DIFC

DPO CONTROLLER ANNUAL ASSESSMENT CHECKLIST & FAQS

Commissioner of Data Protection

DIFC

CONTENTS

1. Introduction

Part 2 of the Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law") and Section 4 of the Data Protection Regulations 2020 (the "Regulations") cover the topic of the Data Protection Officer ("DPO") Controller Assessment (the "Annual Assessment"), which effectively is regarding transfers of Personal Data outside of the DIFC.

Personal Data is defined in the DIFC DP Law as, "Any Data referring to an Identifiable Natural Person" and Special Category Data is defined as, "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person." Such data includes but is not limited to name, address, business or personal email address, business or personal phone numbers, geolocations, job title or other employee data, health and biometric data, religious affiliations or criminal history.

In sum, Personal Data generally can be any information that when viewed together (or in some cases is so unique) it clearly identifies a living individual. It could be data about clients, employees, suppliers, or family members, to name a few categories of Personal Data.

Many if not all organizations process Personal Data as a result, and will in some way engage in High Risk Processing ("HRP"), as defined in Schedule 1, Article 3 of the DP Law. In such cases, the entity must appoint a DPO, who then has the responsibility of completing or supporting completion of the Annual Assessment on or before each license renewal date, starting from July 1, 2021. This guidance will provide answers to questions about the Annual Assessment and help support the completion of it in the DIFC Client Portal (the "Portal"). The defined terms used herein have the same meaning as the defined terms in the DP Law.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the DIFC Commissioner of Data Protection (the **Commissioner**) either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

2. Scope

Due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance should be read in conjunction with those existing UK and EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. 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 firm.*

3. Checklist for the Annual Assessment

Before completing the Annual Assessment, please consider the following checklist:

1. Determine whether the entity engages in High Risk Processing

The Commissioner's Office has provided guidance and an HRP assessment tool to help determine whether the entity engages in HRP.

2. Appoint a DPO, where required

If, after reviewing the HRP guidance and / or survey, you determine that the entity does not engage in HRP, there is no need to appoint a DPO and therefore no need to complete the Annual Assessment. *If it does engage in HRP, a DPO must be appointed, by updating the Article 14 Notification (the "Notification") in the Portal*.

In certain cases, the Commissioner may direct an entity to appoint a DPO, or appointment of a DPO may be made on a voluntary basis, and therefore does mean that the Annual Assessment should be completed.

A DPO appointment assessment tool is also available to support making this important decision around accountability of your entity for ethical data management.

DIFC Bodies: Article 16 also states that DIFC Bodies must appoint a DPO. For the avoidance of doubt, entities holding any form of license or permission registered with the Registrar of Companies is *not* a DIFC Body.

3. Accessing the Annual Assessment – the DIFC Client Portal

The Annual Assessment is available as a service request under the Services tab of the DIFC Client Portal. In most cases, it is unlikely the DPO is also the portal user. In this case, the Portal user may provide access to the DPO as a user for Portal access, or the Portal user may work with the DPO to complete the Annual Assessment form. A Portal Access Guide for providing such access is available in the Handbooks and Fees section of the DIFC website.

Until July 1, 2021, a manual form was available on the DIFC DP website for reference, to help prepare DIFC entities for the Annual Assessment. This form was decommissioned when the automated template went live on July 1, 2021.

4. Information about Processing activities that is needed to complete the Annual Assessment

Primarily, to complete the Annual Assessment you will need to know about the Personal Data collection, sharing, deletion and storage methods. You will also need to understand the nature and scope of processing activities, the context of processing, purposes for processing and necessity and proportionality of the processing of Personal Data.

Most of the questions in each of these sections of the Annual Assessment will guide you with suggested responses for guidance purposes, and you must select something as these are also items the Commissioner's Office wants to understand about your data protection methods. But if you think there is more to tell us, you should provide additional information in text boxes, or by uploading flow diagrams, policies, links to online notices and information, or anything else that may help the Commissioner's Office understand the processing activities.

The information you will be asked about includes:

- Data collection methods
- Internal or external data sharing
- Why the data must be processed in the manner(s) it is
- Where it is processed, including transfers
- What technical and organizational measures are taken to secure the processing
- Lawful basis for processing
- Policies and procedures for providing notice to individuals about all of the above, as well as how to respond to their requests for access and information about the Personal Data your entity benefits from

5. Consider the Risks around the type(s) of processing the entity engages in

Remember that you are completing this form normally because the entity engages in HRP and has to appoint a DPO, or the leadership of the entity thought it is good practice in any case to

voluntarily appoint a DPO. This necessarily means there are risks associated with the processing.

The Commissioner's Office has provided a pre-populated risk assessment and mitigation template for you based on the answers provided in the Annual Assessment form, which will appear after the assessment part of the form is completed.

It is essential to note, in addition to the suggested answers in the selection lists throughout the form that the risk assessment and suggested mitigation actions ***are for guidance purposes only***. Each entity is responsible for assessing its own risks. If the pre-populated responses in the form or the risk assessment / mitigation actions sufficiently represent the position of the entity, the DPO may take it at face value and operate in accordance with it.

However, if there are additional responses and associated risks, please feel free to use this pre-populated risk assessment template as a starting point for your entity. You may download and edit it, add to it, remove anything that is not correct or quite right for your entity, or simply ignore it and do your own risk and mitigation assessment.

6. Submitting the Annual Assessment and next steps

Please submit the Annual Assessment like any other Service Request ("SR") in the Portal. There is no fee for the submission at this time. Once it is submitted, the information will be maintained in your account. A separate form will be available for any updates over the course of the year until your next Annual Assessment is due.

The Commissioner's Office does not approve the Annual Assessment in the Portal, but will review most of the submissions and may include certain entities for inspection purposes, based on response and clarity of the information, as well as the risks associated with the processing. In addition, you are always welcome to contact the Commissioner's Office with any questions or comments, or to request a voluntary inspection or consultation. Contact details for the Commissioner's Office are above. Your final submission and risk assessment guidance is available via the process set out below.

4. FAQs

It's called the DPO Controller Assessment in the DP Law. My entity is only a Processor but I have appointed a DPO in accordance with Article 16. Must I complete this form?

If your entity has appointed a DPO, it must complete this form. Even entities that are traditionally Processors can be and often are also Controllers, in that they collect Personal Data from employees, directors, suppliers, potential clients, stakeholders and other individuals, and thereby alone or jointly with others determines the purposes and means of the processing.

The idea is not to get too hung up on whether your entity is strictly a Controller or a Processor, as the line is often blurred and the two designations may apply to the same entity. More importantly, accountability is key, which your leadership probably has already agreed by doing a compliance assessment or other decision making process to ultimately appoint a DPO. It is accountability that the Annual Assessment seeks to instill in DIFC entities, starting with those that have appointed a DPO.

Is there a fee for submitting the Annual Assessment?

For the initial year of Annual Assessment submission, there will be no fees collected for its submission. As this is a pilot phase of the form, certain services and support may be derived and implemented by the Commissioner's Office to better assist your entity's compliance with the DP Law. Nominal fees may be collected at that time.

Is there a fine if the DPO does not complete the Annual Assessment?

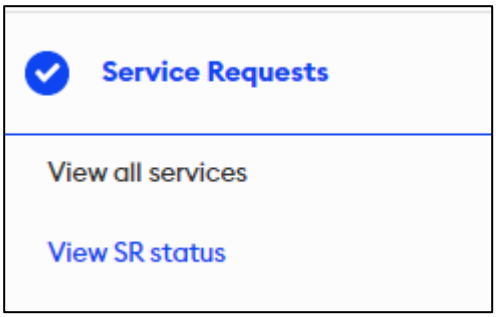
There is currently no fine for failure to complete the Annual Assessment. However, there are fines for the following related actions:

- Failure to notify the Commissioner's Office of Personal Data processing operations (Article 14(7))
- Failure to appoint a DPO where required (Article 16)

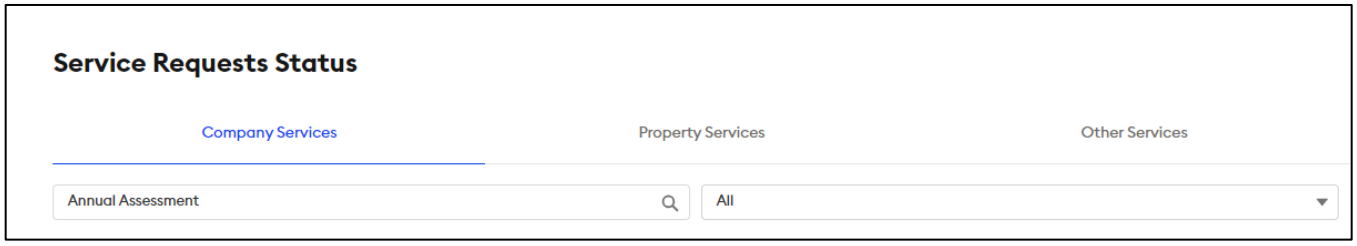
How can I access the Annual Assessment and Risk Matrix after I have made the submission for the year?

Please follow this process:

1. Go to the Client Portal home screen for your business
2. Click on Service Requests → View SR Status



3. In the search bar, type “Annual Assessment”



4. A list of all the Annual Assessments submitted for the business account you are logged in under will appear, and you can then select the assessment you wish to view. It will show you your answers to all of the questions, as well as the Risk Matrix. You can also search on the SR number, which is in the email from your submission notice.
5. Please note that you may download the Risk Matrix as a CSV (excel) file, but only prior to submitting the Annual Assessment. If you wish to download it to view it after submission, you can only download a PDF.

What's the difference between the Notification and the Annual Assessment?

Notification required under Article 14 is rather objective and basic in format, only asking certain initial questions during onboarding for new entities to get started on a compliance framework, or for existing entities that begin processing Personal Data to help them either start on a framework or add to what they already have in place.

The Annual Assessment, as you will see by completing it, is much more detailed, provides the risk assessment and mitigation template, and results in a much more subjective analysis of the entity's compliance with the DP Law. Once completed, it will supplement the Notification and may result in a few updates to it.

Lastly, remember that the Annual Assessment must only be completed where a DPO has been appointed. This is a limited number of DIFC entities. The Notification must be submitted by ***any*** DIFC entity that processes Personal Data, regardless of whether a DPO has been appointed.

What happens if I decide the entity no longer needs a DPO or that it no longer engages in HRP?

If the entity, in its own self-assessment, determines that it no longer engages in HRP, then it may update the Notification accordingly as this is a question asked in that template.

Remember however that if the DPO appointment line item in the Notification is not de-selected, the entity will receive a reminder at the next license and Notification renewal period that the Annual Assessment is also due. It is linked to the selection in the Portal of a DPO.

If HRP is no longer undertaken, the entity may still have a designated DPO as in ordinary processing environments, it is a voluntary appointment in any case. Remember that, again, if a DPO is appointed for whatever reason, the Annual Assessment must be submitted.

How do I update my entity's Notification?

Please access the Portal and submit a service request with the updated information. There may be a fee for submitting certain amendments in the Portal. Please see the Notifications section of the DIFC DP website.

5. Questions and Comments

Please contact the DIFC Commissioner of Data Protection either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office for any clarifications or questions related to this document. You may also wish to refer to the DIFC Online Data Protection Policy.