DIFC

Data Export & Sharing Handbook

Commissioner of Data Protection

CONTENTS

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

1. Introduction

Part 4 of the Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law 2020") and Section 5 of the Data Protection Regulations 2020 (the "Regulations") cover the topic of Data Export and Sharing, which involves transfers of Personal Data outside of the DIFC. DIFC's Data Export and Sharing Handbook (the "DES Handbook") will address the circumstances and methods for safe, controlled data sharing.

Personal Data is defined in the DP Law 2020 as, "Any Data referring to an Identifiable Natural Person" and Special Category Data is defined as, "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person." Such data includes but is not limited to name, address, business or personal email address, business or personal phone numbers, geolocations, job title or other employee data, health and biometric data, religious affiliations, or criminal history.

Personal Data generally can be any information that when viewed together (or in some cases is so unique) it clearly identifies a living individual. It could be data about clients, employees, suppliers, or family members, to name a few categories of Personal Data. Many if not all organisations process Personal Data as a result, and will in many cases have to transfer such data outside the DIFC at some point in a transaction. Even the UAE, because it is separate from the DIFC as a legal jurisdiction, must be currently viewed as a Third Country under the DP Law 2020 to which data export considerations and safeguards apply.

The defined terms used herein have the same meaning as the defined terms in the DP Law.

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

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

2. Scope

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

*Please note that **this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice**. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

3. Checklist for Data Export to a non-DIFC jurisdiction:

Before making any transfers of Personal Data outside the DIFC, please consider the following checklist (each section described in detail below):

Q1. Is a transfer of Personal Data[1] outside of the DIFC being made?

If no, you can make the transfer. If yes go to Q2

Q2. Has the DIFC recognised the country or territory where the recipient is located as having an adequate data protection law or regime in place, in accordance with Article 26(1)(a)?

If yes, you can make the transfer, but may wish to work through the process below / apply additional safeguards / review the EDMRI (defined below, and detailed in Part 4, Q3D). If no go to Q3

Q3. Is one of the appropriate safeguards referred to in the DP Law 2020 in place, in accordance with Article 27(2)?

If yes, you can make the transfer. If no go to Q4

Q4. Do any of the derogations listed in Article 27(3) apply?

If yes, you can make the transfer. If no go to Q5

Q5. Does one of the limited circumstances provided for in Article 27(4) the DP Law 2020 apply?

If yes, you can make the transfer. If no you cannot make the transfer in accordance with the DP Law 2020

Q6. Have you considered the obligations under Article 28 regarding sharing Personal Data with government authorities, specifically documenting either a) a bilateral risk assessment through a form of "written assurances" under Article 28(1)(a to c) or b) a unilateral risk assessment under Article 28(2)?

To better understand your data sharing activities and what you need to do to comply with the DP Law 2020, you may, among other options, read through this DES Handbook, review the DP Law 2020 and Regulations, or run this Data Export assessment tool and the Article 28 assessment tool to do a quick knowledge check, to set you on the right course.

[1] A transfer of Personal Data may be sending an email with contact or other identifiable information in it, either in the body or as an attachment; sharing employee payroll or health information with a services provider; or anything else that meets the definition of Processing in Schedule 1, Article 3 of the DP Law 2020.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

4. Data Export and Sharing in Detail:

Q1) Is a transfer of Personal Data outside of the DIFC being made?

The DP Law 2020 refers to jurisdictions outside of the DIFC as Third Countries or International Organisations. Please note that the UAE is considered a Third Country as well.

Under Article 26(1) of DP Law 2020:

Processing of Personal Data that involves the transfer of Personal Data from the DIFC to a Third Country or to an International Organisation may take place only if:

(a) an **adequate level** of protection for that Personal Data is ensured by Applicable Law, as set out in Articles 26(2) and (3), including with respect to onward transfers of Personal Data; or

(b) it takes place **in accordance with Article 27**.

Where the conditions above have not been met, then any other transfers are "restricted", in that they cannot take place. If they do, it will violate DP Law 2020. In other words, you are making a "restricted transfer" if:

- the DP Law 2020 applies to your processing of the Personal Data you are transferring. In general, the DP Law 2020 applies if you are processing Personal Data in the DIFC, and may apply in specific circumstances if you are outside the DIFC and processing DIFC-related Personal Data. The DIFC DP Commissioner's Office has produced an applicability assessment tool to understand whether DP Law 2020 applies to the processing in question;
- you are sending Personal Data, or making it accessible, to a recipient in a jurisdiction with no substantive data protection law, privacy regime or privacy culture, as determined by Commissioner's guidance such as the DIFC Ethical Data Management Index[2] (the **Index or EDMRI**), and no additional safeguards are in place per Article 27; ***and***
- the recipient is a separate organisation or individual. This includes transfers to another company within the same corporate group.

NOTE: If you are sending Personal Data to someone employed by you or by your company, this is not by default a "restricted" transfer. Best practice, however, is to ensure that if you share Personal Data within your organisation but to a recipient based outside of the DIFC, then an intra-company agreement(s) incorporating **standard contractual data protection clauses** (details below, point 3C) attached or other available mechanisms assuring how Personal Data is processed once it arrives there should be engaged.

Generally, transfers within the DIFC are out of scope for this guidance because they are permitted provided they comply generally with the DPL. However, please account for other considerations, for example the proviso set out under question 2 below, and also whether there will be any onward

[2] The Index is the intellectual property of DIFC Authority.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

transfers from the third-party entity with which you shared the Personal Data that may be considered restricted.

"Transfer" and "transit" are different terms and have different consequences. Transit, means that data is in route to the recipient, typically on a computer network.

Uploading Personal Data on to a website, for example, will often be considered a restricted transfer under DP Law 2020 because someone outside the DIFC may accesses that Personal Data via the website. Or, if you load Personal Data onto a DIFC-based server that is then available through a website, and you plan or anticipate that the website may be accessed from outside the DIFC, you should treat this as a restricted transfer and apply the appropriate safeguards, where necessary.

Q2) Has the DIFC recognised the country or territory where the recipient is located as having an adequate data protection law or regime in place, in accordance with Article 26(1)(a)?

Adequacy recognition is a finding by the Commissioner set out in the Data Protection Regulations that the Third Country or International Organisation's legal framework in place provides similar or equivalent protections and controls for individuals' rights regarding their Personal Data.

If the restricted transfer is covered by an adequacy decision, generally, you may go ahead with the restricted transfer. The list of adequate jurisdictions currently recognised are available on the Data Export and Sharing page on the DIFC website.

The process and methodology for making an adequacy decision is based on:

- Risk assessment of a Third Country or International Organisation outcome from the EDMRI;
- Comparative factors based on common data protection principles set out in DP Law 2020 and potentially in the Third Country or International Organisation legislation;
- Undertakings regarding government data sharing practices and applying data protection principles, in accordance with Article 28 of the DP Law 2020;
- Any supplemental conditions necessary to ensure on-going application and enforcement of the relevant framework under assessment, as approved and set out in the Regulations, and / or updated on the Data Export and Sharing page from time to time; and
- A commitment to an on-going relationship with the Commissioner's Office, including regular communications and meetings with the supervisory authority of the applicant jurisdiction

Of course, you must still comply with the rest of the DP Law 2020, regardless of such decision.

Practical application: Adequacy is a powerful tool for companies to rely on, as it somewhat eases the need for compliance and administrative work to support controlled transfers of Personal Data. However, even though a jurisdiction has a data protection law that is considered adequate, the company (controller or processor) in another country or jurisdiction (*any* country or jurisdiction) that your DIFC entity is engaged with may not appropriately apply or internally implement those obligations, even if another authority has recognised its jurisdiction for adequacy purposes.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Adequacy is only one possible transfer safeguard recognised under Part 4 of the DP Law 2020. A DIFC (or any) entity has every right to insist on additional safeguards if it so wishes in accordance with the guidance provided in the Commissioner's Ethical Data Management Risk Index or based on its own risk assessment and analysis, and <u>regardless</u> of whether the Third Country or International Organisation is deemed adequate (by any supervisory authority!).

Additional safeguards and controls you can opt to employ include additional, robust privacy enhancing technology, an "adequacy" assessment of the importing entity, use of contractually agreed audits and policy reviews, conducting joint training sessions, requiring annual risk assessments or data protection impact assessments to be completed (and providing documented evidence thereof), or enforcing voluntary notification to the DIFC Commissioner's Office in order to work with your business.

Please see DIFC Data Export and Sharing webpage for the more on adequacy assessment templates and other supplementary materials, which may be updated and re-posted from time to time. If any materials are momentarily unavailable, please check back or email commissioner@dp.difc.ae to obtain them.

Q3) Is one of the appropriate safeguards referred to in the DP Law 2020 in place, in accordance with Article 27(2)?

If the Regulations and / or the current list of adequate jurisdictions set out on the Data Export and Sharing page do not specify that the Third Country or International Organisation is adequate (or even if it does), you should then find out whether you can make the transfer subject to 'appropriate safeguards', which are listed in the DP Law 2020 in Article 27(2). Supplemental safeguards may be found on the Data Export and Sharing page and will be updated from time to time based on further risk index assessments, described in further detail below.

These and any other relevant "appropriate safeguards" ensure that both you and the recipient of the transfer are legally required to protect individuals' rights and freedoms for their Personal Data, the same and in substantially the same way it would be protected in the DIFC.

If is the transfer is will be covered by an appropriate safeguard, you may go ahead with the restricted transfer. Of course, you must still comply with the rest of the DP Law 2020.

The primary, commonly used appropriate safeguards are set out below:

A. Legally binding instrument between public authorities

You can make a restricted transfer using a legal instrument between public authorities provided that the legal instrument provides 'appropriate safeguards' for the rights of the individuals whose Personal Data is being transferred and it is legally binding and enforceable. The 'appropriate safeguards' must include enforceable rights and effective remedies for the individuals whose Personal Data is transferred.

<u>Practical application:</u> This safeguard is used less frequently than others and should be supported by review of the Commissioner to ensure it covers all necessary elements of the DP Law 2020. It would be more efficient to apply DIFC standard contractual (data protection) clauses (DIFC SCCs).

from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

B. Binding corporate rules

You can make a restricted transfer if both you and the recipient have signed up to a group privacy policy regime called binding corporate rules (BCRs).

To date, BCRs are normally an EU-based safeguard mechanism. BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of Personal Data from the group's EEA entities to non-EEA group entities.

This may be a corporate group, or a group of undertakings or enterprises engaged in a joint economic activity, such as franchises or joint ventures. Very often, additional contractual requirements are necessary to conduct compliant transfers to non-group entities, such as clients or suppliers, and in the case of DIFC transfers, even to government authorities based on Article 28.

You must submit EU-supervisory authority approved BCRs for review and approval by the Commissioner before the transfer goes ahead on this basis, or you may request review and approval by the Commissioner's Office for DIFC-approved and originating BCRs.

Practical application: Again, this safeguard is used less frequently than others, and must be supported by review and approval of the BCRs by the Commissioner to ensure it covers all necessary elements of the DP Law 2020. Unless your entity as a group has BCRs that have been approved already, it is often more efficient to apply the DIFC SCCs. That said, the Commissioner's Office is available to review and approve your company's proposed EU-approved BCRs. You may also wish to engage in consultation with the Commissioner's Office as permitted by Article 21, in order to discuss intra-company framework agreements in place that incorporate relevant safeguards that act similarly to BCRs or are "placeholder" agreements until BCRs are approved. BCR requirements are set out in Appendix 1.

C. DIFC SCCs adopted by the Commissioner and set out in the Regulations

You can make a restricted transfer if you and the importing recipient have entered into a contract incorporating standard data protection clauses adopted by the Commissioner, per the then-current DIFC Data Protection Regulations. They normally must be entered into by both the data exporter (based in the DIFC) and the data importer (outside the DIFC).

The DIFC SCCs contain contractual obligations of the data exporter and the data importer, and address the rights for the individuals whose Personal Data is processed via transfer. Individuals can directly enforce those rights against the data importer(s) *or* the data exporter through available redress options, including initiating a claim in the DIFC Courts.

The DIFC SCCs have been revised recently and are available for download on the Data Export and Sharing page. For ease of compliance, they are based on current best practice in principal jurisdictions with existing clauses that may be used by a parent or affiliated entity based elsewhere, i.e., in the EU, UK, etc.

The latest DIFC SCCs combine the safeguard requirements of these jurisdictions into one document, rather than two separate documents for controllers and processors that were previously approved for use. Taking the EU model clauses updated in 2021 as an example, the "Obligations of the Parties" section sets out four (4) modules (the "Modules") to be applied as appropriate. ***The DIFC SCCs do not have multiple modules***.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

This is because on comparison of the Modules[3], the similarities and requirements could be synthesized into common "strictest standard" responsibilities, emanating from the data protection principles set out in the DP Law 2020, without sacrificing content or substance.

Ultimately, the Modules boil down to two types of transfers from any type of exporting entity in the DIFC to any type of data importers – whether controllers or to processors - outside of the DIFC.

Whether the transfer initiates from DIFC controllers versus processors is less relevant from the Commissioner's view because it is where the data resides – and the compliance implementation of the importing entity after the transfer(s) – that should be the focus. Understanding whether the privacy culture, regime, and propensity for compliance of companies there may require extra care and diligence to ensure the processing in the data's new "home" is undertaken as though the DP Law 2020 applies.

The relevance of the type of data exporters comes into play regarding the type of provenance and instructions that are given to the data importer. Effectively, the Commissioner's Office takes the view that the DP Law 2020 applies largely the same way to both Controllers and Processors, apart from a few minor differences in accountability for processing. So should it apply to those entities outside the DIFC, regardless of other contractual obligations or instructions.

In other words, the DP Law 2020 is the hub and the DIFC SCCs are one of the spokes that carry the obligations through to the importing jurisdiction. The DIFC SCCs compliment and support the DP Law 2020, and ensure that *all* relevant articles are accounted for, creating a compliance obligation in the importing jurisdiction[4].

The revised DIFC SCCs take all of this into account, and where specific situations must be addressed due to the onus of accountability for processing, such as where data subjects make a request to a Controller for access to information about how their Personal Data is processed, or where a Sub-processor is engaged by a Processor, clear requirements choices are set out and the appropriate contractual outcome will be interpreted accordingly. Where a particular clause is not applicable, the entities will not be held to account. This approach also allows for flexibility, so that if the roles of any Parties to the DIFC SCCs change or updates are made to the processing activities, the obligations are already captured and only the relevant Appendices will need to be updated.

In applying the DIFC SCCs, be aware that basic or enhanced due diligence to ensure compliance with them and the DP Law 2020 may be recommended or required[5], depending on the risk level applied to a jurisdiction vis a vis the Ethical Data Management Risk Index. Enhanced due diligence may include imposing additional relevant contractual, technical or organisational safeguards put in place to supplement the safeguards. The Commissioner may provide a list of such enhanced due diligence requirements via Regulations and / or on the Data Export and Sharing page of the DIFC website. Please always check this page for any updates. The EDMRI is available on this page as well. The methodology for the EDMRI is set out in Appendix 2 of this handbook, and is reflected in the importing country compliance narratives behind each hyperlink on the Index.

If you are entering into a new contract, you must use the approved standard contractual clauses **without amendment wherever possible**. You can include additional clauses on business related issues, provided that they do not contradict or invalidate the standard contractual clauses. You can

[3] Available at this link

[4] This aligns with Article 6(3)(b) applicability as well.

[5] Not necessarily mandatory requirement imposed by the Commissioner's Office for full compliance, but as a policy requirement within your company's compliance program.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

also add parties (i.e. additional data importers or exporters) provided they are also bound by the standard contractual clauses.

Practical application: The objective is to streamline use of the DIFC SCCs, while remaining compliant not only with DP Law 2020 but other potentially applicable laws such as the EU General Data Protection Regulations (the "GDPR") or the UK Data Protection Act 2018 / UK GDPR.

With certain transfer mechanisms recently invalidated, and others such as BCRs used on a limited basis, the use of (DIFC) SCCs is the most common way of ensuring appropriate safeguards are applied to an otherwise restricted transfer[6].

There are currently various possible contractual clause options, including the EU Model Clauses[7], the UK International Data Transfer Agreement (UK IDTA)[8] and the DIFC SCCs. All of them contain substantially the same safeguards and require additional risk or other assessments of any additional necessary actions to assure the safety of the transfer.

If you are already required to use another set of substantially similar clauses, you may do so in place of or in addition to the DIFC SCCs. Please, however, ensure that you make it very clear in the description of the transfer or as appropriate in the contract documentation that data will be shared from or to the DIFC jurisdiction as well, and that for the purposes of such transfer, the other jurisdiction's clauses apply but that the DP Law 2020 and Commissioner may also have jurisdiction.

As mentioned, understanding the risks in an importing recipient jurisdiction and *within the importing recipient's processing operations* is critical to truly understanding the overall privacy culture and ultimately how Personal Data will (or will not) be ethically managed there. Certain elements of a jurisdiction may reinforce privacy principles, while others leave Personal Data vulnerable to loss or misuse. The Index and methodology (see Appendix 2) provides an explanation about the types of risks to Personal Data in jurisdictions outside of the DIFC and mitigation options. Any additional risk mitigation requirements, or technical and organisational measures should be included in the descriptions set out in the relevant appendices to the DIFC SCCs (or any similar Third Country's template that may be used).

D. The EDMRI and EDMRI+

In order to properly apply any of the above safeguards for international transfers and to generally comply with DP Law 2020, or most data protection laws globally, a Controller or Processor should undertake risk assessments. Doing so will help to truly understand the business and privacy culture of the organisations involved in any data sharing arrangements. Risk assessments for international transfers should not be based only on the DP law in a jurisdiction, but ideally should also aim to understand the environment to which you are sending Personal Data, so that it is treated with as much care and safety as at home.

To this end, the EDMRI and methodology was created by the DIFC Commissioner's Office to assess the compliance risk of an importing business or entity in a jurisdiction complying or not with contractual, legal, technical, and organisational obligations when receiving Personal Data from a DIFC entity. EDMRI looks holistically at many common factors that all privacy pros have examined,

[6] A transfer of Personal Data may be electronically accessing DIFC information from a non-DIFC jurisdiction; sending an email with contact or other identifiable information in it, either in the body or as an attachment; sharing employee payroll or health information with a services provider; or anything else that meets the definition of Processing in Schedule 1, Article 3 of the DP Law 2020.

[7] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en

[8] The consultation draft is referenced herein. Please check www.ico.org for current draft.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

but then provides an objective analysis of the likelihood and impact of any potential risk indicators, thematically and individually. Among these indicators are compliance or potential for compliance with the applicable data protection law (if there is one) but also including all those other elements that perhaps make up for lack of a data protection law or regime. The research for the risk index is available as well by clicking on the country hyperlinks, giving further insight by theme and correlated to the overall risk assessment methodology.

Once you have reviewed the importing jurisdiction(s) on the EDMRI, where you have any doubt, you can do your own enhanced due diligence assessment not of the country but of the importing organisaion by completing the EDMRI+ Due Diligence Risk Assessment, (EDMRI+). This supplemental tool helps you to document the compliance preparedness of the importing entity you are about to share data with, and associated risks. This is important because even with adequacy or other transfer control mechanisms in place for your data sharing activities, you should seek to understand whether the businesses your company engages with are fostering privacy in its own organisation.

If your business exports (or transfers) personal data to another processor or controller in a high risk or very high-risk jurisdiction, the Commissioner's Office urges you to complete the EDMRI+ Due Diligence Risk Assessment, but at this time it is not mandatory. Please refer to the EDMRI Guidance to view the risk rating and explanations for each country evaluated so far, as published by the Commissioner's Office.

Final tip: always document and re-review compliance controls that are in place, and always leave room to question when and how to apply extra measures to safeguard data, regardless of what accepted norms may be.

Q4) Do any of the derogations listed in Article 27(3) apply?

Derogations are circumstances that allow for the restricted transfer to take place. If it is covered by a derogation, you may go ahead with the restricted transfer. Of course, you must still comply with the rest of the DP Law 2020.

Article 27(2) lists the appropriate safeguards that may be applied to restricted transfers. The primary, commonly used derogations are set out below, where the restricted transfer is:

A. made with the explicit consent of the Data Subject

B. necessary for the performance of a contract between a Data Subject and Controller

C. necessary for reasons of Substantial Public Interest

D. necessary for the establishment, exercise, or defense of a legal claim

E. necessary to comply with applicable anti-money laundering or counterterrorist financing obligations that apply to a Controller or Processor or for the prevention or detection of a crime

Practical application: These derogations are for us in very limited, specific circumstance and should be narrowly interpreted. If you are uncertain as to whether one of them may apply you may seek general guidance from the Commissioner's Office or contact a legal advisor for support.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Q5) Is the restricted transfer covered by one of the limited circumstances set out in Article 27(4) of DP Law 2020?

If you are making a restricted transfer that is not covered by an adequacy decision, nor an appropriate safeguard or derogation, then you can only make that transfer if it is covered by one of the limited circumstances set out in Article 27(4) of the DP Law 2020.

You should only apply this clause where such limited circumstances are clear exceptions from the general rule that you should not make a restricted transfer unless it is covered by an adequacy decision, appropriate safeguards, or a substantiated derogation is in place.

Practical application: If it is covered by such a limited circumstance exception, you may go ahead with the restricted transfer. Please continue to evaluate all such use and seek feedback from the Commissioner through prior consultation or other similar recourse if in doubt. Of course, as always, you must still comply with the rest of the DP Law 2020.

Q6) Have you considered the obligations under Article 28 regarding sharing Personal Data with government authorities, specifically documenting either a) a risk assessment and a form of "written assurances" under Article 28(1)(a to c) or b) a risk self-assessment under Article 28(2)?

While law enforcement and government authorities have powers prescribed to them by local laws, there are protections set out in the DP Law 2020 in relation to the sharing of Personal Data by DIFC controllers or processors with government authorities under Article 28.

Where a controller or processor receives a request from any public authority, whether in the UAE or outside the UAE, for the disclosure and transfer of Personal Data, it must undertake the following actions:

(a) determine the validity and proportionality of the request, and to ensure that any disclosure of Personal Data is carried out solely for the purpose of meeting the objectives identified in the request from the public authority;

(b) carry out an assessment of the impact of the proposed transfer in light of the potential risks to the rights of any affected data subjects and, where appropriate, implement measures to minimise such risks (e.g. redacting or minimising Personal Data or utilising appropriate technical or other measures to safeguard the transfer); and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the public authority that it will respect the rights of data subjects and comply with the general data protection principles set out in Part 2 of the DIFC DPL.

Controllers and processors (upon reasonable notice to the controller) may disclose or transfer Personal Data to the public authority provided they have taken reasonable steps to ensure that the request from the public authority is valid and proportionate and the public authority will respect the rights of data subjects when processing any Personal Data shared with it by the Controller. Reasonable steps may include for example:

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

(a) refining the scope of a request that is deemed overly broad or beyond the purposes, if any, described in the request;
(b) documenting an impact assessment of sharing the data versus not sharing it, i.e., effect on rights of the data subject versus the common good;
(c) confirming the recipient / requestor is employing privacy enhancing technology, training, policies and other measures to assure the safety of the data;
(d) agreeing that when the purpose is fulfilled the data is returned or destroyed by the recipient / requestor.

Where necessary, the requirements of Articles 26 and 27 also apply.

Practical application: Accordingly, if a (UAE or Dubai) government authority makes a request that involves the sharing of Personal Data, then such a request must take into account the framework of obligations set out in Article 28. All entities in the DIFC have to make an assessment in accordance with this Article as outlined above before sharing any Personal Data with such authorities and all such authorities should recognise the legal basis of the DP Law 2020 given that it ultimately derives from UAE constitutional powers and appointments.

Article 28 gives the exporting entity three (3) options to ensure data shared with an importing government authority is controlled in some manner. Each option results in one common, risk-based outcome: to document the decision properly, demonstrating that the issue of government access has been considered and safeguarded.

Article 28(1) suggests that an exporting entity "should" take such steps, recognizing that it is not always a) possible under applicable laws and regulations – particularly regarding prevention and investigation of alleged financial crime – or b) necessary, with respect to very basic, low risk requests, to obtain written assurances. In any case, where the importing government authority engages in the bilateral effort to agree that DP Law-based terms for sharing Personal Data with it, they both have a documented, fair opportunity to give input into the necessary safeguards and limitations, if any, on the scope of the request.

Article 28(2) is the basis for the exporting entity to make its own assessment and document any risks and prepare to mitigate them. Article 28(2) suggests that a Controller or Processor should conduct an impact / risk self-assessment to ensure the requirements of sub-paragraphs a and b are sufficiently met. The similarity here with Article 28(1)(c) is the concept of "written assurances", in that a DPIA for example or perhaps even a policy document is created to clarify to the organisation the appropriate steps for sharing data with government authorities.

A fallback position, to consult with the Commissioner, is set out in Article 28(3). A further nuance to this option, however, is that where requested, it is possible that the requesting government entity and / or the consulting entity may receive guidance from the Commissioner's Office, or any of the entities involved may submit a complaint, seek a decision of contravention or no contravention of the DPL, seek a direction, or rely on other remedies as set out in Part 9 of the DP Law 2020.

"Reasonably practicable" in this context broadly means an assessment of where there is room and scope to discuss safeguards and applicability of the DPL to the transfer. The DPL will always apply, however, there are terms within the DPL that permit sharing for regulatory purposes, (substantial) public interest, to prevent financial crime, etc. Short of the importing government authority having a court order, warrant, or other specific judicial or regulatory mandate, it is usually "reasonably practicable" to at least have the discussion about obtaining such assurances.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

"Written assurances" could come in many forms, including a basic data sharing MOU or annex to the DIFC SCCs. It could also be a simple email agreement citing Article 28 of the DP Law 2020, or even a full data protection agreement. Again, the DIFC Commissioner's Office is available to consult on possible forms of "written assurances" and whether pursuit of obtaining this safeguard is warranted.

Please check the DP website and Data Export & Sharing page for any updates and applicable documents further detailing the applicability and effect of Article 28. Templates, including a sample Article 28 MOU, are available on the templates section of the Accountability & Rights page of the DIFC DP website. Specific guidance on Article 28 is available as well.

Note on the Schrems I and II decisions

On July 16, 2020**, t**he Court of Justice of the European Union in its ruling in the Schrems II case invalidated a data sharing agreement between the EU and the US, called Privacy Shield, as a legitimate transfer mechanism between the US and the EU / EEA. DIFC had not permitted Privacy Shield as a mechanism for international transfers as it applied to transfers and onward transfers from the EU to the US only. In any case, it had a significant impact on data transfers globally, as for a long period of time, technically, transfers to the US from Europe were "illegal", and potentially onward transfers from DIFC or other non-EU jurisdictions would have been "illegal" as well.

On March 25, 2022, the US Government and the European Commission announced an agreement in principle to a new framework for transfers from the EU to the US, called the Trans-Atlantic Data Privacy Framework (the "Framework"). Please review the White House joint statement with the European Commission setting out the general elements of the framework.

DIFC DP Commissioner's Office anticipates that, as above, the Framework will not apply to transfers *directly* from the DIFC as it is an agreement between the EU and the US. However, if your entity is part of a multi-national or group business that engages in transfers / onward transfers from the EU, it may come into play. In such cases, please consider reviewing the transfers made by your entity once Personal Data leaves the DIFC for processing in the EU, to ensure the transfers remain compliant with Article 27 of the DIFC DP Law 2020. For further assistance, please review the Commissioner's comprehensive guidance on DP Law 2020 as well as the Data Export assessment tool. Please note that any such guidance is for informational purposes only and should not be construed as legal advice provided by the Commissioner's Office.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

5. Conclusion

International data export, sharing and transfers (including onward transfers) can be a complex area of data protection law, and will often require professional feedback. If you have questions or require clarity, please feel free to contact the DIFC Commissioner's Office.

Email: commissioner@dp.difc.ae

Telephone: 04 362 2222

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

6. Appendices

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Appendix 1: BCR Guidance and Application Process

Introduction

Like many globally accepted world class data protection laws, Data Protection Law, DIFC Law No 5 of 2020 (the DPL) restricts transfers of Personal Data outside of the DIFC to ensure that the level of protection afforded by the DPL is preserved. Personal Data may only be transferred to a jurisdiction outside the DIFC (a 'third country') or international organisations in compliance with certain safeguards and conditions for transfers. Binding Corporate Rules ('BCRs') are one way that controllers and processors can comply with the DPL's third country data transfer requirements. They are explicitly recognised in the DPL as a mechanism providing appropriate safeguards for third country data transfers (Article 27(2)(b))[9].

What are BCRs?

BCRs are legally binding and enforceable internal rules and policies for data transfers within multinational group companies and work in a way somewhat similar to an internal code of conduct. They allow multinational companies to transfer Personal Data internationally within the same corporate group to countries that do not provide an adequate level of protection for Personal Data as required under the DPL.

BCRs ensure that all data transfers within a corporate group comply with the DPL and must contain:

- data protection principles, such as transparency, data quality, and security;
- tools of effectiveness (such as audit, training, and complaint handling); and
- an element proving that the BCRs are binding, both internally and externally such as an intra-company agreement, DPA or similar binding instrument

Controller BCRs and Processor BCR's

Controller BCRs

Controller BCRs are suitable for data transfers from controllers established in the DIFC to other group company controllers or to processors established outside the DIFC. They apply to entities within the same group acting as controllers and to entities acting as 'internal' processors.

Processor BCRs

Processor BCRs apply to Personal Data received from a controller established in the DIFC which is not a member of the group and then processed by group members as processors or sub-processors. These type of BCRs are an alternative to incorporating the DIFC SCCs into service agreements with controllers.

[9] Article 27(2)(b) DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Why Binding Corporate Rules are a Useful Option

BCRs can be tailored to fit the needs of the business and once implemented and operational, are much easier to maintain compared to intra-group contracts incorporating the DIFC SCCs. They also set a high standard for compliance with the DPL which should reduce business exposure and are seen as the ensuring robust compliance with the DPL.

Additionally, BCRs provide a great degree of flexibility not found in other adequacy mechanisms, as the Commissioner does not need to approve non-material updates to BCRs.

Implementing BCRs also acts to further raise awareness of data protection compliance within a business and serves to demonstrate accountability, as required under the DPL.

Whereas standard contractual clauses (EU Model Clauses, UK IDTA, DIFC SCCs, etc) generally work well for smaller companies and bilateral data sharing, their use in a large multinational can be very cumbersome and impractical:

- Standard contractual clauses may not be fit for purpose where there is a complex web of processing activities.
- Larger companies with many affiliates abroad often need to put in place hundreds of standard contractual clauses which can be very costly.

Application and approval process

1. The content of BCRs applications

BCRs should be tailored to the particular corporate group. BCRs may consist of several documents so long as the legal relationship between the group of companies / affiliates is clearly set out. One suggested approach is that the main principles for compliance will be set out in one document and that this will then be complemented by policies, guidelines, audit and training programs, etc.
DIFC does not have a standard application form at this time. The current process covers either

- ✓ recognition of existing BCRs from another competent supervisory authority (i.e., an EU Member State DP regulator); or

- ✓ creation of DIFC BCRs, which is based on the current EU BCR application framework and approval process.

Whether the latter would be accepted or recognised by other competent supervisory authorities as a transfer mechanism may be a risk to consider when applying only such BCRs.

The benefits however are:

- ✓ that approval of DIFC BCRs is at least as a set of internal data protection policies and procedures that have been reviewed and approved by the Commissioner, which can be incorporated into EU or UK model clauses in terms of measures in place to safeguard Personal Data; or

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- ✓ for the purposes of a "dry run" for an EU BCR approval through the review process here, it may make very good sense to attempt BCR approval here in the DIFC.

For guidance, there is a suite of documents available to prepare an application in line with the EU requirements, which are the same as the DIFC approach, and which can be found at the following URL.[10]

Provided the framework is adhered to and the required information set out below (and if set out in the DIFC Data Protection Regulations, where amended) is made available to the Commissioner for approval, and that the applicant cooperates in providing additional supporting information as required, and on an on-going basis, these documents as a whole will comprise the DIFC application package.

2. Requesting Commissioner's Approval of Existing BCRs

If you wish to request review and approve of existing BCRs, in accordance with Article 27(8) of the DPL[11], please submit the appropriate documentation, which shall include:

(i) a full copy of its Binding Corporate Rules and confirmation as to whether such Binding Corporate Rules have been approved by any competent data protection authority;

(ii) details of the transfers it intends to make or receive in reliance on the Binding Corporate Rules; and

(iii) where the Binding Corporate Rules operate on the basis that members of the Controller's or Processor's Group (including the Controller or Processor) will bind other members of the Group, such as by way of power of attorney, full evidence of all valid instruments necessary to create such powers to bind should also be provided.

Please also provide a website, if available, where the group's BCRs are posted for inclusion on the DIFC DP Data Export and Guidance page listing of approved BCRs.

3. Requesting Approval of New, DIFC-approved BCRs

Please ensure that your application package, again which has no specific template other than to follow the format of the EU BCR approval process, includes the following elements:

Main principles document

The main principles document will need to address the key principles provided for in the DPL[12]. This includes:

- transparency, fairness and lawfulness;
- data minimisation and accuracy;
- purpose limitation;

[10] Article 29 Working Party Guidance (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf) Please see also https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[11] Article 27(8) DIFC Data Protection Law No.5 (2020)

[12] Article 9 DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- storage period limitation;
- sharing with third parties and government authorities; and
- security / storage / retention

It should also provide guarantees regarding:

- processing of Special Categories of Personal Data;
- restrictions on transfers and onward transfers to external processors and controllers without BCRs but with other accepted safeguard mechanisms in place;
- compliance with Article 24 of the DPL[13] for agreements with processors (both within the group and externally); and
- an obligation to notify data breaches to the Commissioner (or other competent authorities), the DPO if any, and the data subject (if applicable).

The scope of the Personal Data covered by the BCRs should also be set out.

Other elements

The following elements must also be addressed in the BCRs, either in the main principles document or associated supporting documents:

- ✓ **Scope of application:** The BCRs must specify the data transfers to which they apply, the categories of Personal Data, the type of processing and its purpose, the types of data subjects, and identify any third countries where data is transferred.

- ✓ **Group structure:** The BCRs must specify the group structure, the list of entities bound by the BCRs and their contact details. It should also be stated whether they apply to all Personal Data transferred from the DIFC or to all processing of Personal Data within the group, whatever the origin.

- ✓ **Binding nature of BCRs[14]:** BCRs must be legally binding and governed by the DPL. The BCRs must include a duty for each BCR member and its employees to respect the BCRs.

- ✓ **Accountability:** Every entity acting as a controller must be able to demonstrate compliance with the BCRs[15]. Processors should make information available (where not otherwise restricted by applicable laws) to the controller to demonstrate their compliance with the BCRs, including through audits and inspections[16].

- ✓ **Complaint handling[17]:** There must be an established system that allows data subjects to complain about any BCR member. Any such complaints must be dealt with by a clearly identified department without undue delay, and in any event, within one month. Additionally, the people handling the complaints must have an appropriate level of independence in exercising their functions.

[13] Article 24 DIFC Data Protection Law No.5 (2020)

[14] Article 27 DIFC Data Protection Law No.5 (2020)

[15] Article 14 DIFC Data Protection Law No.5 (2020)

[16] Article 24(5)(b)(x) and 46(3)(b) DIFC Data Protection Law No.5 (2020)

[17] Article 60 DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- ✓ **Third-party beneficiary rights[18]:** The BCRs must grant data subjects the right to enforce BCRs as third-party beneficiaries.

- ✓ **Transparency:** Data subjects should be provided with the information in Articles 29 and 30 of the DPL[19] and information on their third-party beneficiary rights in relation to how their data is processed and how they can exercise those rights. Specifically, the BCRs must include clauses on liability and the data protection principles, and information must be provided in full or provide links to other data protection notices such as to privacy policies[20]. For these purposes, they may incorporate the DIFC SCC Clauses 8 to 15.[21]

- ✓ **Easy Access[22]:** BCRs must contain the right for every data subject to have access to them. For example, relevant information should be published on the website or internet for employees.

- ✓ **Third country legislation[23]:** The BCRs must include a commitment that any third country legal requirements likely to have a substantial adverse effect on the guarantees of the BCRs will be reported to a competent supervisory authority; for example, any legally binding request for disclosure by law enforcement or state security authorities must be reported. The BCRs must also include a commitment that if there is a conflict between applicable laws and the BCRs, the DIFC entity, the BCR member with delegated data protection responsibilities, or any other relevant privacy officer or function, will take reasonable decision on the appropriate action and consult with the Commissioner if there is any doubt.

- ✓ **Right to lodge a complaint[24]:** Data subjects should be able to bring a claim before the Commissioner, or a supervisory authority in their home country, country of work, where the alleged infringement took place, before the DIFC Courts, or in the data subject's country of residence.

- ✓ **Relationship with national laws[25]**: The BCRs should state that where local laws require a higher level of protection for Personal Data, the local laws will take precedence over the BCRs.

- ✓ **Cooperation with supervisory authorities[26]**: The BCRs must contain clear and unambiguous undertakings that all BCR members as a whole, and any members of the group separately, will cooperate with relevant supervisory authorities, accept to be audited by relevant supervisory authorities; and comply with the advice of relevant supervisory authorities.

[18] Article 63 DIFC Data Protection Law No.5 (2020)

[19] Articles 29 and 30 DIFC Data Protection Law No.5 (2020)

[20] Article 9 and Part 2(D) DIFC Data Protection Law No.5 (2020)

[21] Clause 8-15 DIFC Standard Contractual Clauses

[22] Article 33 DIFC Data Protection Law No.5 (2020)

[23] Article 10(1)(c) and Article 11(j) DIFC Data Protection Law No.5 (2020)

[24] Articles 53 and 60 DIFC Data Protection Law No.5 (2020)

[25] Article 10(1)(c) and Article 11(j) DIFC Data Protection Law No.5 (2020)

[26] Article 27(8)-(10) DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- ✓ **Liability**[27]: The DIFC entity must accept responsibility for and agree to take the necessary action to remedy acts of other group members outside the DIFC. The BCRs must also contain an obligation on the DIFC entity to pay compensation for damages arising from a breach of BCRs by any member of the group. There must also be a statement that the responsible group member bears the burden of proof in relation to alleged breaches of BCRs by a group member outside the DIFC.

Binding nature

The above principles need to be binding within the corporate group, as against employees and subcontractors[28]. The documents likely to achieve this are:

- A resolution of the parent company's board to make the principles binding;
- An employee notice requiring application of the principles;
- Pro forma contract terms for use with subcontractors; and
- Intra-group contract that confers third party rights.

- ✓ **Further evidence**
  As well as the main principles document and the binding documents discussed above, the following also need to be documented:

- ✓ **Training**[29]
  Training on BCRs must be provided to those employees who have regular or permanent access to Personal Data. When seeking approval of BCRs, supervisory authorities will require evidence that the commitments in the BCRs are being respected. Such evidence may include examples and explanations of the training programmer employees regarding the BCRs; for example, records may be kept about the training that employees receive such as records of the content of the training, attendee lists, and training schedules.

- ✓ **Audit programme**[30]

  The process for auditing compliance with BCRs on a regular basis will be documented and reported directly to the ultimate parent's board or to the DPO. The BCRs must also state that the audit programme will cover all aspects of the BCRs and ensure that any necessary corrective action will be taken. The data protection audit programme and plan must be clearly set out either in a document containing the group's data protection standards or in other internal procedure documents. The BCRs must also specify when the audits will take place (this must be on a regular basis).

  Additionally, audits must be carried out at the request of the DPO or at the request of any other competent function within the group, and the BCRs must state that the supervisory authorities can have access to the results of the audits on request. The BCRs must grant the supervisory authorities the right to carry out a data protection audit themselves (or independent auditors on their behalf), and each member of the group must accept that it could be audited by the supervisory authorities and abide by their advice on any issue related tithe BCRs.

[27] Articles 23 and 64 DIFC Data Protection Law No.5 (2020)

[28] Article 27(8)(iii) DIFC Data Protection No.5 (2020)

[29] Article 18(3)(a)(iii) DIFC Data Protection No.5 (2020)

[30] Article 18 DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

- ✓ **Compliance and supervision**[31]
  The BCRs must include a brief description of the internal structure, role, position and tasks of the DPO and the appropriate network created and must set out a system that guarantees awareness and implementation of BCRs within the corporate group. Articles 16 to 19 of the DPL cover this information.

Decision process

The applicant should submit an initial draft to the Commissioner or a legal advisor for review and to respond to any queries. Then, a consolidated draft addressing the queries and filling any information gaps should be submitted. Once the Commissioner decides that the applicant has prepared a consolidated draft to a satisfactory standard, it will invite the applicant to send it the final draft, adding any other provisions or requirements it finds necessary to ensure compliance within the organisation. When the final draft is submitted, the Commissioner will approve and refer the matter to the Board for informational purposes. The approved BCRs may then be applied to relevant transfers.

Checklist of documents to be provided to the Commissioner

1. The main principles document
2. A document setting out third party rights (if third party rights clause is not contained in the main principles document)
3. Application based on the content provisions set out herein (please also see below)[32]
4. Documents to make the BCRs binding. (e.g. resolution of parent company board to make the principles binding; employee notice to require application of the principles; pro forma contract terms for use with subcontractors; intra-group contract which confers third-party rights)
5. Supporting documents that demonstrate that commitments in the BCRs are being respected by the members

Updates to BCRs

BCRs should include an obligation that significant changes to the BCRs or to the list of BCR members are notified to all group members and to the Commissioner or relevant supervisory authorities. Any significant changes to the BCRs must be communicated to data subjects. Certain modifications will also require a new authorisation from the Commissioner.It is possible to update BCRs without having to re-apply for authorisation, provided that:

- Personal Data is not transferred to a new group member until the data exporter has ensured that the new member is effectively bound by the BCRs and can ensure compliance.
- An identified person or department keeps a fully updated list of members of the BCRs, keeps track of and records any updates to the BCRs and provides the necessary information tithe data subjects or the Commissioner or supervisory authorities on request.
- Any changes to the BCRs or to the list of BCR members should be reported once a year to the Commissioner, along with a brief explanation of the reasons justifying the update.

The BCRs should also contain an obligation that the group will ensure compliance with the above requirements for updates to the BCRs.

[31] Article 16-19 DIFC Data Protection Law No.5 (2020)

[32] Article 46 DIFC Data Protection No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Examples of supporting documents to demonstrate commitment to BCRs

- Privacy Policies
- Employee guidelines for those who have access to Personal Data
- Data protection audit plan and programme
- Examples and explanation of training programmes for employees
- Documents demonstrating that the member of the group transferring data outside the DIFC, and the DIFC entity itself has sufficient assets to pay any compensation resulting from breach of the BCRs
- A description of the internal complaint system
- A list of entities in the group bound by the BCRs
- A security policy for IT systems that process Personal Data
- A certification process to ensure that all new IT applications that process Personal Data are compliant with the BCRs
- Any standard contracts that are used with processors that process DIFC Personal Data and incorporate the appropriate Article 24 elements / model clauses[33]
- A job description of the DPO or other persons that are in charge of data protection

BCR Assurance

The effectiveness of a BCR may be assessed by submitting them to a formal audit and assurance assessment. As discussed above, BCRS contain a commitment to have their implementation audited/reviewed on a regular basis. Depending on the exact wording of the BCR, the organisation can commit itself to a certain level of review.

[33] Article 24 DIFC Data Protection Law No.5 (2020)

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Appendix 2: Ethical Data Management Risk Index 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, ***reduces 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.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

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?

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

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 right 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 worth having 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.
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.

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Assessment Criteria	Risk Weighting Rationale
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 requirement, 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?
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?

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Please provide comments or feedback on the Index methodology to commissioner@dp.difc.ae

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.

Version control

Data Export Guidance Guidance about exporting data to non-adequate jurisdictions outside the DIFC.	Version - updated July 2020
Updates made based on SCC consultation	October 2021
Updated information regarding Article 28 and EDMRI	August 2022

CONFIDENTIALITY NOTICE and DISCLAIMER – This document and any attachment are confidential and may be privileged or otherwise protected from disclosure and solely for the use of Dubai International Financial Centre Authority. No part of this document may be copied, reproduced, or transmitted in any form or by any means without written permission.