DIFC

CONSULTATION PAPER:

NON-LEGISLATIVE PROPOSAL ON MULTI-LATERAL DATA SHARING AGREEMENT AND ENABLING TECHNOLOGY PLATFORM

NOVEMBER 2022

Commissioner of Data Protection

DIFC

CONTENTS

DIFC

CONSULTATION PAPER ON NON-LEGISLATIVE PROPOSAL RELATING TO TECHNOLOGY PRINCPLES AND MULTI-LATERAL DATA SHARING

Why are we issuing this consultation paper?

This Consultation Paper issued November 2022 ("Consultation Paper") in accordance with Article 46(4) of the Data Protection Law, DIFC Law No. 5 of 2020 (the **DP Law 2020**) seeks public comments on the proposal by the Dubai International Financial Centre Authority (**DIFCA**) to develop a pilot program to test a multi-lateral, international data sharing agreement and adequacy decision, supported by digital economy enabling technology promulgated by best practice technology development principles (the **Multi-lateral Data Sharing Pilot**). Details about this concept are set out in the "Background" section.

Who should read this paper?

1. This Consultation Paper would be of interest to people conducting or proposing to conduct business and Processing operations in the DIFC. In particular:

   (a) companies currently operating in the DIFC or intending to operate in the DIFC;

   (b) employees and customers of such companies;

   (c) parties seeking to enter into transactions with companies in the DIFC, including by providing services to companies in the DIFC;

   (d) international groups of companies with cross-border data flows in and out of the DIFC; or

   (e) legal advisors and compliance advisors.

How to provide comments

3. All comments should be provided by submitting them via this response link.

You may also submit written comments, questions or concerns to:

Jacques Visser
Commissioner of Data Protection[1]
DIFC Office of Data Protection[2], DIFC Authority
Level 14, The Gate, P. O. Box 74777
Dubai, United Arab Emirates
Or by e-mail to: commissioner@dp.difc.ae

4. You may choose to identify the organisation you represent in your comments, if applicable.

5. DIFCA reserves the right to publish, on its website or elsewhere, any comments you provide, unless you expressly request otherwise at the time the comments are made. Comments will be published anonymously in any case.

6. Responding to this non-legislative consultation is voluntary, and any Personal Data submitted will be managed in accordance with the DIFC Online Data Protection Policy.

What happens next?

7. The deadline for providing comments on the proposals in this Consultation Paper is **30 November 2022**. At that time we will consider further requirements.

8. **Please note that this consultation is not for legislative purposes**. This consultation is being conducted to demonstrate DIFC's interests in accountability and transparency, thought leadership and willingness to seek all views and concerns about this important subject matter. DIFC Authority does not usually conduct public consultation on guidance related issues and will only do so in limited circumstances in the future.

[1] Hereinafter referred to as the Commissioner
[2] Hereinafter referred to as the Office

Defined terms

9. Defined terms are identified throughout this paper by the capitalisation of the initial letter of a word or of each word in a phrase or by definition in the DP Law 2020. Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning.

Background[3]

10. Adequacy and other transfer safeguards were developed to support safe transfers of Personal Data when the only existing relevant law was the 1995 EU directive / implementing national laws in each Member State. At this point, there are over 100 data protection laws. Given the participation of many of these jurisdictions in Convention 108+ in some form, whether as ratifiers or observers, and as reliable research shows that many of them have significant similarities, arguably the laws in these places are fruit of the original tree.[4]

11. As such, then it should be possible to agree at least a bare minimum acceptance of the same requirements and synergies of most data protection laws at their core. Furthermore, how exporters and importers apply them is of significant importance in the current debate about data export and sharing.

12. Currently, decision-making around transfer mechanisms is rather limited to a binary decision – apply the relevant model clauses (because there is not an adequacy decision in place in that jurisdiction) or not (because there is an adequacy decision in place). This is because:

    a) there are 32 companies with (EU Commission) approved binding corporate rules in place, and external agreements are required anyway to use them as a transfer mechanism with third parties;

    b) derogations ought to be applied sparingly due to their very specific, conditional nature.

[3] Please note that the contents of this section are drawn and developed from the Abstract of the underlying concept paper found at this link.

[4] https://www.dataguidance.com/comparisons/comparing-privacy-laws, https://www.dlapiperdataprotection.com/

13. Correct application and use of relevant model clauses is complex for most organisations, and even then, in certain jurisdictions, is not always the safest safeguard and additional measures may be (and often are) required.[5]

14. Adequacy itself is currently only a bilateral or sometimes only a unilateral mechanism. One country may recognize another as having essentially equivalent protections in place, or a bilateral decision of both jurisdictions recognizing each other may be issued.

15. Various workstreams and thought leaders are attempting to better enable global transfers and flow of data. At the same time, data flows have never before been more under threat of stopping, possibly globally. As an example, if regulators order a stop to data sharing to the US due to perceived and documented (in case law) threats to individual rights and freedoms, it seems global data flows would stop, full stop.

16. Viewed side by side, however, many, many jurisdictions (even within the EU) have similar issues as those issues raised in the "transfers to the US" discussion. The DIFC Ethical Data Management Risk Index (EDMRI) and supporting research demonstrates these similarities[6], yet other jurisdictions do not necessarily appear to receive the same level of scrutiny.

17. Meanwhile, the EU and the US, the main players in the data transfers “fray” are working hard to agree something that will fix the outstanding issues raised in Court of Justice of the European Union decisions C-362/14 and C-311/18, aka Schrems I and II.[7] The recent announcement of an Executive Order issued by President Biden to implement the European Union-US data privacy framework is the latest attempt to resolve outstanding issues around intelligence gathering and individual privacy protections and rights, however there are already preparations to potentially challenge it.[8]

18. As such, there are some possibilities to consider when looking for a solution to safe, yet practical, data export and import:

    a) Data protection laws, principles and transfer safeguards should aim to facilitate a proactive culture of privacy based on factors supporting education and behavioral change

[5] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
[6] https://www.difc.ae/business/operating/data-protection/data-export-and-sharing/#s6
[7] Schrems I and Schrems II
[8] https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law

b) Most companies and people managing them wish to comply and behave ethically

c) Data flows to the US, or the EU, or the UK, or anywhere else should not / cannot stop both in terms of international trade as well as the personal and business interests of data subjects themselves

d) Even if a given mechanism (adequacy, SCCs etc.) fails, data flows will not likely stop. For example, exporters instead may assess available options given the regulatory environment, which may include operating in breach until clear, alternative mechanisms are sorted

e) Due to factors such as confusion over guidance, differences in laws between jurisdictions, the cost of compliance, and the strong likelihood of enforcement action regardless of compliance efforts, many companies may already operate in breach or potential breach of data protection laws

Objectives and Outcomes

19. For complete information, please read Section 3, "Setting the framework for a multilateral agreement" of the concept paper (at hyperlink) that serves as the foundation of this project.

20. The proposed multi-lateral data sharing and enabling technology concept aims to find an inclusive, practical solution to safe, multi-lateral data sharing with otherwise "caveat emptor" jurisdictions, and that yields the following outcomes (and others, as development permits):

a) AI or similar business enabling technology principles suitable for the GCC region

b) Principles-based, data export / import enabling technology built into a data sharing compliance monitoring platform and founded on those principles (the **Platform**)

c) Ongoing research (automated, if possible) about compliance propensity in the most common jurisdictions to and from which data flows, to supplement and enhance the compliance evaluation criteria and resulting risk assessment in the EDMRI. The information fed into the platform would produce:

i. a regulators' dashboard of supervision, monitoring and enforcement actions; and

ii. a dashboard of current company compliance statistics of those involved in the pilot testing, ideally fed by compliance information provided by regulated financial services entities (the **Pilot Regulated Entities**). This database includes items

such as regulatory filings, assessments, notifications, publicly available information, etc.

Multilateral Data Sharing Consortium Agreement

d) Drafting and executing a multilateral data sharing (adequacy) agreement amongst participating international financial centers (the **Participating Jurisdictions**) to allow for efficient, comprehensive, responsible, explainable and reliable tech-driven due diligence and data sharing (the **Multi-lateral Data Sharing Consortium Agreement**).

The agreement must be based on a detailed mapping of core data protection requirements of each jurisdictions' data protection laws and regulations. Please see Figure 1 below:

Figure 1: Core data protection laws and regulations mapping

Figure 1 describes the assumption that many laws are fundamentally the same at their core. Where there are gaps between requirements in relevant laws and regulations, the Participating Jurisdictions must agree the terms and conditions (controls and safeguards)

that each Participating Jurisdiction must commit to implementing in order to fill them and maintain an agreed, "low risk" regulatory compliance status. If the information is not provided or circumstances change in the Participating Jurisdiction, then that status changes from low risk to "at risk" or "at high risk" (the **Participating Jurisdiction Status**).

Terms and Conditions for Pilot Regulated Entities

e) Draft standard Consortium participation terms and conditions (the **Consortium Terms**) and open the Platform to Pilot Regulated Entities, setting out compliance requirements to be shared and fed automatically via integration with Platform where possible, or manually if necessary, creating a low risk, at risk or high risk status (the **Pilot Entities Status**). Similarly, if the required information is not provided or circumstances change in the processing operations or environment of the Pilot Regulated Entity(ies), then the Pilot Status changes from low risk to "at risk" or "at high risk".

f) Together, Participating Jurisdictions and the Pilot Regulated Entities will collectively form the **Consortium Members** or **Consortium Membership**. The Participating Jurisdiction Status and the Pilot Entities Status, via the Multi-lateral Adequacy Consortium Agreement and via the Consortium Terms, respectively, comprise an overall adequacy status equilibrium indicated in a master dashboard of low risk, at risk or at high risk status (the **Multi-lateral Equilibrium Status**). Please see Figure 2 for an overview.

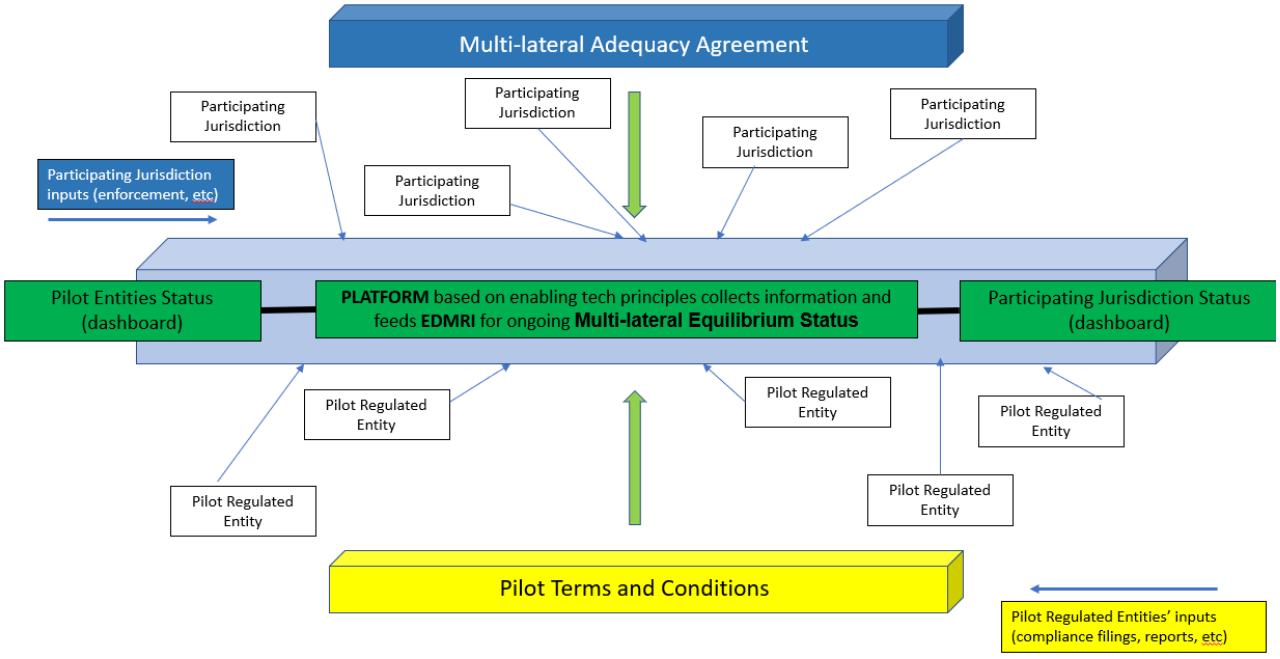

Figure 2: Configuration of Multi-lateral Adequacy Consortium

21. In short, this project seeks to prepare and test a low risk, multi-way adequacy agreement for financial services using principles-based technology to ensure all participating regulators are holding up their end of the bargain, and that the same goes for all participating financial services entities that contribute data to confirm on-going compliance with applicable laws and regulations.

22. The detailed, draft concept paper is available for further information at this link.

Q & A

The concepts set out above may have elicited a number of questions while reading through this consultation paper. The following section aims to resolve some of them. When you complete the response form, please feel free to add any additional questions and your thoughts.

Q1. What are the benefits to a Data Protection / Supervisory Authority acting as a Participating Jurisdiction and what are the risks?

Especially where international financial centers (IFC's) act in this capacity, given the usual size of these jurisdictions, this project serves to support better, more structured and consistent record keeping, enforcement, ability to share enforcement information in a constructive way, and build a more robust data protection regime, as a sort of neural network to more safely support data sharing between their jurisdictions.

The primary risks are where laws and policies change, or leadership decides on a new approach. If such changes result in the inability to remain in the Consortium, the knock on effect is similar to that of the collapse of certain data transfer mechanisms. Back up planning to ensure stability would be part of the Multilateral Adequacy Agreement so a transition out of the Consortium could happen with minimal impact on both the Supervisory Authority and the entities exporting / importing data under this arrangement.

Q2. What about onward transfers from Pilot Entities to other entities in non-Participating Jurisdictions? What safeguards would apply?

Data export and import is never a unilateral or bilateral effort. There are of course transfers occurring in all directions, 360 degrees, 24 hours a day, 7 days a week. Inevitably there will be transfers outside of the Participating Jurisdictions Consortium environment. For such situations, the same safeguards and lawful basis assessments and implementation would have to be in place. In reality, however, this isn't any different than the majority of other jurisdictions outside of the usual adequacy recognition environment. There are a total of 41 countries in the world with adequacy decisions in place. That leaves over 100 other countries that do not have this status, and that will have to operate accordingly in terms of applying safeguards. The situation resulting from this project regarding onward transfers would be no different.

Q3. What is the likelihood this concept would be accepted as a legitimate transfer platform?

That remains to be seen. If it works, and provides a clear outcome of reliable, objective adequacy status maintenance based on both legal regimes and real-time compliance (which, in all practicality, is the important part), then there should be little reason to not accept it.

Q4. Doesn't this concept only serve to increase the compliance burden on Pilot Entities?

Shouldn't it? Compliance requirements exist, regardless of this project. Many organisations assert that they "comply with XYZ data protection laws" or have assessments done to prove their organization is trustworthy. Presumably, this is true. If they are already compliant, then there should be no additional burden as it is simply a matter of an automated process to pull compliance confirmations, statistics and reporting (where required) into a central database to maintain the dashboard status. It is where organisations say they are compliant but could probably stand to sure up their documentation, policies, record keeping, etc., where this could be burdensome. These organisations do not have to participate. Indeed, the reason to start in IFCs with Pilot Regulated Entities is because they are presumably more prepared to comply or simply are compliant (and more reliable regarding safe processing), such that they can feed this information easily into the status platform.

Q5. Are there legal barriers to adequacy between non-sovereign countries, in other words, "International Organisations"?

Possibly, yes. Certain countries' laws or policies set out limitations about the type of organization that can be recognised for adequacy or simply do not have adequacy recognition as an option in their laws or policies. They would not be able to participate, unfortunately, at least not without a change to the laws or policies that limit participation.

Q6. Does this project concept anticipate legal challenges or judicial review?

Yes. That may simply be unavoidable and quite likely.

Q7. How is this different from systems like Cross Border Privacy Rules (CBPR?

This concept advances the idea that AI / enabling technology principles complement or may be the next generation of privacy principles. It is also based on the concept of an automated platform to maintina adequacy recognition status that holds both regulators and participating companies accountable, while CBPR is a certification system (albeit with similar drivers). Finally, participation in this consortium could support ongoing certification requirements for CBPR participating companies.

The Commissioner's Office thanks you for your time and attention.

DIFC

Consultation Questions on the Proposed Enabling Technology Principles and Multi-Lateral Data Sharing Platform

Q1. Which of the following existing set of principles or guidelines seem most appropriate for the enabling technology driven businesses in the DIFC? If you choose more than one, we will assume you mean that a combination of principles or guidelines would be useful. Please clarify, if necessary.

- ☐ **DUBAI DIGITAL AUTHORITY**
- ☐ **OECD**
- ☐ **UNESCO**
- ☐ **CBUAE, SCA, DFSA and FSRA GUIDELINES FOR FINANCIAL INSTITUTIONS**
- ☐ **MONETARY AUTHORITY OF SINGAPORE FEAT**
- ☐ Other

Q2. Based on Q1, is it necessary to create and adopt any further GCC focused, general principles or guidelines for enabling technology such as AI? If so, please consider clarifying why using the free test box.

Proposed principles are set out in **Appendix 2** for your consideration.

Q3. What additional controls do you suggest to help reduce the risk of bias (political, environmental, social, etc.) in building the Platform?

- ☐ Peer review of the Platform / Human in the loop
- ☐ Fully automated, non-learning inputs of certain information to create balance
- ☐ Feeds from independent databases
- ☐ Combination of the above
- ☐ Other

Q4. What additional compliance or regulatory input criteria do you suggest is evaluated in the EDMRI to enhance and better safeguard any Consortium members' undertakings as part of the Multi-lateral Adequacy Consortium Agreement or Consortium Terms?

Appendix 1 sets out the current EDMRI criteria and methodology. A test version of the EDMRI research tool is available here. A separate feedback link is available here if you wish to provide comments about this tool only.

- ☐ Use of enabling technology / existence of principles or regulations in the jurisdiction
- ☐ Case law / changes in case law regarding national security and bulk intelligence gathering / intelligence practices / Frequency of changes to case law or regulations
- ☐ Other

Q5a. As set out in the discussion around Figure 1 above, under the model proposed in this consultation paper, would mapping and agreeing key synergies amongst data protection laws to the degree that only minimal gaps may be identified provide confidence in data flows with trust?

Q5b. If so, would proportionate undertakings to fill those gaps, such as those set out in recent EU Commission adequacy decisions, become the basis for a multi-lateral data sharing agreement amongst jurisdictions?

Q6. What are the risks associated with the approach set out in Q5 and what are the benefits? Please select an option and clarify your response in the text box.

- ☐ It is too broad an assumption that many DP Law and Regulations are similar
- ☐ Independent and binding redress will always be a concern in most jurisdictions, regardless of the existing of DP Laws and Regulations or similar obligations set out in other laws
- ☐ It is likely that many DP Laws and Regulations are quite similar and this exercise presents minimal risk, but it may be difficult to convince other jurisdictions to agree to such undertakings
- ☐ It is likely that many DP Laws and Regulations are quite similar and this exercise presents minimal risk, and for the sake of safer yet quicker, reliable data flows, other jurisdictions will be amenable to such undertakings
- ☐ Other

Q7. Hypothetical: If one of the Participating Jurisdictions fails to contribute information that supports its Multi-lateral Adequacy Consortium Agreement undertakings / low risk Participating Jurisdictions Status and moves from low risk to at risk or at high risk, which recommendation would you consider best to ensure exports to that jurisdiction remain safeguarded until the status can be returned to low risk? Please select all relevant answers and if needed, please explain your answer.

- ☐ Give the Participating Jurisdiction 14 days to clarify the issue to Consortium Members, and where possible, 90 days to cure with a further 90 day extension if reviewed and approved by all Consortium Members
- ☐ Require Pilot Regulated Entities to perform basic due diligence and contract review of engagements with importers in the changed-status jurisdiction and implement temporary or permanent safeguards, such as maintaining originally agreed data processing contractual requirements, to the extent permissible by law.
- ☐ Introduce undertaking levels, such as EDMRI low risk / no undertakings required, EDMRI medium risk / minimal undertakings required, EDMRI high risk / all agreed undertakings required, and allow the Consortium Members to evaluate based on circumstances.
- ☐ All of the above – these measures should sufficiently resolve most instances
- ☐ None of the above – there may be too much risk to data in the importing, changed-risk jurisdiction involved
- ☐ Other (please explain)

Q8. With the same considerations above in mind, where a Participating Jurisdiction Status cannot return to low risk because of a relatively permanent change or unforeseen factor, what options for remaining in the Consortium Membership should be considered and applied? Please select all options you think apply, or please explain your answer.

- ☐ If cure is not possible within 30 days, suspend the Participating Jurisdiction from the Consortium for 180 days and review again at that time.
- ☐ Expel the Participating Jurisdiction indefinitely
- ☐ None of the above – there may be too much risk to data in the importing, changed-risk jurisdiction involved
- ☐ Other (please explain)

Q9. Under what circumstances should a Pilot Regulated Entity be suspended or expelled from Consortium Membership?

- ☐ The Participating Jurisdiction fails to contribute regulatory information more than 2 quarters in a row
- ☐ The Participating Jurisdiction contributes inaccurate information subject to review of the Consortium Members more than 4 quarters in a row
- ☐ Another Participating Jurisdiction requests a review of the Consortium Members to suspend or expel, subject to review protocols
- ☐ Other (please explain below)

Q10. How accurate do you think the following position statements are: (optional)

a) Data protection laws, principles and transfer safeguards should aim to facilitate a proactive culture of privacy based on factors supporting education and behavioral change.

Very accurate **Accurate** **Somewhat accurate** **Not accurate**

b) Most companies and people managing them wish to comply and behave ethically.

Very accurate **Accurate** **Somewhat accurate** **Not accurate**

c) Data flows to the US, or the EU, or the UK, or anywhere else should not / cannot stop both in terms of international trade as well as the personal and business interests of data subjects themselves.

Very accurate **Accurate** **Somewhat accurate** **Not accurate**

d) Even if a given mechanism (adequacy, SCCs etc.) fails, data flows *will not* likely stop. For example, exporters instead may assess available options given the regulatory environment, which may include operating in breach until clear, alternative mechanisms are sorted.

Very accurate **Accurate** **Somewhat accurate** **Not accurate**

e) Due to factors such as confusion over guidance, differences in laws between jurisdictions, the cost of compliance, and the strong likelihood of enforcement action regardless of compliance efforts, many companies may *already* operate in breach or potential breach of data protection laws.

Very accurate **Accurate** **Somewhat accurate** **Not accurate**

You may explain your selected responses if needed. **All responses will remain confidential and will not be considered as indicative of your business's compliance program**. This question will help the Commissioner's Office to gauge general thoughts about compliance best practices and burdens.

Appendix 1 – EDMRI Methodology

Assessment Criteria	**Risk Weighting Rationale**
DP Law in the jurisdiction	Existence of a DP Law is a mitigating factor, ensuring lower risk when processing Personal Data in a jurisdiction, but ***it does not guarantee either effectiveness or enforcement***. It also is ***not determinative that businesses will implement the law when processing Personal Data due to a variety of factors****, including awareness*. Further considerations: What will better secure effectiveness or enforcement by a regulator, and what will encourage businesses in the jurisdiction to implement the DP law at all?
TI rating from DIFC AML Country List (to be provided as needed)	For the purposes of data sharing when required by other regulators, such as for financial crime prevention, the likelihood of government access to shared Personal Data in a high financial crime risk importing jurisdiction is higher and therefore creates greater risk due partly to the volume of Personal Data that must be exported. It also raises the risk that redress options for data subjects in the exporting jurisdiction will be minimal. Finally, higher occurrence of corruption in a jurisdiction potentially indicates that businesses may be less compliant with laws generally and / or less accountable or transparent generally.
Cyber security laws / policies?	Laws or policies regulating ***cyber security and advanced IT risks***, when implemented and enforced, ***reduce risk to Personal Data processing in the importing organisation***. Further considerations: Even with cyber security measures in place, why are there still breaches or mishandling of Personal Data and what can be done to better prevent them? Some suggestions include better education about common mistakes and human error; practical guidance from regulators / more willingness to give direct, "instructional" guidance; fool-proofing through privacy engineering or mandates around security baselining hardware / cloud tools in terms of access, portability, etc.
Non-privacy laws with DP Elements (HR, Consumer protection, Health data)	Laws other than a national privacy law may exist in a jurisdiction that provide as much if not more protection of Personal Data imported into it. Jurisdictions with laws regulating processing of medical insurance information, criminal records, children's' privacy online, and consumer privacy may be considered as lower risk despite the lack of a national privacy law.

Assessment Criteria	**Risk Weighting Rationale**
E-Privacy / direct marketing and digital footprint / tracking laws?	Laws or policies regulating marketing and tracking IT use / online presence, when implemented and enforced, reduce risk to Personal Data processing in the importing organisation.
Adequacy recognition from another jurisdiction	If another authoritative regulator has assessed the jurisdiction, ***it's likely, although not determinative, that processing operations*** by organisations in the importing jurisdiction ***will be properly undertaken***. The risk is in any case likely to be lower in such jurisdictions. Further considerations: While the EU has traditionally been the only issuer of adequacy decisions, Brexit has shown us that many DP laws supporting the regulator making adequacy decisions exist, and that the option should be exercised. This may lead to adequacy "cross-pollination". How does that impact the EU / UK approach and compliance requirements, and what is the knock on effect of coordinating the various recognitions that may result?
Independent regulator managing any **privacy** related aspects, enforcement	Oversight by a regulator with the power to independently enforce the law significantly reduces the risk of privacy breaches.
Independent regulator managing any **security** related aspects, enforcement	Oversight by a regulator with the power to independently enforce the law significantly reduces the risk of cybersecurity incidents.
Notification or registration (or licensing) requirements for entities?	***Notification*** to an independent regulator with the power to inspect / investigate for compliance with the law ***significantly reduces the risk of privacy breaches***. Further considerations: What other information, analytics or benefits could be gleaned from an entity's notification to the supervisory authority / regulator? Would it, for example, satisfy a privacy notice requirement if a small / any company linked to its notification with a lead authority? Does this help reduce the compliance burden?
Accountability requirements? DPO, privacy policy, etc.	Appointing a DPO and requiring privacy policies, compliance programs, etc., creates awareness within the processing organisation and ensures a better, more consistent overall application of the law, or indeed, *any* application of the law within a business / jurisdiction. Thus, a culture of privacy is more likely to exist, and risk is reduced. Further considerations: Should DPO appointment be mandatory full stop?

Assessment Criteria	Risk Weighting Rationale
Access to guidance / information?	Guidance and outreach provided by an independent regulator to ***help raise awareness and ensure compliance*** with the law significantly reduces the risk of privacy breaches and general non-compliance. Further considerations: Would a list of *what not to expect* from a regulator be helpful?
Requirement to report data breaches to regulator?	Transparency with the regulator in a jurisdiction and an understanding of what causes data breaches is necessary for reducing risk.
Requirement to report data breaches to individual / data subjects?	Transparency with and accountability to individuals in a jurisdiction and an understanding of what causes data breaches is necessary for reducing risk.
Cultural respect for privacy?	If the jurisdiction has a basic, ***ethical foundation of privacy and respect for human rights to privacy,*** to the extent it can be ascertained, the risk is reduced. Further considerations: How can this be quantified?
Enhanced limitations on processing Special Category data?	Particularly sensitive data that may create or exasperate the vulnerability of an individual likewise creates risk for that individual when his or her data is processed without knowledge or express permission, where required. Enhanced limitations and controls existing in the local privacy or other similar laws supports a reduced risk assessment. Further considerations: Is it still relevant to maintain a separate definition of "Special Category" or sensitive data? Should there be no distinction such that all Personal Data be upgraded and considered the same? Does this distinction complicate things or does it in fact help to better protect Personal Data?
Prohibitions on specific types of data processing?	See above
Right to privacy principles in other laws	Where the right to privacy exists in a foundational legal tenant or instrument, such as constitution or founding laws, the importing jurisdiction is more likely to process data in an ethical way and the risk may be less.

Assessment Criteria	Risk Weighting Rationale
Judicial system / redress available for privacy violations	Where access to ***judicial redress is available in the importing jurisdiction***, it is more ***likely that individual rights will be protected*** where Personal Data has been processed unlawfully.
Access by law enforcement	If ***law enforcement has unlimited, uncontrolled access*** to Personal Data for any purpose or without providing sufficient detail and support for requesting Personal Data, the risk is increased.
Access by government departments, agencies or international organisations	If government entities have unlimited, uncontrolled access to Personal Data for any purpose or without providing sufficient detail and support for requesting Personal Data, the risk is increased.
Extra-territorial reach of any DP related laws?	Where privacy or similar laws of the exporting jurisdiction have ***sufficient, legally enforceable reach*** to protect Personal Data to the extent it is implemented by the importing entity, the risk of privacy lapses is reduced. Further considerations: What would a "global" privacy law look like? More importantly, is it even practical to think one could be developed? If so, how?
Individual privacy rights (access, erasure, etc.)	Transparency with and accountability to individuals in a jurisdiction by providing more control over how Personal Data is processed is necessary for reducing risk.
Unusual limitations on individual privacy rights?	Transparency with and accountability to individuals in a jurisdiction by providing more control over how Personal Data is processed is necessary for reducing risk.
Industry specific codes of conduct or certification scheme?	Where a secondary, non-privacy regulator also ***requires accountability through a code of conduct, or certification scheme*** is implemented by a privacy regulator, risk is reduced. Further considerations: Should these be further developed as a better form of transfer mechanism?

Assessment Criteria	Risk Weighting Rationale
Surveillance and investigatory powers balanced with necessity and proportionality	***Unsubstantiated, uncontrolled surveillance and the lack of access to judicial redress associated with inappropriate invasion of privacy rights*** through such surveillance increases risk of privacy violations and contravention of data protection laws and principles. Further considerations: What are the realistic, practical pros and cons of surveillance and investigatory powers? Will future generations be as concerned about it, living their lives online already? What's next?

DIFC

Appendix 2 – Draft Enabling Technology Principles

Upon analysis of several well-curated, robust principles supporting the unbiased, responsible promulgation of AI and other enabling technologies, for the purposes of this (and potentially other) use cases, the follow locally-developed principles may be proposed and subsequently considered and / or adopted by any participating jurisdiction, authority or other government entity that deems them reasonable and appropriate. As a result of this consultation, the concepts below are subject to change.

Fair

Systems that are developed with well-being as an equal consideration to a system's intended function. This is achieved by ensuring outcomes empower human beings, and do not infringe on fundamental rights.

Ethical

Algorithmic decisions and associated data lineage should be able to be unbiased. This principle is closely linked with the principle of transparency.

Transparent

Systems must ensure processing of people's Personal Data is explainable to end-users and other stakeholders in non-technical terms, with appropriate supporting evidence.

Secure

Systems must keep Personal Data protected and kept confidential and prevent data breaches which could cause reputational, psychological, financial, professional or other types of harm.

Accountability

Mechanisms are in place to ensure responsibility and accountability for enabling systems and their outcomes. Such mechanisms may include internal governance and control frameworks in place for monitoring our systems, processes and projects regularly or external organisation auditing our processes regularly, enabling the assessment of algorithms, data and design processes.