Below are TEST answers only. All possible positive response options have been selected so you can see the corresponding risk per question reflected in the Risk Matrix.

The link for the Overall Risk column of the Risk Matrix is:

https://portal.difc.ae/clientportal/resource/1676034393000/DPO_Overall_Risk_Key

Summary

Print Download

1. Objectives of the Annual Assessment

DIFC DP Law 2020 sets out principles of accountability, transparency and fairness to support individuals whose data is processed by DIFC licensed entities and certain third parties. While Data Protection Officer (DPO) appointment is only mandatory for DIFC Bodies (i.e., the Courts, DIFCA, DFSA) or for entities conducting High Risk Processing activities, any entity may voluntarily appoint a DPO. If you have done so, whether voluntarily appointed or not, you are required to complete this Annual Assessment. It is not the same as the Article 14(7) Notification.

The main objective of the Annual Assessment is to ensure that each entity that has appointed a DPO is reviewing its compliance, processes and procedures required by the DP Law 2020.

The Annual Assessment is comprised of 3 main parts: **Assessment** (to be completed by the entity DPO or similar representative), **Risk Review and Mitigation** (pre-populated guidance / best practice), and **Summary**

Please note that while the Annual Assessment is mandatory for organizations that must appoint a DPO, the multiple choice responses and the risk assessment and mitigation measures that your answers produce are **only possible answers or assumptions** based on current market knowledge and information. As such, **the responses and risk section contain non-binding guidance and suggested best practices.** You may leave them as is, as a sufficient response for the processing your organization does, or you may elaborate on in order to provide detailed data protection compliance measures. If the pre-determined response option provided does not sufficiently address your organization's data processing structure and requirements, text boxes are available in many places throughout the Annual Assessment form to provide such details, additional notes or supporting informational or policy documentation.

Thank you for completing this form. Any questions please contact info@difc.ae; commissioner@dp.difc.ae; by telephone on +971 4 362 2222, or via the Make an Enquiry page on the DIFC website.

2. Describe the Processing

a. Describe the nature of the Processing:

Briefly describe in your own words the ways in which your company or group of companies processes Personal Data by way of collection, use, storage and deletion. Please also describe the lawful bases for processing and the types of Personal Data that are processed.

How does your organisation Collect personal data?
Test 123

How does your organisation Use personal data?
Test 123

How does your organisation Delete personal data?
Test 123

How does your organisation Store personal data?
Test 123

Does the collected data include Special Category data? This includes data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records or offences, trade-union membership and health or sex life, as well as genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

FYI - Special Category Personal Data is defined in the DP Law 2020, Schedule 1, Article 3.
Yes

Does the collected data include information about vulnerable groups or individuals, i.e., children, people of determination, or others that may be considered vulnerable in the jurisdictions from which the data is collected?
Yes

What is the lawful basis for Processing?
Article 10(a);Article 10(b);Article 10(c);Article 10(d);Article 10(e);Article 10(f);Article 11(a);Article 11(b);Article 11(c);Article 11(d);Article 11(e);Article 11(f);Article 11(g);Article 11(h);Article 11(i);Article 11(j);Article 11(k);Article 11(l)

What is the source of the data?
Data subject directly;External sources

If external sources is selected, please list and identify external or any other sources (Optional)
Test 123

Does your organisation share Personal Data with any internal stakeholders or external third parties?
Yes

Please list any third parties (internal / external)
Internal - within the group of companies or between departments;External - with suppliers, vendors, contractors

Additional Notes (Optional)
Test 123

Provide a flow diagram (if available) or another way of describing the data processing flows. You may provide a written description of the data flows in the text box below, and you may upload a flow diagram in the "DOCUMENTS" section of this form, if one is available. Either action is (optional).
Test 123

b. Describe the scope of the Processing:

What types of Processing in your organisation's operations have been identified as likely to be high risk? High Risk processing is defined in the DP Law 2020, Schedule 1, Article 3. If you appointed a DPO in accordance with Article 16, it is usually because you engage in HRP. You may assess any changes or updates to this status using the HRP tool available at the hyperlink and on the DIFC DP Guidance page.

Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights;A considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject;The Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling;A material amount of Special Categories of Personal Data is to be Processed

Please provide any other helpful information to respond to the above question

If Other is selected, please specify

Test123

If Other is selected, please specify

Test123

c. Describe the context of the Processing:

What is the nature of your relationship with the individuals whose data your organisation processes?

Clients / Customers;Employees;Personal contacts;Business Partners / Suppliers;3rd Party or many 3rd Parties;Generative technology / AI users or developers;Other

Does your organisation provide a privacy policy or other notice to explain its processing activities in accordance with Articles 29 or 30?

Yes

Based on the privacy policy or other notice, would your organisation's processing operations match the expectations of a data subject (i.e., owners of the Personal Data)?

Yes

What is the current state of emerging or advanced technology in this area?

AI;Biometric identification – i.e., fingerprints;Blockchain;Cloud servers / processing;Other

Are you signed up to any approved code of conduct or certification scheme (if any have been approved for use in any jurisdiciton in which your organisation is based, such as CBPR(s)?

Yes

d. Describe the purposes of the Processing:

What will be achieved by Processing the various types and categories of Personal Data?

Test 123

You have chosen "None of the above", alone or in addition to other choices. If none of the choices apply, please only choose "None of the above". In that case, you would appear not to engage in HRP and therefore there is no mandatory requirement to appoint a DPO. If you do not engage in HRP for any of the reasons provided in the definition under the DP Law 2020, but you have opted to appoint a DPO, then please confirm why you have appointed a DPO, i.e., voluntarily for governance, required to do so by another law, etc

How long will your organisation keep such data?

We keep data indefinitely for research, statistics and scientific purposes, or for the length of applicability of an Article 22(4) exception;In accordance with internal retention policies;For the transaction only, but no personal data is stored or processed(documentation of regular cleansing available upon request);We have no set policy but will develop one;Other

How often is such data collected?

Automated or recurring basis through regular streaming / file download from a website using bots, scraping or other file transfer mechanism;Occasionally, as needed (transactional basis);When data subjects visit our webpage and request information or assistance, or to use our apps;When provided to us by a controller or processor (if the entity is a sub-processor);Other

What geographical area(s) does the collection and processing of personal data cover?

North America (Canada or Mexico);USA;South America;EU / UK;Middle East;Africa;South East Asia;North East Asia;China;Central Asia;India / subcontinent;Australia / New Zealand / Pacific Islands

If Other is selected, please specify

Test123

Additional Notes (Optional)

Test 123

Are there prior concerns or potential security flaws stated in the media, industry or amongst technology or privacy / security experts over this type of Processing ?

Yes

If Other is selected, please specify

Test123

Please give information about the code or scheme to which your entity is aligned.

Test 123

What legitimate purpose or benefit to individuals, if any, does the Processing serve?

Test 123

3. Assess accountability, necessity and proportionality

Describe accountability, necessity and proportionality measures, in particular:

How does your organisation ensure compliance with lawfulness / fairness, accuracy, minimisation, purpose specification and retention principles set out in Article 9 of DP Law 2020?

Test 123

If Other selected, please specify

Test123

Are transfers outside of the DIFC required for your organisation to operate / carry on processing operations?

Yes

What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?

DP and Security Policies and procedures (Organisational measures);Physical access security (IDs, sign in / out at building entry and exit);Security or privacy enhancing technology (technical measures);Cyber incident reporting and monitoring tools;Access management or retention procedures / approvals are in place;Record of processing activities;Due diligence as part of privacy by design / default;Other (please provide details)

In accordance with Articles 23 to 24, where applicable, what measures do you take to ensure any internal or external processors comply with DP Law 2020, to the extent it applies to the Processing activities?

Test 123

How does your organisation safeguard any international transfers?

In accordance with Article 26;In accordance with Article 27

If you selected Article 27, please choose the mechanism(s) your organization applies.

A27(1)(a) the Controller or Processor in question has provided appropriate safeguards (as described in Article 27(2)), and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available.;A27(1)(b) one of the specific derogations in Article 27(3) applies.;A27(1)(c) the limited circumstances in Article 27(4) apply.

If Other is selected, please specify

Test123

Additional Comments

None

If Other is selected, please specify

Test 123

Are any additional due diligence measures applied prior to the transfers?

Yes – DIFC EDMRI and EDMRI +;Yes – EU Transfer Impact Assessment;Yes – UK IDTA / Addendum;Yes – All of the above;Yes – Other (please provide details)

In what ways does your organisation support individuals' rights in line with Articles 32 to 40?

Subject access request / data subjects rights response policy;Data mapping of all systems, processors, sub-processors to ensure efficient retrieval of information;Provide multiple contact options to individuals who wish to request access to or control of their personal data;Provide regular training and reinforcement of how to identify an access request and handling measures to assure a response is provided within the lawful time period;All of the above;Additional Comments

Please describe your organisation's breach reporting policies and procedures that implement Articles 41 and 42.

Incident Management / Breach Reporting Policy;DPIA assessing nature / sensitivity of the Personal Data involved;All the above;Other (please provide details)

Download Risk Matrix As CSV

Identify, Assess and Mitigate Risks

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
Does the collected data include Special Category data? FYI – Special Category Personal Data is defined in the DP Law 2020, Schedule 1, Article 3.	**Yes**	**We process special category personal data on a regular basis in order to conduct our business**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
Does the collected data include information about vulnerable groups or individuals?	**Yes**	**We process personal data that contains information about children or other vulnerable individuals on a regular basis in order to conduct our business.**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing children's PD through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where children's PD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 10(a)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**Low**	**Medium**	**Reasonable Assurance**	**Risk is lowered when processing with data subject consent, provided that Article 12 elements are met. A regular assessment of compliance with this legal basis would be necessary to maintain a lower risk rating.**	**Conduct regular processing activities impact assessments, to ensure that consent is not stale and complies with Article 12. Maintain a consent preference database.**	**Risk remains relatively low provided recommended or other mitigation measures are in place.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What is the lawful basis for processing?	**Article 10(b)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**Low**	**Medium**	**Reasonable Assurance**	**Risk is lowered when processing based on performance of a contract to which the data subject is a party, or at the request of the data subject prior to entering into such contract. A regular assessment of compliance with this legal basis would be necessary to maintain a lower risk rating.**	**Conduct regular processing activities impact assessments, to ensure that the contract performance requirements, regardless of data subject participation, do not negatively impact the data subject.**	**Risk remains relatively low provided recommended or other mitigation measures are in place.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted**
What is the lawful basis for processing?	**Article 10(c)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**Low**	**Medium**	**Reasonable Assurance**	**Risk is lowered when processing is necessary for compliance with Applicable Law that a Controller is subject to. A regular assessment of compliance with this legal basis would be necessary to maintain a lower risk rating.**	**Conduct regular processing activities impact assessments, to ensure that the conditions of the Applicable Laws to which this basis applies continue to be enforceable and in effect.**	**Risk remains relatively low provided recommended or other mitigation measures are in place.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted**
What is the lawful basis for processing?	**Article 10(d)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**Low**	**Medium**	**Reasonable Assurance**	**Risk is lowered when processing is necessary to protect the vital interests of a data subject or of another natural person (i.e., a child or other vulnerable person). A regular assessment of compliance with this legal basis would be necessary to maintain a lower risk rating.**	**Conduct regular processing activities impact assessments, to ensure that the conditions relevant to the presumed vital interests continue to be in effect.**	**Risk remains relatively low provided recommended or other mitigation measures are in place.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted**
What is the lawful basis for processing?	**Article 10(e)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**Low**	**Medium**	**Reasonable Assurance**	**Risk is lowered when processing is necessary for DIFC Bodies (or relevant Third Parties) to perform a task or carry out regulatory powers or functions. A regular assessment of compliance with this legal basis would be necessary to maintain a lower risk rating.**	**Conduct regular processing activities impact assessments, to ensure that the conditions of this basis continue to be in effect.**	**Risk remains relatively low provided recommended or other mitigation measures are in place.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
What is the lawful basis for processing?	**Article 10(f)**	**One or more of our lawful bases for processing PD complies with Article 10 of the DP Law 2020.**	**High**	**High**	**Very Limited Assurance**	**Legitimate interests, when applied broadly (regardless of conditions set out in Article 13), and where such interests are outweighed by the interests or rights of a data subject, may not be a valid legal basis until such assessment is conducted and applied appropriately to safeguard data subjects interests or rights.**	**Conduct regular processing activities impact assessments, to demonstrate that legitimate interest(s) is identified properly and documents, and that broad reliance on legitimate interests is balanced with the interests or rights of a data subject and that the processing is necessary to achieve such interests.**	**Risk reduces somewhat, provided recommended or other mitigation measures are in place.**	**Some risk will remain where legitimate interests basis is applied. We must proceed with caution and continuously assess the identifiable interest(s), and the necessity and proportionality of such interests in comparison to a data subject's interests or rights.**
What is the lawful basis for processing?	**Article 11(a)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What is the lawful basis for processing?	**Article 11(b)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(c)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(d)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(e)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(f)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What is the lawful basis for processing?	**Article 11(g)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for Processing?	**Article 11(h)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020.**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA. Where Article 28 applies to the processing under this Article, we evaluate the risks and applies the additional safeguards set out in A28.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(i)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(j)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**
What is the lawful basis for processing?	**Article 11(k)**	**One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020**	**High**	**High**	**Very Limited Assurance**	**As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.**	**Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.**	**Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What is the lawful basis for processing?	Article 11(l)	One or more of our lawful bases for processing PD involves Special Category PD so requires compliance with Article 11 of the DP Law 2020	High	High	Very Limited Assurance	As a result of the regular processing of special category data, there may be a negative impact on the individuals to whom the PD belongs, and thereby causing harm to them if the processing results in a breach, unlawful disclosure or other data loss, and / or is not conducted in compliance with the DP Law 2020 or other applicable laws.	When we collect special category PD for processing, we can reduce the risk of loss, breach or negative impact on individual rights by complying with Article 11 of the DP Law 2020, and only collecting and allowing limited organizational access to the SCPD necessary to support the specific purpose for which it is obtained, as well as keep it accurate and up to date, and retain as little of it as possible to conduct our processing activities. Where this type of data supports HRP, we will take the actions set out above as well, including DPO appointment and regular DPIA / AA.	Risk is reduced by reducing ambiguity about obligations around processing special category data through training, enhanced security and retention policies, and access limitations.	Some risk will remain where SCPD must be processed. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO with all necessary tools including resources and training to ensure effective compliance.
What is the source of the data?	Data subject directly	We collect data directly from the data subject	Medium	Medium	Reasonable Assurance	Collecting PD directly from the data subject / individuals is less likely to cause harm to him or her because they have handed it over directly, but if there is a breach or unlawful / accidental data loss, the severity of harm is high.	Overall we can reduce our risk and provide a higher level of assurance that PD will be protected via internal policies and procedures for safe data processing of PD collected directly from them and our privacy policy reflects all collection methods and uses.	Organizational understanding and culture of personal data protection reduces risks.	Minimal; regular checks on compliance and implementation of any obligations are conducted
What is the source of the data?	External sources	We collect data from a 3rd party such as suppliers, vendors, contractors.	Medium	High	Very Limited Assurance	Collecting PD from a 3rd party is more likely to cause harm to a data subject / individual because they have not handed it over directly, and if there is a breach or unlawful / accidental data loss, the severity of harm is very high.	Overall we can reduce our risk and provide a higher level of assurance that PD will be protected via internal policies, procedures and contracts with the 3rd parties entailing DP obligations, to ensure safe data processing of PD collected indirectly and our privacy policy reflects all collection methods and uses. Such policies should include providing appropriate notices in accordance with Article 30.	Contractual obligations and consistent practices between organizations reduces risks.	Minimal; regular checks on compliance and implementation of any obligations are conducted
Does your organisation share personal data with any internal stakeholders or external third parties?	External – with suppliers, vendors, contractors	Yes we share PD externally, i.e., with suppliers, vendors, contractors	Medium	High	Limited Assurance	Sharing PD outside the group may be unlikely to cause harm but if there is a breach, the severity of harm will be high as there is less control over access and security once it has left an internal, controlled environment.	Overall we can reduce our risk and provide a higher level of assurance that PD will be protected if we adhere to Articles 23 to 28 of the DP Law 2020, executing contracts that include the required clauses, as well as where possible gaining agreement from 3rd parties that they will adhere to data protection principles and policies we are required to implement in compliance with DP Law 2020 for safe data processing. We can also conduct EDMRI+ due diligence assessment. [NOTE hyperlink for EDMRI+ is here: https://survey.alchemer.com/s3/6932685/DIFC-EDMRI-plus]	Contractual obligations and consistent practices between organizations reduce the risk created. Internal policies and training reduces risk of lack of knowledge about proper data handling practices.	Minimal; regular checks on compliance and implementation of any obligations are conducted
Does your organisation share personal data with any internal stakeholders or external third parties?	Internal – within the group of companies or between departments	Yes we share PD internally, i.e., within the group of companies or between departments	Low	Medium	Reasonable Assurance	Sharing PD within the group is less likely to cause harm but if there is a breach, the severity of harm is higher if the staff does not understand how to safely process PD within our company or group of companies.	Risk can be reduced by implementing additional policies (i.e., retention, subject access request) and training regarding lawful processing. Mechanisms for international transfers such as Binding Corporate Rules (certified, intragroup privacy procedures) or internal auditing / due diligence will also reduce risk when sharing data internally.	Significantly increases the effectiveness of technical and organisational measures, and more awareness around breach reporting, security, int'l transfer requirements, etc.	Minimal; regular checks on compliance and implementation of any measures are conducted

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What types of Processing in your organisation's operations have been identified as likely to be high risk?	**A considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject**	**We engage in one or more high risk processing activities**	**High**	**High**	**Very Limited Assurance**	**As a result of HRP activities identified such as A considerable amount of Personal Data will be Processed (including staff and contractor Personal Data) and where such Processing is likely to result in a high risk to the Data Subject, and where such Processing is likely to result in a high risk to the Data Subject, personal data processing by our company may negatively impact the individuals to whom the PD belongs, and thereby cause harm to them if the processing is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**Wherever possible, we will not rely on HRP for PD we collect and store. Where we do have to rely on HRP, we will adequately inform the relevant individuals and appoint a Data Protection Officer, as required under Article 16 of the DP Law 2020, who will be responsible for ensuring accountability of the organization and for the senior management's understanding of proper data management obligations and risks.**	**Notification to individuals and appointment of DPO results in transparency and accountability, reducing the risk of our organization contravening the DP Law 2020 and / or having a negative impact on the rights of individuals.**	**Some risk will remain where HRP must be conducted, due to the nature of the processing or the type of PD processed. We must proceed with caution and provide the DPO with all necessary tools including resources and training to ensure effective compliance.**
What types of Processing in your organisation's operations have been identified as likely to be high risk?	**The Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling**	**We engage in one or more high risk processing activities**	**High**	**High**	**Very Limited Assurance**	**As a result of HRP activities identified such as The Processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated Processing, including Profiling, and where such Processing is likely to result in a high risk to the Data Subject, personal data processing by our company may negatively impact the individuals to whom the PD belongs, and thereby cause harm to them if the processing is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**Wherever possible, we will not rely on HRP for PD we collect and store. Where we do have to rely on HRP, we will adequately inform the relevant individuals and appoint a Data Protection Officer, as required under Article 16 of the DP Law 2020, who will be responsible for ensuring accountability of the organization and for the senior management's understanding proper data management obligations and risks.**	**Notification to individuals and appointment of DPO results in transparency and accountability, reducing the risk of our organization contravening the DP Law 2020 and / or having a negative impact on the rights of individuals.**	**Some risk will remain where HRP must be conducted, due to the nature of the processing or the type of PD processed. We must proceed with caution and provide the DPO with all necessary tools including resources and training to ensure effective compliance.**
What types of Processing in your organisation's operations have been identified as likely to be high risk?	**A material amount of Special Categories of Personal Data is to be Processed**	**We engage in one or more high risk processing activities**	**High**	**High**	**Very Limited Assurance**	**As a result of HRP activities identified such as [Replace Selected Response], and where such Processing is likely to result in a high risk to the Data Subject, personal data processing by our company may negatively impact the individuals to whom the PD belongs, and thereby cause harm to them if the processing is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**Wherever possible, we will not rely on HRP for PD we collect and store. Where we do have to rely on HRP, we will adequately inform the relevant individuals and appoint a Data Protection Officer, as required under Article 16 of the DP Law 2020, who will be responsible for ensuring accountability of the organization and for the senior management's understanding proper data management obligations and risks.**	**Notification to individuals and appointment of DPO results in transparency and accountability, reducing the risk of our organization contravening the DP Law 2020 and / or having a negative impact on the rights of individuals.**	**Some risk will remain where HRP must be conducted, due to the nature of the processing or the type of PD processed. We must proceed with caution and provide the DPO with all necessary tools including resources and training to ensure effective compliance.**
What types of Processing in your organisation's operations have been identified as likely to be high risk?	**Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights**	**We engage in one or more high risk processing activities**	**High**	**High**	**Very Limited Assurance**	**As a result of HRP activities identified such as Processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a Data Subject or renders it more difficult for a Data Subject to exercise his rights, and where such Processing is likely to result in a high risk to the Data Subject, personal data processing by our company may negatively impact the individuals to whom the PD belongs, and thereby cause harm to them if the processing is not conducted in compliance with the DP Law 2020 or other applicable laws.**	**Wherever possible, we will not rely on HRP for PD we collect and store. Where we do have to rely on HRP, we will adequately inform the relevant individuals and appoint a Data Protection Officer, as required under Article 16 of the DP Law 2020, who will be responsible for ensuring accountability of the organization and for the senior management's understanding of proper data management obligations and risks.**	**Notification to individuals and appointment of DPO results in transparency and accountability, reducing the risk of our organization contravening the DP Law 2020 and / or having a negative impact on the rights of individuals.**	**Some risk will remain where HRP must be conducted, due to the nature of the processing or the type of PD processed. We must proceed with caution and provide the DPO with all necessary tools including resources and training to ensure effective compliance.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
How long will your organisation keep such data?	We keep data indefinitely for research, statistics and scientific purposes, or for the length of applicability of an Article 22(4) exception	In terms of data retention periods, we apply available permissions or exemptions to the retention principle for specific processing activities.	High	High	Limited Assurance	Provided our company has a set policy or guidance for data retention periods for specific processing activities, we may continue to process PD regardless of requests to cease processing or in accordance with the retention principle, until such specific circumstances or requirements change.	We will create, adhere to and train our staff on a detailed data retention policy that substantiates the circumstances for specific processing activities the permit or exempt us from deletion od PD or cessation of processing. It will be designed to require archiving PD that does not meet the specific processing activities criteria.	Enforcing data minimization and retention principles through such policies reduces the organization's risk of inadvertently processing PD that is no longer required to be retained either in practice or by law.	Minimal; regular checks on compliance and implementation of any obligations are conducted
How long will your organisation keep such data?	In accordance with internal retention policies	In terms of data retention periods, we have a set policy or guidance for when to archive or delete it, based on best practice or legal requirements.	Low	Medium	Limited Assurance	Because our company has a set policy or guidance for data retention periods, we are at risk of actively processing too much PD, PD that is inaccurate or not up to date, or PD that is being used for a purpose for which it was not collected, in direct breach of the data protection principles set out in Article 9 of the DP Law 2020	We will regularly review, update adhere to and train our staff on a detailed data retention policy. We have incorporated any requirements around putting PD beyond further use as set out in Article 22 of the DP Law 2020.	Enforcing data minimization and retention principles through such policies reduces the organization's risk of inadvertently processing PD that is no longer required to be retained either in practice or by law.	Minimal; regular checks on compliance and implementation of any obligations are conducted
How long will your organisation keep such data?	For the transaction only, but no personal data is stored or processed(documentation of regular cleansing available upon request)	In terms of data retention periods, our organisation's policy is to delete or cleanse data from our systems.	Low	Low	High Assurance	Transactional data that contains no personal data and is deleted or cleansed from our system is not ordinarily subject to the DIFC DP Law.	We will regularly review whether such processing ever contains PD as defined under the DIFC DP Law.	Enforcing data minimization and retention principles reduces the organization's risk of inadvertently processing PD that is no longer required to be retained either in practice or by law.	Minimal; regular checks on compliance and implementation of any obligations are conducted.
How long will your organisation keep such data?	We have no set policy but will develop one	In terms of data retention periods, we have no set policy or guidance for when to archive or delete it.	High	High	Very Limited Assurance	Because our company has no set policy or guidance for data retention periods, we are at risk of actively processing too much PD, PD that is inaccurate or not up to date, or PD that is being used for a purpose for which it was not collected, in direct breach of the data protection principles set out in Article 9 of the DP Law 2020.	We will create, adhere to and train our staff on a detailed data retention policy. It will be designed to require archiving PD that is no longer in use, up to date, or unnecessary to fulfil our specific processing purposes. We have incorporated any requirements around putting PD beyond further use as set out in Article 22 of the DP Law 2020.	Enforcing data minimization and retention principles reduces the organization's risk of inadvertently processing PD that is no longer required to be retained either in practice or by law.	Minimal; regular checks on compliance and implementation of any obligations are conducted
How often is such data collected?	Automated or recurring basis through regular streaming / file download from a website using bots, scraping or other file transfer mechanism	Our company collects data on an automated or other recurring basis through regular streaming / file download from a website using bots, scraping or other file transfer mechanism	Medium	High	Limited Assurance	Due to the frequency of data collection through the method of automated or other recurring basis through regular streaming / file download from a website using bots, scraping or other file transfer mechanism, there is a risk that we are breaching the data minimization and / or purpose specification principles by collecting too much data and / or for processing in a manner that is incompatible with what we have notified individuals about.	We can reduce our risk of contravening the DP Law 2020 and negatively impacting individual rights by collection PD directly from individuals who have been provided appropriate notice of processing activities, wherever possible. We also take necessary precautions where collection of data by this method is transferred to a non-DIFC, non-adequate jurisdiction, by applying the same principles and obligations in the destination as would be applied in the DIFC.	Less risk through direct collection and if not then applying through contracts, policies and procedures the same law and ethical requirements around data collection within the organization and in the destination of processing.	Minimal; regular checks on compliance and implementation of any obligations are conducted
How often is such data collected?	When provided to us by a controller or processor (if the entity is a sub-processor)	Our company collects data through regular, stable arrangements i.e., when provided to us by a controller or processor (if we are acting as a sub-processor)	Medium	High	Limited Assurance	Due to obtaining PD indirectly from a third party, we do not have direct consent or instructions or other legitimate basis provided by the individual to whom the data belongs for processing, and we are trusting that the controller or processor that shared it with us is in compliance with applicable DP laws, including specifically requirements for transfers outside the DIFC and / or any other data sharing requirements.	We can reduce our risk of contravening the DP Law 2020 and negatively impacting individual rights by collection PD directly from individuals who have been provided appropriate notice of processing activities, wherever possible. We also take necessary precautions where collection of data by this method is transferred to a non-DIFC, non-adequate jurisdiction, by applying the same principles and obligations in the destination as would be applied in the DIFC.	Less risk through direct collection and if not then applying through contracts, policies and procedures the same law and ethical requirements around data collection within the organization and in the destination of processing.	Minimal; regular checks on compliance and implementation of any obligations are conducted

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What geographical area does it cover?	**EU / UK**	**Our company transfers PD to lower risk jurisdictions for processing PD. They are lower risk because they have a DP law and / or operating environment that is compatible or equivalent to the DIFC, and there are very few remaining enforcement or implementation concerns for the exporting entity to be aware of. Onward transfers should be monitored as needed.**	**Low**	**Medium**	**High Assurance**	**Because we must transfer PD to a place that may have / has a compatible or equivalent DP Law and operating environment to that of the DIFC, we have a lower risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 are less likely to occur as a result.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Very little risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**Australia / New Zealand / Pacific Islands**	**Our company transfers PD to lower risk jurisdictions for processing PD. They are lower risk because they have a DP law and / or operating environment that is compatible or equivalent to the DIFC, and there are very few remaining enforcement or implementation concerns for the exporting entity to be aware of. Onward transfers should be monitored as needed.**	**Low**	**Medium**	**High Assurance**	**Because we must transfer PD to a place that may have / has a compatible or equivalent DP Law and operating environment to that of the DIFC, we have a lower risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 are less likely to occur as a result.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Very little risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**India / subcontinent**	**Our company transfers PD to very high risk jurisdictions for processing PD. They are high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be very closely monitored as well.**	**High**	**High**	**Very Limited Assurance**	**Because we must transfer PD to a place that does not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a higher risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**We will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Greater amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What geographical area does it cover?	**China**	**Our company transfers PD to very high risk jurisdictions for processing PD. They are high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be very closely monitored as well.**	**High**	**High**	**Very Limited Assurance**	**Because we must transfer PD to a place that does not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a higher risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**We will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Greater amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**Africa**	**Our company transfers PD to very high risk jurisdictions for processing PD. They are high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be very closely monitored as well.**	**High**	**High**	**Very Limited Assurance**	**Because we must transfer PD to a place that does not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a higher risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**We will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Greater amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**USA**	**Our company transfers PD to very high risk jurisdictions for processing PD. They are high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be very closely monitored as well.**	**High**	**High**	**Very Limited Assurance**	**Because we must transfer PD to a place that does not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a higher risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**We will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Greater amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**Central Asia**	**Our company transfers PD to very high risk jurisdictions for processing PD. They are high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be very closely monitored as well.**	**High**	**High**	**Very Limited Assurance**	**Because we must transfer PD to a place that does not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a higher risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**We will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Greater amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What geographical area does it cover?	**North East Asia**	**Our company transfers PD to medium to high risk jurisdictions for processing PD. They are medium to high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be monitored on a regular, on-going basis.**	**Medium**	**High**	**Limited Assurance**	**Because we must transfer PD to a place that may not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a medium to high risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur regardless of the relative safety of the jurisdiction.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Certain amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**Middle East**	**Our company transfers PD to medium to high risk jurisdictions for processing PD. They are medium to high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be monitored on a regular, on-going basis.**	**Medium**	**High**	**Limited Assurance**	**Because we must transfer PD to a place that may not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a medium to high risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur regardless of the relative safety of the jurisdiction.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Certain amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**North America (Canada or Mexico)**	**Our company transfers PD to medium to high risk jurisdictions for processing PD. They are medium to high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be monitored on a regular, on-going basis.**	**Medium**	**High**	**Limited Assurance**	**Because we must transfer PD to a place that may not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a medium to high risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur regardless of the relative safety of the jurisdiction.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Certain amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What geographical area does it cover?	**South East Asia**	**Our company transfers PD to moderate risk jurisdictions for processing PD. They are moderate risk because they have a DP law and / or operating environment that is compatible or equivalent to the DIFC, but there are remaining enforcement or implementation concerns for the exporting entity to be aware of. Onward transfers should be monitored as part of regular review.**	**Medium**	**Medium**	**Reasonable Assurance**	**Because we must transfer PD to a place that may have / has a compatible or equivalent DP Law and/ or operating environment to that of the DIFC, we have a moderate risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur as a result.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Some risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What geographical area does it cover?	**South America**	**Our company transfers PD to medium to high risk jurisdictions for processing PD. They are medium to high risk because they do not have a DP law and / or operating environment that is compatible or equivalent to the DIFC. Onward transfers should be monitored on a regular, on-going basis.**	**Medium**	**High**	**Limited Assurance**	**Because we must transfer PD to a place that may not have a compatible or equivalent DP Law and / or operating environment to that of the DIFC, we have a medium to high risk that it will not be treated by the organization receiving it with the same care and diligence. Breaches, inappropriate onward transfers, or other circumstances that directly contravene the DP Law 2020 may occur regardless of the relative safety of the jurisdiction.**	**Where adequacy recognition has not been provided, we will reduce our risk by executing contracts that include required DP clauses and additional safeguards provided for in Article 27, so that the PD will be treated by the organization receiving it with the same care and diligence as it does in the DIFC.**	**Less risk of breaches or inappropriate data sharing by the importing organization, less risk of our organization contravening the DP Law 2020.**	**Certain amount of risk will remain where PD must be processed outside of the DIFC in these jurisdictions. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
Are there prior concerns or potential security flaws in the media, industry or amongst technology or privacy / security experts over this type of processing ?	**Yes**	**We engage in processing that is associated with known prior concerns or security flaws.**	**Medium**	**High**	**Very Limited Assurance**	**Processing methods we use are unproven, or otherwise raise valid concerns about security or validity of the processing, which may result in data breaches or other unlawful access, or may negatively impact data subjects' rights such as erasure, objection or rectification.**	**We will reduce our security risk around the type of processing we engage in by ensuring appropriate technical and organizational measures are in place, and / or seeking consultation with IT and security experts on Privacy Enhancing Technologies.**	**TOMs and PET will reduce our risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain where PD must be processed by way of emerging or technology, which may also be considered HRP, or technology that in any case may prevent individuals from exercising their rights. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What is the current state of emerging or advanced technology in this area?	**AI**	**We engage in the following types of emerging or advanced IT to conduct our business and / or processing activities: (populate with the choices from above)**	**Medium**	**High**	**Very Limited Assurance**	**Processing methods we use have yet to be completely understood by individuals whose data is subject to it, and this lack of understanding may negatively impact data subjects' rights such as erasure, objection or rectification.**	**We will reduce our security risk around the type of processing we engage in by ensuring appropriate technical and organizational measures are in place, and / or seeking consultation with IT and security experts on Privacy Enhancing Technologies.**	**TOMs and PET will reduce our risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain where PD must be processed by way of emerging or technology, which may also be considered HRP, or technology that in any case may prevent individuals from exercising their rights. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What is the current state of emerging or advanced technology in this area?	**Cloud servers / processing**	**We engage in the following types of emerging or advanced IT to conduct our business and / or processing activities: (populate with the choices from above)**	**Medium**	**High**	**Very Limited Assurance**	**Processing methods we use have yet to be completely understood by individuals whose data is subject to it, and this lack of understanding may negatively impact data subjects' rights such as erasure, objection or rectification.**	**We will reduce our security risk around the type of processing we engage in by ensuring appropriate technical and organizational measures are in place, and / or seeking consultation with IT and security experts on Privacy Enhancing Technologies.**	**TOMs and PET will reduce our risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain where PD must be processed by way of emerging or technology, which may also be considered HRP, or technology that in any case may prevent individuals from exercising their rights. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What is the current state of emerging or advanced technology in this area?	**Blockchain**	**We engage in the following types of emerging or advanced IT to conduct our business and / or processing activities: (populate with the choices from above)**	**Medium**	**High**	**Very Limited Assurance**	**Processing methods we use have yet to be completely understood by individuals whose data is subject to it, and this lack of understanding may negatively impact data subjects' rights such as erasure, objection or rectification.**	**We will reduce our security risk around the type of processing we engage in by ensuring appropriate technical and organizational measures are in place, and / or seeking consultation with IT and security experts on Privacy Enhancing Technologies.**	**TOMs and PET will reduce our risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain where PD must be processed by way of emerging or technology, which may also be considered HRP, or technology that in any case may prevent individuals from exercising their rights. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**
What is the current state of emerging or advanced technology in this area?	**Biometric identification – i.e., fingerprints**	**We engage in the following types of emerging or advanced IT to conduct our business and / or processing activities: (populate with the choices from above)**	**Medium**	**High**	**Very Limited Assurance**	**Processing methods we use have yet to be completely understood by individuals whose data is subject to it, and this lack of understanding may negatively impact data subjects' rights such as erasure, objection or rectification.**	**We will reduce our security risk around the type of processing we engage in by ensuring appropriate technical and organizational measures are in place, and / or seeking consultation with IT and security experts on Privacy Enhancing Technologies.**	**TOMs and PET will reduce our risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain where PD must be processed by way of emerging or technology, which may also be considered HRP, or technology that in any case may prevent individuals from exercising their rights. We must proceed with caution and provide our staff with training and enhanced security policy instructions, and providing the DPO (if appointed) with all necessary tools including resources and training to ensure proper accountability and data sharing practices.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**DP and Security Policies and procedures (Organisational measures)**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Physical access security (IDs, sign in / out at building entry and exit)**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Security or privacy enhancing technology (technical measures)**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Cyber incident reporting and monitoring tools**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Due diligence as part of privacy by design / default**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Record of processing activities**	**If it is unclear what technical and organisational measures (TOMs) apply within an organisation, or if the TOMs are not in line with best practice, robust, or clear to the staff how to apply them, general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate policies, procedures, security and privacy enhancing technologies, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 .**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
What technical and organizational measures are taken to secure and control the environment in which the Personal Data are processed in accordance with Article 9(j) and Article 14(2) of the DP Law 2020?	**Other (please provide details)**	**While non-standard or untested TOMs can be effective, until vetted properly, use of such TOMs potentially increases the propensity for non-compliance with DP Law 2020 and lack of appropriate safeguards for exported Personal Data.**	**TBD by DPO**	**TBD by DPO**	**UNKNOWN**	**While non-standard or untested TOMs can be effective, until vetted properly, use of such TOMs potentially increases the propensity for non-compliance with DP Law 2020 and lack of appropriate compliance with the DP Law 2020.**	**Regular review, updates and internal audit of TOMs aids continuous improvement of accountability of the organisation. Incorporating generally accepted TOMs may also mitigate risk.**	**TOMs should create and support a culture of compliance, as well as reduce our risk significantly if implemented correctly and if resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
Are transfers outside of the DIFC required for your organisation to operate / carry on processing operations?	**Yes**	**When personal data is transferred to a jurisdiction outside of the DIFC, the risk increases with respect to whether similar protections exist in that importing jurisdiction, i.e., in law or national policy, etc.**	**Medium**	**High**	**Very Limited Assurance**	**Our organisation sends data outside the DIFC and must therefore consider risks of the personal data being processed without appropriate safeguards as set out in either Article 26 or 27.**	**We will apply the DIFC, EU, UK or other approved standard contractual clauses, binding corporate rules, or other available transfer mechanisms as set out in the DP Law 2020 or prescribed DP Regulations and Export Handbook. Derogations (A27(3)) and limited circumstance (A27(4)) transfer mechanisms are generally less reliable than SCCs, BCRs or others in A27(2) but may be applied. To do so, we should conduct an impact assessment to assess the risk of the transfer taking place in this manner.**	**Applying appropriate safeguards, particularly contractual safeguards such as the SCCs, will lower risk and ensure a certain level of protection / compliance with laws.**	**Some risk will remain as personal data is generally safer in the home jurisdiction where the regulator and applicable laws are consistent for that entity to comply with. Compliance with new laws or reliance on an importer to apply local DP laws, if any, in the importing jurisdiction creates uncertainty and results in a certain amount of residual risk.**
How does your organisation safeguard any international transfers?	**In accordance with Article 26**	**We transfer data to importers in Third Countries or to International Organisations that have been assessed as having same or similar DP Laws and Regulations. Such transfers may include access from our entity in the DIFC for the purposes remote processing in the cloud.**	**Medium**	**Medium**	**Limited Assurance**	**Sharing personal data with an importer in a jurisdiction that has similar laws, regulations, supervision and enforcement mechanisms in place provides limited assurance that the processing environment to some degree provides appropriate safeguards. It does not however guarantee safe processing in the importing organisation itself.**	**Additional assessments of risk such as reference to the Ethical Data Management Risk Index (EDMRI) Guidance and EDMRI+ due diligence tool will further mitigate issues of importer non-compliance, even in an "adequate" jurisdiction. Implementing additional safeguards where necessary for importer compliance will further enhance the safeguards provided in such jurisdictions.**	**Implementing all safeguards as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
How does your organisation safeguard any international transfers?	**In accordance with Article 27**	**We transfer data to importers in Third Countries or to International Organisations that have not been assessed as having same or similar DP Laws and Regulations. Such transfers may include access from our entity in the DIFC for the purposes remote processing in the cloud.**	**High**	**High**	**Very Limited Assurance**	**Sharing personal data with an importer in a jurisdiction that does not have similar laws, regulations, supervision and enforcement mechanisms in place results in very limited assurance that the processing environment is secure and compliant with applicable laws.**	**Additional assessments of risk such as reference to the Ethical Data Management Risk Index (EDMRI) Guidance and EDMRI+ due diligence tool will further mitigate issues of importer non-compliance, even in an "adequate" jurisdiction. Implementing additional safeguards where necessary for importer compliance will further enhance the safeguards provided in such jurisdictions.**	**Implementing all safeguards as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
If you selected Article 27, please choose the mechanism(s) your organization applies.	**A27(1)(b) one of the specific derogations in Article 27(3) applies.**	**Transferring Personal Data outside of the DIFC may result in it coming to rest in a jurisdiction that does not have a robust or any data protection law, or importer non-compliance risk exists, or both.**	**Medium**	**High**	**Limited Assurance**	**Implementing one of the available derogations, which are often subjectively assessed by the exporter, provides limited assurance that the processing in the importing jurisdiction will be compliant with applicable DP Laws and best practices.**	**Where possible, review and further implement all safeguards as necessary and proportionate, such as doing impact assessments or applied use of a combination of measures. Bare minimum safeguarding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all safeguards as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
If you selected Article 27, please choose the mechanism(s) your organization applies.	**A27(1)(c) the limited circumstances in Article 27(4) apply.**	**Transferring Personal Data outside of the DIFC may result in it coming to rest in a jurisdiction that does not have a robust or any data protection law, or importer non-compliance risk exists, or both.**	**High**	**High**	**Very Limited Assurance**	**Implementing one of the available derogations, which are often subjectively assessed by the exporter, provides limited assurance that the processing in the importing jurisdiction will be compliant with applicable DP Laws and best practices.**	**Where possible, review and further implement all safeguards as necessary and proportionate, such as doing impact assessments or applied use of a combination of measures. Bare minimum safeguarding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all safeguards as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
Are any additional due diligence measures applied prior to the transfers?	**Yes - DIFC EDMRI and EDMRI +**	**Doing the bare minimum to comply with Article 27 is insufficient in terms of best practice or organisational accountability.**	**Medium**	**Medium**	**Limited Assurance**	**Use of such due diligence measures increases the propensity for compliance with DP Law 2020, clarifies the knowledge of the importer's practices and compliance framework, and enhances accountability of all parties to the transfer.**	**Where possible, review and further implement all due diligence measures as necessary and proportionate, such as use of the DIFC EDMRI / EDMRI+, as bare minimum understanding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all due diligence measures as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
Are any additional due diligence measures applied prior to the transfers?	**Yes - EU Transfer Impact Assessment**	**Doing the bare minimum to comply with Article 27 is insufficient in terms of best practice or organisational accountability.**	**Medium**	**Medium**	**Limited Assurance**	**Use of such due diligence measures increases the propensity for compliance with DP Law 2020, clarifies the knowledge of the importer's practices and compliance framework, and enhances accountability of all parties to the transfer.**	**Where possible, review and further implement all due diligence measures as necessary and proportionate, such as use of the DIFC EDMRI / EDMRI+, as bare minimum understanding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all due diligence measures as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
Are any additional due diligence measures applied prior to the transfers?	**Yes - UK IDTA / Addendum**	**Doing the bare minimum to comply with Article 27 is insufficient in terms of best practice or organisational accountability.**	**Medium**	**Medium**	**Limited Assurance**	**Use of such due diligence measures increases the propensity for compliance with DP Law 2020, clarifies the knowledge of the importer's practices and compliance framework, and enhances accountability of all parties to the transfer.**	**Where possible, review and further implement all due diligence measures as necessary and proportionate, such as use of the DIFC EDMRI / EDMRI+, as bare minimum understanding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all due diligence measures as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
Are any additional due diligence measures applied prior to the transfers?	**Yes - All of the above**	**Doing the bare minimum to comply with Article 27 is insufficient in terms of best practice or organisational accountability.**	**Medium**	**Medium**	**Limited Assurance**	**Use of such due diligence measures increases the propensity for compliance with DP Law 2020, clarifies the knowledge of the importer's practices and compliance framework, and enhances accountability of all parties to the transfer.**	**Where possible, review and further implement all due diligence measures as necessary and proportionate, such as use of the DIFC EDMRI / EDMRI+, as bare minimum understanding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all due diligence measures as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
Are any additional due diligence measures applied prior to the transfers?	**Yes - Other (please provide details)**	**Doing the bare minimum to comply with Article 27 is insufficient in terms of best practice or organisational accountability.**	**TBD by DPO**	**TBD by DPO**	**UNKNOWN**	**While non-standard or untested due diligence measures can be effective, until vetted properly, use of such measures potentially increases the propensity for non-compliance with DP Law 2020 and lack of appropriate safeguards for exported Personal Data.**	**Where possible, review and further implement all safeguards as necessary and proportionate, such as use of the DIFC EDMRI / EDMRI+, as bare minimum understanding of the processing environment where Personal Data comes to rest does not sufficiently assure the accountability and compliance of the importer.**	**Implementing all due diligence measures as necessary and proportionate will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws vary somewhat between jurisdictions, importers may not sufficiently apply contractual or legal obligations, or litigation regarding transfer mechanisms may render specific ones non-compliant such that a replacement will urgently be required.**
In what ways does your organisation support individuals' rights in line with Articles 32 to 40?	**Subject access request / data subjects rights response policy**	**Without policies, procedures or training about handling data subject access and information requests, the risk of negatively impacting individuals' rights increases significantly.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate handling of data subject access and information requests provides reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement appropriate handling of data subject access and information requests, as response preparation assures organisational accountability and a culture of compliance.**	**Implementing appropriate handling of data subject access and information requests will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
In what ways does your organisation support individuals' rights in line with Articles 32 to 40?	**Data mapping of all systems, processors, sub-processors to ensure efficient retrieval of information**	**Without policies, procedures or training about handling data subject access and information requests, the risk of negatively impacting individuals' rights increases significantly.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate handling of data subject access and information requests provides reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement appropriate handling of data subject access and information requests, as response preparation assures organisational accountability and a culture of compliance.**	**Implementing appropriate handling of data subject access and information requests will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
In what ways does your organisation support individuals' rights in line with Articles 32 to 40?	**Provide multiple contact options to individuals who wish to request access to or control of their personal data**	**Without policies, procedures or training about handling data subject access and information requests, the risk of negatively impacting individuals' rights increases significantly.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate handling of data subject access and information requests provides reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement appropriate handling of data subject access and information requests, as response preparation assures organisational accountability and a culture of compliance.**	**Implementing appropriate handling of data subject access and information requests will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
In what ways does your organisation support individuals' rights in line with Articles 32 to 40?	**Provide regular training and reinforcement of how to identify an access request and handling measures to assure a response is provided within the lawful time period**	**Without policies, procedures or training about handling data subject access and information requests, the risk of negatively impacting individuals' rights increases significantly.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate handling of data subject access and information requests provides reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement appropriate handling of data subject access and information requests, as response preparation assures organisational accountability and a culture of compliance.**	**Implementing appropriate handling of data subject access and information requests will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
In what ways does your organisation support individuals' rights in line with Articles 32 to 40?	**All of the above**	**Without policies, procedures or training about handling data subject access and information requests, the risk of negatively impacting individuals' rights increases significantly.**	**Low**	**Medium**	**High Assurance**	**Creating and implementing appropriate handling of data subject access and information requests provides reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement appropriate handling of data subject access and information requests, as response preparation assures organisational accountability and a culture of compliance.**	**Implementing appropriate handling of data subject access and information requests will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Minimal; regular checks on compliance and implementation of any obligations are conducted.**
Please describe your organisation's breach reporting policies and procedures that implement Articles 41 and 42.	**Incident Management / Breach Reporting Policy**	**When a data breach occurs, an organisation must be prepared to determine whether the breach is reportable, and if so, whether to report to the Commissioner and / or the Data Subject. Lack of preparation means that general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate breach / incident assessment and reporting policies and procedures, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement robust breach / incident assessment and reporting policies and procedures, use informational resources effectively, and regular mapping the location, processors, and systems in which Personal Data is processed, as breach / incident response preparation assures organisational accountability and a culture of compliance.**	**Implementing many breach / incident response measures, as necessary and proportionate, will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws and reporting obligations vary somewhat between jurisdictions, and technology to enable breaches is rapidly evolving.**
Please describe your organisation's breach reporting policies and procedures that implement Articles 41 and 42.	**DPIA assessing nature / sensitivity of the Personal Data involved**		**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate breach / incident assessment and reporting policies and procedures, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement robust breach / incident assessment and reporting policies and procedures, use informational resources effectively, and regular mapping the location, processors, and systems in which Personal Data is processed, as breach / incident response preparation assures organisational accountability and a culture of compliance.**	**Implementing many breach / incident response measures, as necessary and proportionate, will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws and reporting obligations vary somewhat between jurisdictions, and technology to enable breaches is rapidly evolving.**
Please describe your organisation's breach reporting policies and procedures that implement Articles 41 and 42.	**Other (please provide details)**	**When a data breach occurs, an organisation must be prepared to determine whether the breach is reportable, and if so, whether to report to the Commissioner and / or the Data Subject. Lack of preparation means that general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**TBD by DPO**	**TBD by DPO**	**UNKNOWN**	**While non-standard or untested breach / incident assessment and reporting policies and procedures can be effective, until vetted properly, use of such measures potentially increases the propensity for non-compliance with DP Law 2020 and lack of appropriate safeguards for exported Personal Data.**	**Where possible, review and further implement robust breach / incident assessment and reporting policies and procedures, use informational resources effectively, and regular mapping the location, processors, and systems in which Personal Data is processed, as breach / incident response preparation assures organisational accountability and a culture of compliance.**	**Implementing many breach / incident response measures, as necessary and proportionate, will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws and reporting obligations vary somewhat between jurisdictions, and technology to enable breaches is rapidly evolving.**

Assessment Question	Assessment Response	Risk Description	Likelihood Of Harm	Severity Of Harm	Overall Risk	Risk Assessment	Mitigation Measures To Reduce Or Eliminate Risk	Effect On Risk	Residual Risk
Please describe your organisation's breach reporting policies and procedures that implement Articles 41 and 42.	**All the above**	**When a data breach occurs, an organisation must be prepared to determine whether the breach is reportable, and if so, whether to report to the Commissioner and / or the Data Subject. Lack of preparation means that general organisational risk and specific risk of negatively impacting accountability for data subjects' personal data will exist.**	**Medium**	**Medium**	**Reasonable Assurance**	**Creating and implementing appropriate breach / incident assessment and reporting policies and procedures, using informational resources effectively, and mapping the location, processors, and systems in which Personal Data is processed, provide reasonable assurance of compliance with the DP Law 2020 as well as accountability and transparency to the regulator and the Data Subject.**	**Where possible, review and further implement robust breach / incident assessment and reporting policies and procedures, use informational resources effectively, and regular mapping the location, processors, and systems in which Personal Data is processed, as breach / incident response preparation assures organisational accountability and a culture of compliance.**	**Implementing many breach / incident response measures, as necessary and proportionate, will result in compliance with the DP Law 2020, creating a culture of compliance and reducing risk significantly if implemented correctly and resource is provided to support these measures.**	**Some risk will remain as data protection laws and reporting obligations vary somewhat between jurisdictions, and technology to enable breaches is rapidly evolving.**

Summary

Confirm whether High Risk Processing Activities are conducted

Yes

DPO details and contact information is included in annual Article 14(7) notification to DIFC DP Commissioner

Yes

Notification to Commissioner is up to date, and includes all necessary information?

Yes