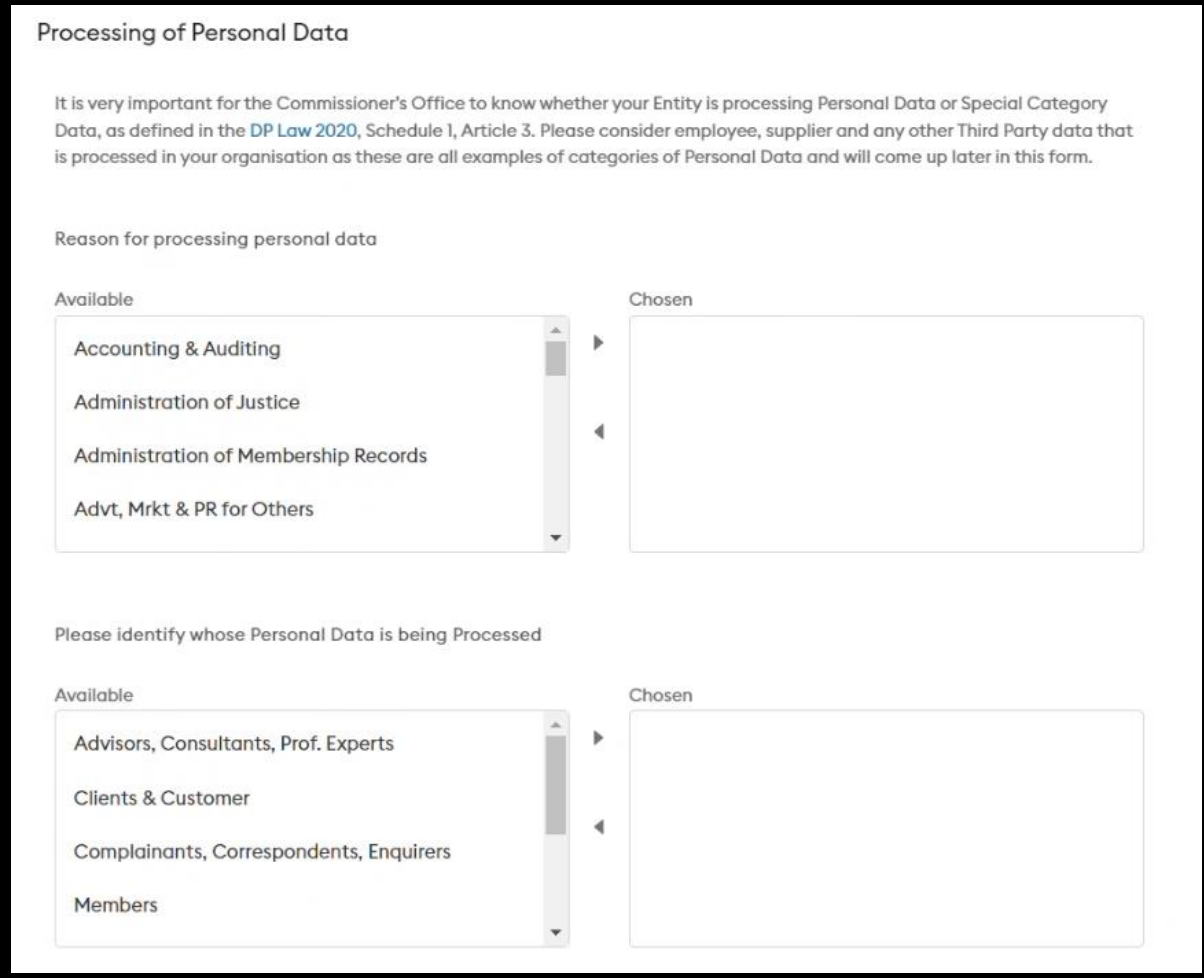
Corresponds to Article 14(7) and (8) of the DP Law and Section 3.1.1 of the DP Regulations

For the purposes of Articles 14(7) and 14(8) of the Law, a Controller or Processor must notify the Commissioner of the following Personal Data Processing operations regarding:

(a) Personal Data Processing;
(b) Transfer of Personal Data to a recipient outside of the DIFC which is not subject to laws and Regulations that ensure an adequate level of protection; and
(c) Special Category Data.

You must also provide detailed information about the reasons for and categories of Personal Data processing





Process flow of Stage 2 / Updating Notification (/2)

From here, the process flow for Stage 2 / Notification Updates follows the flow and sections of DP Law 2020, as set out above

PROCESSING OF PERSONAL DATA

Corresponds to Articles 10, 11 and 13 of the DP Law 2020 and Section 3.1.2 of the DP Regulations

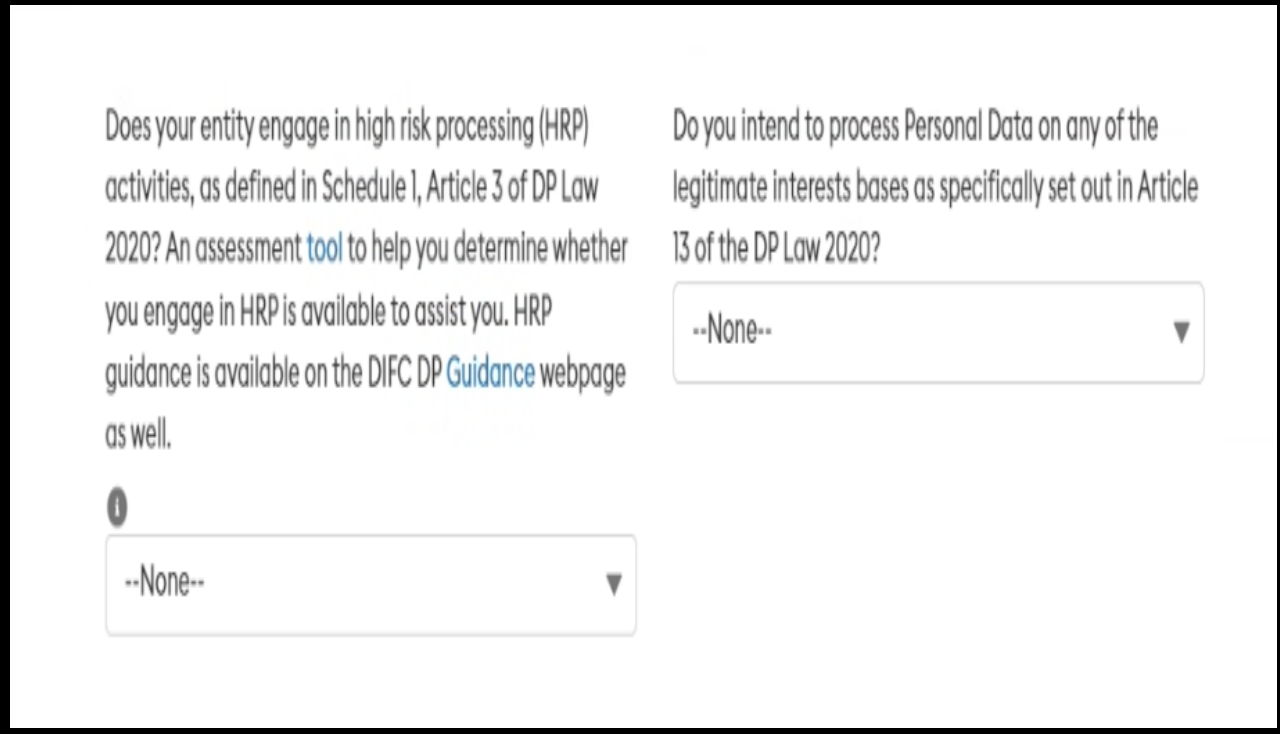
Let's focus on the questions about HRP and Legitimate Interests

Schedule 1, Article 3 definition of High Risk Processing and Article 16 on DPO appointments

If an entity is engaged in HRP, it must appoint a DPO (in the next section), no questions asked. The categories that display after this question are the same as those set out in the DP Law in the definition of HRP at Schedule 1, Article 3. There is HRP guidance and an easy to use HRP assessment tool, as well, available on the Guidance page of the DIFC DP website.

Article 13 – Legitimate Interests as a basis for processing

A public authority may not use this as a basis for processing. Otherwise, entities may use this basis for internal admin procedures or only if it is necessary and proportionate to prevent fraud or ensure network and information security.



Process flow of Stage 2 / Updating Notification (/3)

ACCOUNTABILITY AND OBLIGATIONS

Corresponds to Articles 14(1) to (5), 15, 16 to 18 and 23 to 25 of the DP Law and Section 4 of the DP Regulations. Accountability guidance is available on the Guidance page of the DIFC DP website.

Article 14(1) requires that a Controller or Processor has a compliance program in place. Articles 14(2) to (5) discuss elements of that program, but we do not ask them to confirm these elements in the notification.

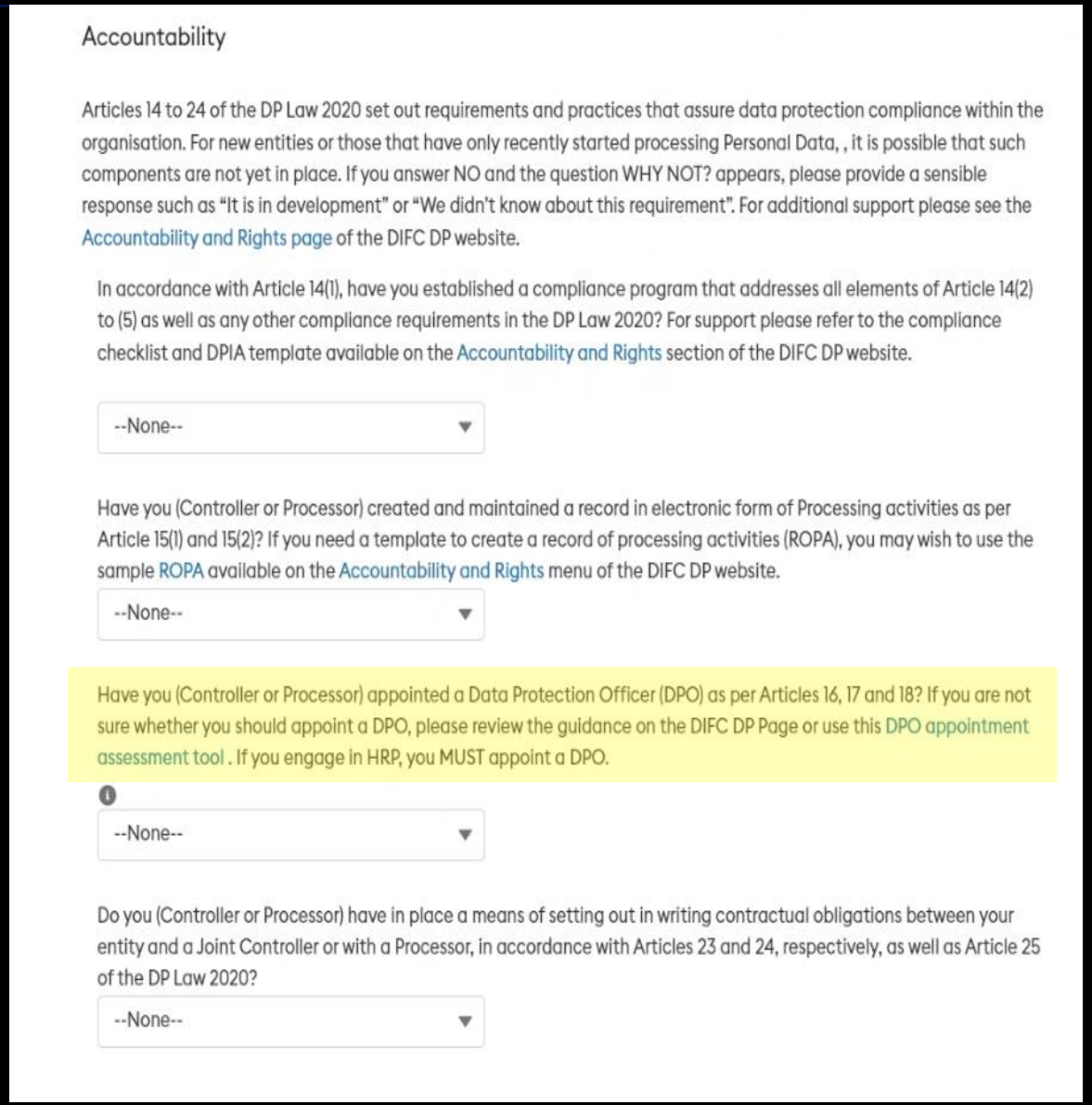
Article 15 requires the Controller or Processor to keep a record of processing activities (ROPA), and includes the items in Article 15(1)(a to h). A good example is to start with the entity's accounts payable report, and narrow it down by retaining only the suppliers / third parties they provide Personal Data to for processing (i.e., payroll, health insurance, IT companies, etc)

Article 16 to 18 discusses the Data Protection Officer (DPO) appointment and DPO responsibilities. Two types of entities MUST appoint a DPO

- **(a) a Centre Body (DIFCA, DFSA, etc.)**
- **(b) An entity engaged in HRP – run through the HRP assessment tool to help determine whether you engage in HRP. If YES, you MUST appoint a DPO**

Whether appointing a DPO or not, **DP contact details must be provided**.

Articles 23 to 25 cover requirements for contracts between 2 controllers, controllers and processors, and between processors and sub-processors. Processors in particular must have contracts in place with the appropriate items set out in Article 24(5)(a) and (b).



Accountability

Articles 14 to 24 of the DP Law 2020 set out requirements and practices that assure data protection compliance within the organisation. For new entities or those that have only recently started processing Personal Data, , it is possible that such components are not yet in place. If you answer NO and the question WHY NOT? appears, please provide a sensible response such as "It is in development" or "We didn't know about this requirement". For additional support please see the Accountability and Rights page of the DIFC DP website.

In accordance with Article 14(1), have you established a compliance program that addresses all elements of Article 14(2) to (5) as well as any other compliance requirements in the DP Law 2020? For support please refer to the compliance checklist and DPIA template available on the Accountability and Rights section of the DIFC DP website.

--None--

Have you (Controller or Processor) created and maintained a record in electronic form of Processing activities as per Article 15(1) and 15(2)? If you need a template to create a record of processing activities (ROPA), you may wish to use the sample ROPA available on the Accountability and Rights menu of the DIFC DP website.

--None--

Have you (Controller or Processor) appointed a Data Protection Officer (DPO) as per Articles 16, 17 and 18? If you are not sure whether you should appoint a DPO, please review the guidance on the DIFC DP Page or use this DPO appointment assessment tool . If you engage in HRP, you MUST appoint a DPO.

--None--

Do you (Controller or Processor) have in place a means of setting out in writing contractual obligations between your entity and a Joint Controller or with a Processor, in accordance with Articles 23 and 24, respectively, as well as Article 25 of the DP Law 2020?

--None--

Process flow of Stage 2 / Updating Notification (/4)

TRANSFERS OF PERSONAL DATA

Corresponds to Articles 26 and 27 of the DP Law and Section 5 of the DP Regulations.

Why are transfers to other jurisdictions such a hot topic?

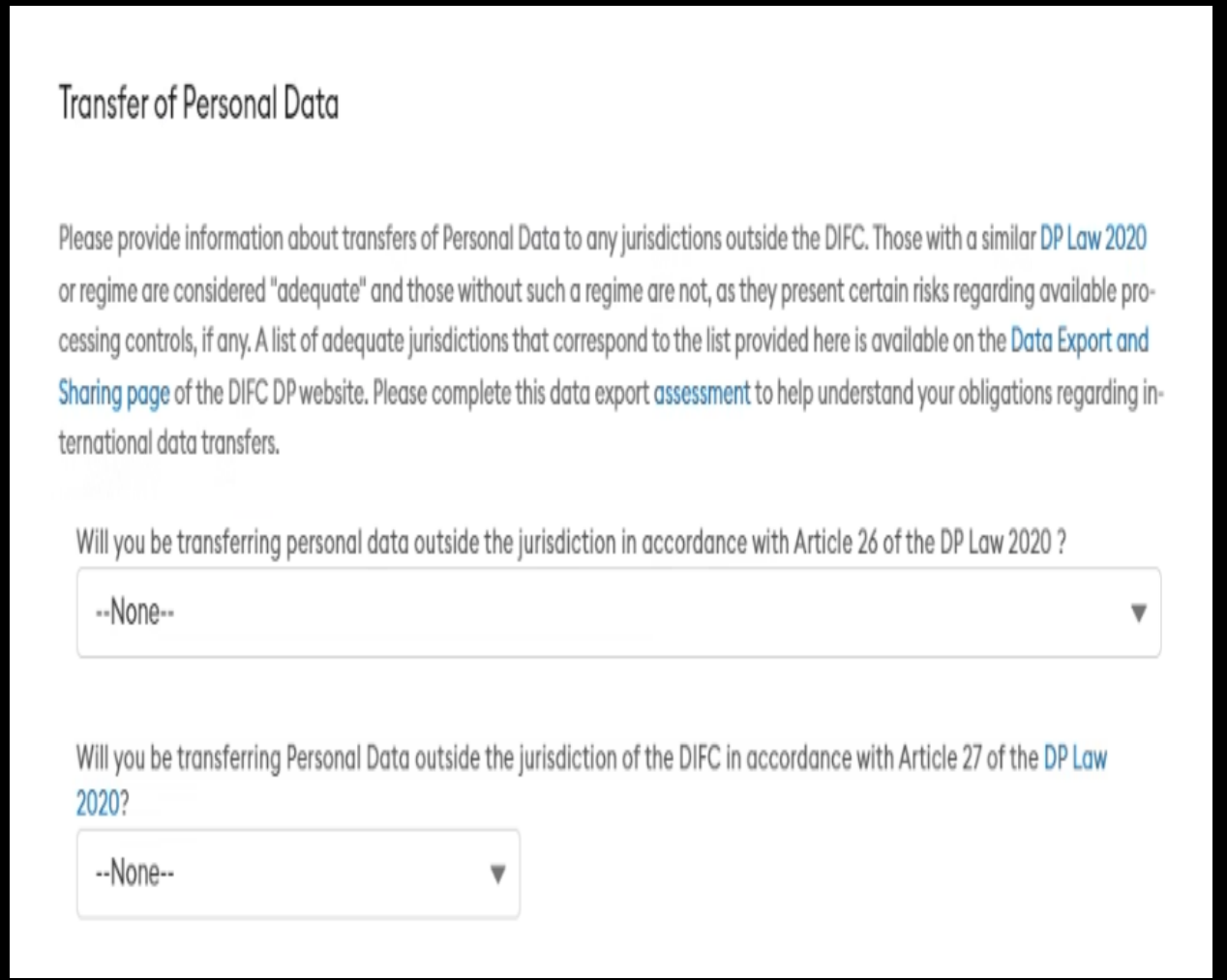
Where there is no data protection law, or even where this is one and it does not meet the standards of the place the data is collected or leaves from, there is no assurance at least in law that the data will be managed in the same way as it is at home. **Articles 26 and 27 of the DIFC DP Law 2020 cover these issues**.

If a country does not appear in one of the lists, it is 99.999% sure to be in the other list and the reason for that is because some are adequate and some are not. **Please double check both lists if it appears that a country is not there**, because it will certainly be in one of the lists.

Data Export guidance and a helpful assessment tool are available to help understand the requirements. Also, the standard data protection clauses for Article 27 compliance are available on the Data Export and Sharing page. This guidance and the list of adequate countries will help complete the questions.

For information about how Schrems I and II impact transfers from the DIFC, please check the relevant notes (which are updated from time to time) on the Data Export and Sharing page.

NOTE: Privacy Shield is now invalid, as is Safe Harbor. These will not be available as options in either transfers list.



Process flow of Stage 2 / Updating Notification (/5)

DATA SUBJECTS' RIGHTS

Corresponds to Articles 22 and 29 to 40 of the DP Law, and Section 6 of the DP Regulations.

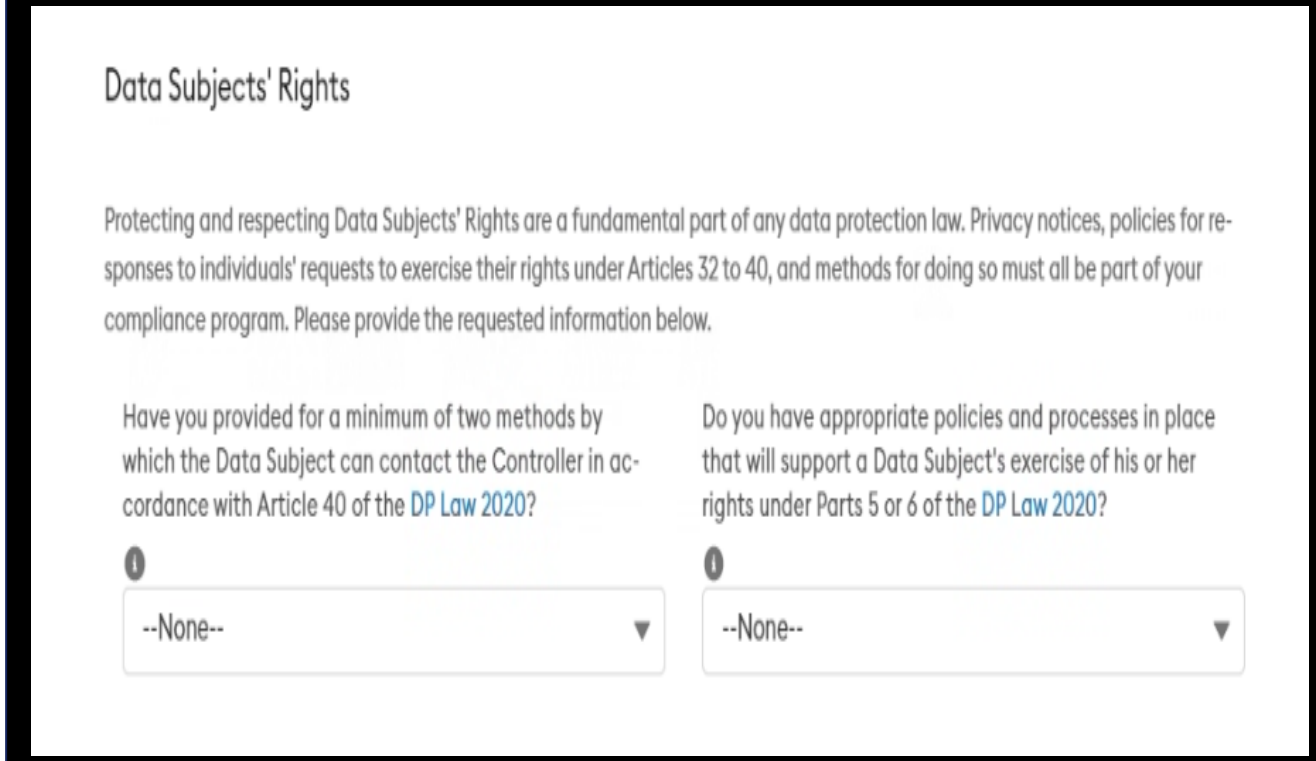
Data subjects' Rights (DSR) section is, after Accountability, possibly the most important part of the DIFC DP Law. In the end, Personal Data belongs to the people that make your business successful. These people are called Data Subjects, as defined in Schedule 1, Article 3.

Controllers must provide 2 ways of getting in touch in accordance with Article 40 of the DP Law, so anyone can ask questions about what is being done with their Personal Data, how to rectify it, remove it, object to processing it and withdraw their consent for its use.

Entities must also have policies in place regarding these issues. Please note, DIFC staff cannot review the policies or to confirm they are implemented correctly. It is therefore not appropriate for the Commissioner's Office or Registry Services to address such questions, apart from recommendations made as a result of formal inspections.

We can however take complaints where a data subject thinks that a Controller or Processor has contravened the DP Law and Regulations, and we can guide Controllers about what they should do to fulfill a DSR requests.

DSR guidance is available on the Guidance page of the DIFC DP website.



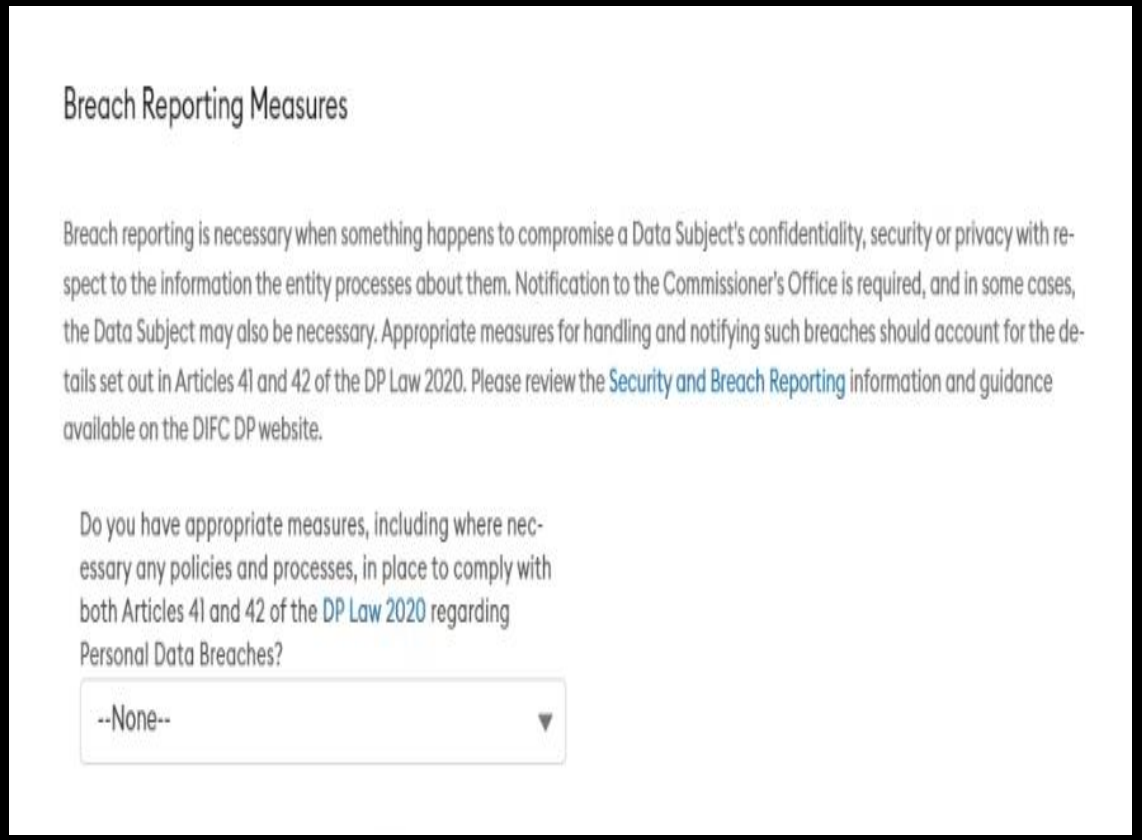
Process flow of Stage 2 / Updating Notification (/6)

BREACH REPORTING MEASURES

Corresponds to Articles 41 and 42 of the DP Law. Personal Data Breach Reporting guidance is available on the Guidance page of the DIFC DP website.

Article 41 requires that a Personal Data Breach is reported to the Commissioner of Data Protection. The law requires that DIFC entities have a policy in place and processes to ensure that these are reported and done so in a timely manner.

Article 42 requires that a Personal Data Breach is also reported to the Data Subject in certain circumstances only. The same requirements apply regarding policies and procedures.



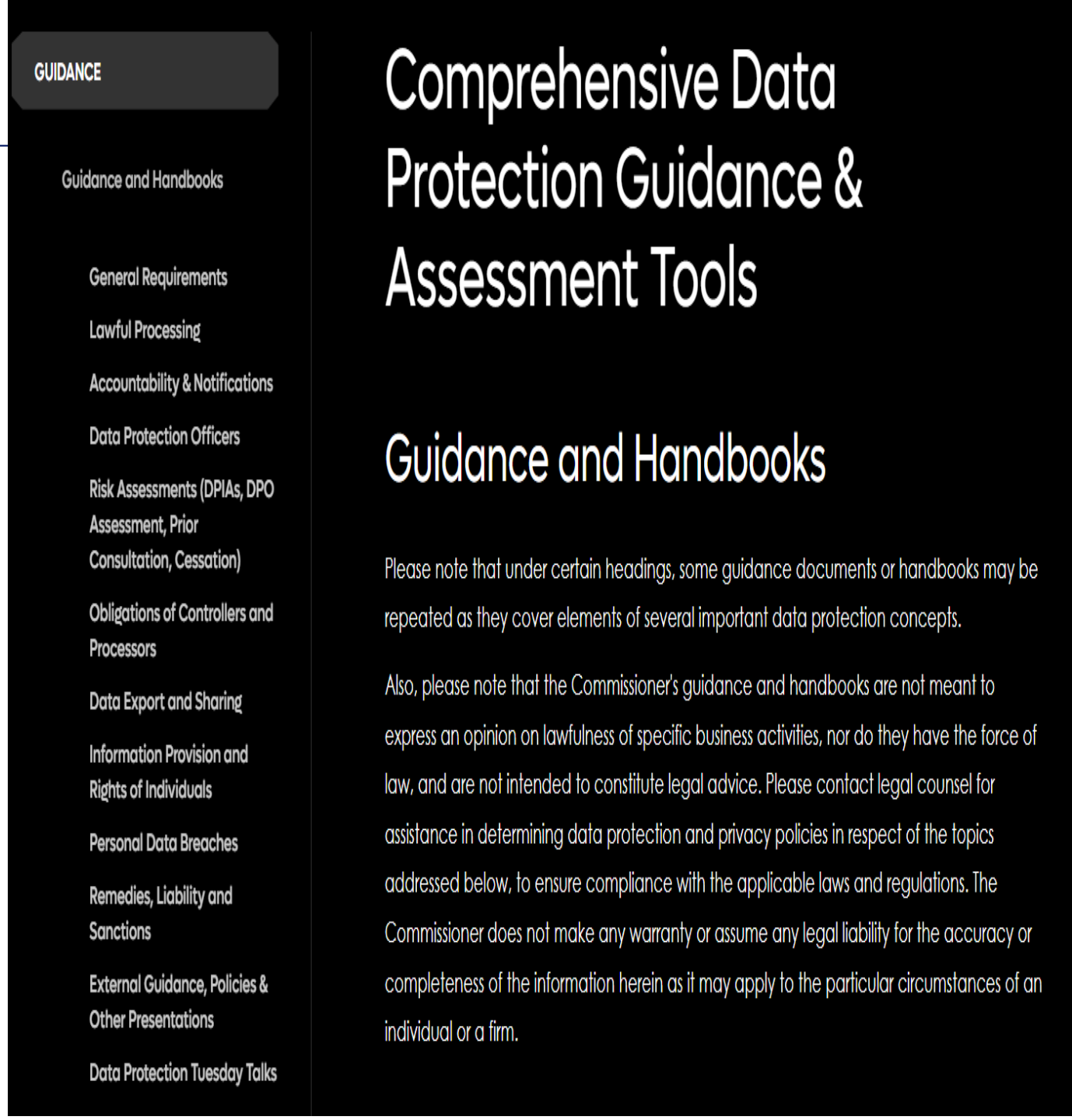
04

Helpful Information

Guidance and Information

DIFC DP Website

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



Guidance and Information

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 assessment tools including the Applicability Assessment tool, the DPO Assessment tool , the Export Assessment tool and the HRP Assessment tool.

Finally, a **free** DIFC DP Law Maturity Assessment tool is available to review your compliance readiness and risk regarding the DP Law 2020. It is provided by a third party, however, so please do review their terms and privacy policy.

What are some other issues to be mindful of?

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, but in certain cases, notification is at least required.

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.

General Resources

DIFC DP Website

DIFC DP Law 2020

DIFC DP Regulations

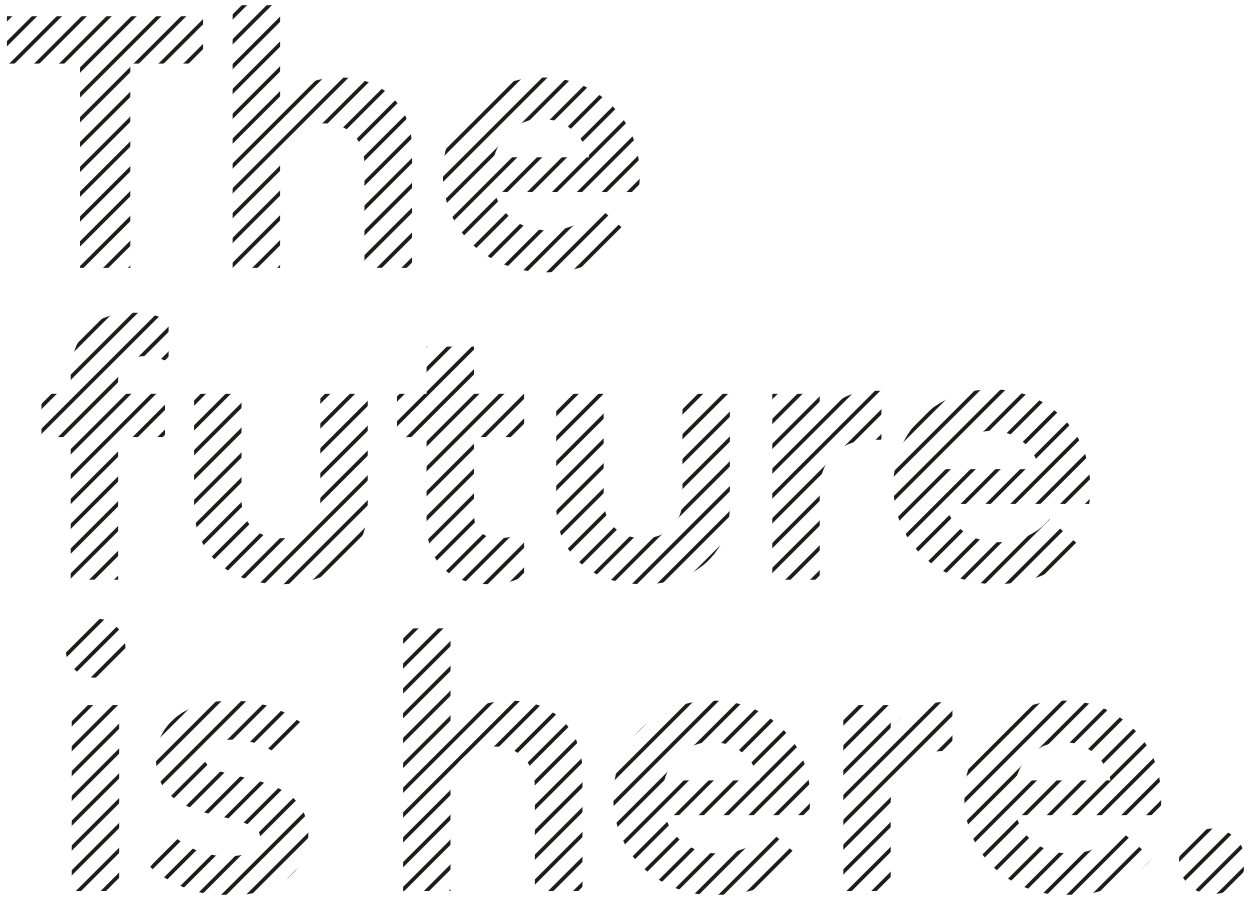
DIFC DP Guidance

DIFC DP FAQs

Clyde & Co article comparing GDPR with DIFC Law

PWC DP Maturity Tool

Compliance checklist and DPIA template



Contact

For further information
please contact:

DIFC DP Commissioner's Office
commissioner@dp.difc.ae

+971 4 362 2222

Gate Building
Level 14
DIFC, Dubai, UAE
PO Box 74777