



**GUIDANCE FOR USE OF
ARTICLE 24
DATA PROTECTION
CLAUSES AND
ABBREVIATED
DIFC SCCs**

Commissioner of Data Protection

CONTENTS

1. Introduction.....	3
2. Scope	4
3. FAQs	5
4. Examples.....	6
5. Transfers and Clauses – Practical Application	8
Appendix 1 – Article 24 Data Protection Clauses	9
Appendix 2 – Abbreviated SCCs with Pre-filled Annexes.....	12
Appendix 3 – Flow chart for appropriate safeguard requirements for data transfers	19

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

The goal of the DIFC Commissioner of Data Protection (the **Commissioner**) in producing this guidance is to assist Controllers and Processors subject to the [Data Protection Law, DIFC Law No. 5 of 2020](#) (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") about standard contractual clauses referred to in Article 24 of the DPL, the implementation of abbreviated DIFC SCCs, and the difference between these sets of clauses.

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

2. Scope

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

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

3. FAQs

What is Personal Data?

Any information which can identify (directly or indirectly) a natural living person e.g., name, an identification number, location data, an online identifier, biometric, genetic, economic, cultural or social identity.

Why do we need data protection clauses in our contracts or in addition to them?

The overarching aim of the DIFC Data Protection Law (DP Law) is to protect the Personal Data of Data Subjects. The DP Law sets various obligations on companies to do so. Whenever you question why something is required under the DP Law, please go back to this overarching aim.

Every contract should have general data protection clauses / a schedule as a minimum that sets out compliance obligations under Articles 23 and 24 of the DP Law 2020 and any further general obligations therein. These clauses are for inclusion in general framework agreements and MOUS, separate and apart from the standard contractual clauses required for certain transfers of Personal Data outside the DIFC, in accordance with Article 27, which is discussed further below.

Also included is an example of a data protection clause and schedule in Appendix 1 of this note. To comply with Articles 23 or 24, they ought to be included in every contract (as minimum) irrespective of whether an external transfer is taking place.

What do we need to do for compliant Data Transfers?¹

When dealing with companies, contracts and transfers think about the “where”. Where is Personal Data being transferred to? This will determine if additional safeguards need to be put into place.

There are 3 main examples of data transfers. These are where²:

1. Personal Data is transferred within the DIFC.
2. Personal Data is transferred outside the DIFC, but is to a recognised jurisdiction which has an adequate data protection law or regime in place (adequate jurisdiction).
3. Personal Data is transferred outside the DIFC, and is to a jurisdiction where there is an absence of an adequate level of protection (non-adequate jurisdiction).

Bear in mind a Controller’s transfers could involve any or all of the above examples.

¹ A flow chart in Appendix 3 of this note provides an overview of this structure.

² Please refer to the [DIFC Data Export and Sharing Handbook](#) for more details and requirements for transfers.

4. Examples

1. Personal Data is transferred within the DIFC

Easy! The transfer of Personal Data can go ahead without any additional safeguards, provided that a general data protection clause/schedule is included in the contract, as DIFC companies are required (and expected) to adhere to the DP law.

2. Personal Data is transferred to an adequate jurisdiction (Article 26)

Easy! If the transfer of Personal Data is to an approved jurisdiction, the transfer of Personal Data can go ahead without any additional safeguards, provided that a general data protection clause/schedule is included in the contract. There may be some cases where the Third Party wants us to use their contract, which is OK, but check for DP clauses that match up with the clauses in the Agreement, MOU or other schedule, if any.

Where do I find the list of “adequate” jurisdictions in line with Article 26?

Below are the approved jurisdictions as listed in the DP Regulations, although these may be updated from time to time. The best place to find the most up to date list is here:

<https://www.difc.ae/business/operating/data-protection/data-export-and-sharing/#s3>

Abu Dhabi Global Market	Japan
Andorra	Jersey
Argentina	Latvia
Austria	Liechtenstein
Belgium	Lithuania
Bulgaria	Luxembourg
California	Malta
Canada	Netherlands
Colombia	New Zealand
Croatia	Norway
Cyprus	Poland
Czech Republic	Portugal
Denmark	Romania
Estonia	Singapore (Including Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP))
Faroe Islands	Slovakia
Finland	Slovenia
France	South Korea (Including Cross Border Privacy Rules (CBPR))
Germany	Spain
Greece	Sweden
Guernsey	Switzerland
Hungary	United Kingdom
Iceland	Uruguay
Ireland	
Isle of Man	

Table 1

3. Personal Data is transferred to a non-adequate jurisdiction (Article 27)

For data transfers outside the DIFC to a jurisdiction that does not have an adequate level of protection of Personal Data, Controllers and their Processors or Co-Controllers need to ensure certain safeguards are in place and that Personal Data is still being protected to a standard required under DP Law. One method is to complete the standard contractual clauses and append them to the agreement.

By adopting the standard contractual clauses into agreements and signing the appendices, Controllers in un-recognised jurisdictions can be held liable for any misuse/mishandling/ or any other Personal Data breach as defined under the DP law. Without these, there is a high risk that you would remain liable. Most importantly, your business will be in breach of the DP Law 2020, or potentially EU or UK DP Law if applicable to its operations, which carries with it hefty fines.

5. Transfers and Clauses – Practical Application

The below table (“**Table 2**”) that breaks the concepts above down into an easy to follow guide:

Where is data transferred to	Requirement within the contract	Where can you find it?
Within DIFC Freezone	Basic data protection clauses (if not already present)	Appendix 1
Outside DIFC- to UAE	Basic data protection clauses (if not already present) Standard Contractual Clauses	Appendix 1 Appendix 2
Outside DIFC- to countries not listed in Table 1	Basic data protection clauses (if not already present) Standard Contractual Clauses	Appendix 1 Appendix 2
Outside DIFC – to country listed in Table 1	Basic data protection clauses (if not already present)	Appendix 1
If DIFC DP Schedules for procurement (or as applicable) are not accepted, then check for the below		
When transferring to EU, UK or ROW not listed in Table 1 via EU or UK	<ul style="list-style-type: none"> - Check for basic DP clauses in general agreement. If none, please add to general agreement. - Check if the basic DP clauses refer to EU SCCs (model clauses) or if they are appended to the contract. If not, please append to general agreement. 	<p>Appendix 1; as this is often non-standard, please seek DP review where possible.</p> <p>Appendix 2 may be acceptable, but often EU / UK entities will require the full EU or UK model clauses to be used.</p>

6. Questions and Comments

For further information about Article 24 requirements, please review guidance about [Obligations of Controllers and Processors](#), and the [relevant assessment tool](#). For further information about Article 27 requirements for exporting data from the DIFC, please review [DIFC Data Export and Sharing Handbook](#) and the [relevant assessment tool](#).

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

Appendix 1 – Article 24 Data Protection Clauses

Standard agreements (MOUs, sponsorship agreements, etc) ought to include this language where Personal Data is involved in the scope of the contract activities. For general framework agreements on Third Party paper where data protection is not covered at all, the following can be inserted:

Definition:

Data Protection Legislation: the Data Protection Law, DIFC Law 5 of 2020, or any amendment or replacement thereof, and applicable data protection laws of other jurisdictions, such as the EU General Data Protection Regulation or the UK General Data Protection Regulation.

- or -

DP Law: the Data Protection Law, DIFC Law 5 of 2020, or any amendment or replacement thereof.

GENERAL DRAFTING NOTE – One of these options should be added if nothing at all is present to define DP Laws. If a definition for data protection legislation *is* present, then it is probably safe to modify the existing language to include reference to the DIFC DP Law, if necessary. If for example the definition says “[EU GDPR, UK GDPR, other DP Law] and any applicable data protection laws or regulations” then it could remain as is, as the DIFC DP Law would effectively fall under “any applicable...” This is a fairly harmless approach and the reviewer can concentrate on other, more critical edits like adding approved Article 24 DP clauses or something like them.

General DP Clauses:

GENERAL DRAFTING NOTE – *if there is a data protection section already present in a third party contract for example, it's fairly easy to map the elements required from our law at Articles 23 and / or 24 and potentially leave that section as is. It's when there is nothing in the contract at all and DP should be addressed, i.e., because Personal Data processing is in scope, then better to add them and then agree a final, negotiated set if necessary.*

1. Data protection and Data Processing

- 1.1 [The definitions set out in Schedule 1, Section 3 of the Data Protection Law, DIFC Law No. (5) of 2020 shall apply to all relevant capitalized terms in this Clause.] *DRAFTING NOTE - similar comment as above re: definition. If there already is DP language in the contract and / or it has a catch all sort of provision, then it's probably safe to modify slightly to make sense or simply leave as is.*
- 1.2 [Unless otherwise agreed on a case-by-case basis, the parties agree to share, at no cost and free from any charge, information, trends, reports, and other such data as may be necessary to achieve the purpose of their co-operation. In particular, the parties may share information and documents in relation to capital markets 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.

technical assistance under the principle of professional secrecy and reciprocity.] *DRAFTING NOTE – can be removed or edited, not a show-stopper.*

- 1.3 Any exchange and/or processing of Personal Data, shall take place in accordance with the provisions of the [DP Law] [Data Protection Legislation]. *DRAFTING NOTE – Choose most appropriate reference as per the law reference definitions selected from the options above.*
- 1.4 To the extent permitted by the laws of a Party subject to a government data sharing request, (“Requesting Party”), the Requesting Party shall inform the Party providing the relevant information (“Providing Party”) about how or where the requested information will be stored or utilized, and any assurances that will further safeguard the requested information. *DRAFTING NOTE – This is generally aligned to Article 28 of the DP Law, but also serves a purpose specification safeguard.*
- 1.5 Unless otherwise agreed in advance, neither party may appoint a Sub-processor of Personal Data processed pursuant to this [Agreement / MOU] without the prior written consent of the other party [which shall not be unreasonably withheld]. Any such appointment must include a written agreement containing all necessary controls and safeguards [as set out in Article 24 of the DP Law]. *DRAFTING NOTE – the language in brackets regarding prior written consent is often requested to be added. It’s fine to include. Start from here only to ensure a higher security standard. The language in brackets regarding Article 24 safeguards may be retained or removed depending on which law reference definition is selected from the options above.*
- 1.6 Both parties shall ensure that any person(s) authorized to process the Personal Data in accordance with this [Agreement / MOU] have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality [as set out in Article 25 of the Data Protection Legislation]. *DRAFTING NOTE – The language in brackets regarding Article 25 obligations may be retained or removed depending on which law reference definition is selected from the options above.*
- 1.7 Both parties shall implement appropriate compliance, technical and organizational measures to ensure the security of the Personal Data obtained or processed for the purposes of this [Agreement / MOU], including conducting risk or processing impact assessments as needed and assisting with audits or inspections conducted by an appropriate, recognised third party, and agree to notify any reportable Personal Data Breaches to the appropriate parties, [including the Commissioner of Data Protection or the Data Subject]. *DRAFTING NOTE – The language in brackets regarding breach notification obligations may be retained, modified accordingly or removed depending on which law reference definition is selected from the options above.*
- 1.8 Regarding any promotion or marketing activity performed under this [Agreement / MOU], both parties shall comply with applicable direct marketing laws, if any.
- 1.9 Without prejudice to the generality of this Clause [X.3], each party will ensure that it has all necessary and appropriate contractual clauses, consents and notices in place generally, and specifically to enable exercise of applicable Data Subjects’ rights (including assisting with responses) or to support lawful processing of Personal Data for the duration and purposes of this [Agreement / MOU].

1.10 Where Personal Data is transferred outside the DIFC to parties in jurisdictions that do not have a data protection law equivalent to that of the Data Protection Legislation in accordance with Article 26 of the Law, [or where an existing law may not be fully enforced such that it impacts accountability of the [THIRD PARTY]], the parties agree to supplement this Clause [X] with applicable standard contractual data sharing clauses approved in accordance with Article 27 and the DIFC Data Protection Regulations 2020. *DRAFTING NOTE – the language in brackets is optional. It aligns to the use of the EDMRI as an additional organisational safeguarding measure.*

Clauses that may already exist based on other information in the Agreement or MOU

DRAFTING NOTE: Due to the nature of the agreement with a Processor or even a Co-Controller, the following clauses as required by Article 24 may already be present in the document under another heading, i.e., recitals, scope of work, schedules, etc. If not, then please ensure the following wording or similar is included. Where wording is in brackets, it is suggested wording to choose or not based on the context and requirements in the Agreement or MOU:

- 1.11 All Parties shall comply with [DIFC Data Protection Law, DIFC Law No. (5) of 2020 and its obligations thereunder] [in addition to applicable [Data Protection Legislation]].
- 1.12 This Agreement shall be entered into by [X], in its capacity as [Controller/Processor] and [X], in its capacity as [Processor/Sub-Processor] of Personal Data whereby [X] will process Personal Data on behalf of and in accordance with the instructions of [Controller/Processor] for the duration of this [Agreement / MOU] or until termination or expiry [in accordance with Clause [X] of this [Agreement / MOU]].
- 1.13 For the purposes of this Agreement, the [Processor/Sub-processor] agrees to process the following Personal Data for the specified purposes:
- (a) [list out type of Personal Data and purpose for Processing],
- 1.14 The [Processor/Sub-processor] will process the Personal Data set out in Clause [X] which relates to the following categories of Data Subjects:
- (a) [set out list of Data Subjects, i.e., employees, clients, suppliers, contacts, etc].

Further guidance:

1. Regarding Clause 1.10 (or equivalent once inserted in relevant general framework agreement or MOU), Appendix 2 provides an option for an abbreviated version to be appended. If a standalone data processing agreement (DPA) is requested or required, please use the document that may be downloaded from this link:

https://www.difc.ae/application/files/6616/8551/6891/DIFC_A_27_SCCs_-_DIFC_Exporter_transferring_to_Importer_AS_DPA_ONLY.docx

It is editable, and can to some extent be negotiated, again, only if used as a standalone DPA.

Appendix 2 – Abbreviated SCCs with Pre-filled Annexes

DRAFTING NOTE: In order to minimise the amount of documentation to be attached to a contract that requires appending the Article 27 standard contractual clauses, the following language and relevant sections / information must be added as a Schedule to the framework agreement and completed. The footnotes contain guidance for how to use and complete these clauses. Please remove these footnotes in the final, applied document.

[As set out in Clause [X] of the [general framework agreement]³ regarding transfers of Personal Data to a Third Country that is not yet considered adequate by the [DIFC Commissioner of Data Protection or relevant supervisory authority [in the EU or UK]], the standard contractual clauses (SCCs) available at the link selected below are deemed to be appended to the general framework agreement and binding on the Parties in order to comply with [choose: Article 27 / 45 for the EU / 46 for the UK] of the [Data Protection Law, DIFC Law No 5 of 2020 / General Data Protection Regulation (EU) 2016/679 / Retained Regulation (EU) 2016/679 (UK GDPR) and the Data Protection Act 2018 (DPA 2018)⁴]⁵

[DIFC SCCs](#)

For the purposes of Clause 9(1)(a), the Parties agree to Option 1 Option 2

For the purposes of Clause 9(2)(a), the Parties agree to Option 1 Option 2

[EU SCCs](#)

Selected modules to be agreed by the Parties in a separate Annex

[UK SCCs](#) / Addendum

Appropriate selections and / or UK addendum for EU transfers to be completed in a separate Annex

OTHER SCCs (To be provided by Exporter or Importer)

³ If applicable. Rename document to appropriate reference as needed.

⁴ Please note that the UK has proposed new legislation to replace the retained GDPR and DPA 2018. Please watch for updates and adjust this text accordingly.

⁵ Suggested introductory text.



On behalf of the Data Exporter:

Name (written out in full): Click or tap here to enter text.
Position: Click or tap here to enter text.
Address: Click or tap here to enter text.

Other information necessary in order for the contract to be binding (if any):

Signature.....[may be e-signed].....

On behalf of the Data Importer(s):

Name (written out in full): Click or tap here to enter text.
Position: Click or tap here to enter text.
Address: Click or tap here to enter text.

Other information necessary in order for the contract to be binding (if any):

Signature.....[may be e-signed].....

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.

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES (SCC) FOR PROCESSING PERSONAL DATA

This Annex forms part of the SCCs and must be completed by the Parties.

Parties Processing Personal Data

Data Exporter

Role (Controller/Processor)⁶: Controller Processor

Please specify briefly your activities relevant to the transfer:

.....[*Scope of the Agreement or MOU*].....

Data Importer

Role (Controller/Processor)⁷: Controller Processor

Please briefly specify your activities relevant to the transfer): ...

.....[*Scope of the Agreement or MOU*].....

Personal Data Being Processed

Data Subjects

The Personal Data transferred concerns the following categories of Data Subjects (please specify):

- Employees Clients / Customers Suppliers
- Other Third Parties / Stakeholders

.....[*If "Other", please provide details as necessary*]

Categories of data

The Personal Data transferred concerns the following categories (please specify):

- Accounts Benefits, Grants, Loans
- Administrative Credit References
- Advertising / Marketing Human Resources

⁶ Could be both – please clarify whether the exporter will also receive any Personal Data as a co-Controller or to be further processed. If neither, it will only be an Exporter for these purposes.

⁷ Could be both – please clarify whether the exporter will also receive any Personal Data as a co-Controller or to be further processed. If neither, it will only be an Importer for these purposes.

- Law Enforcement / Govt
- Legal Services
- Insurance Administration
- Pensions Administration
- Research and Development
- Other

.....[If “Other”, please provide details as necessary]

Special categories of data (if any)

Special categories of data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for Onward Transfers or additional security measures.

The Personal Data transferred concern the following Special categories (please specify):

- Racial or ethnic origin
- Communal origin
- Political affiliations or opinions
- Religious or philosophical beliefs
- Criminal record
- Trade-union membership
- Health or sex life
- Genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person

Processing operations

Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Please describe the frequency of the transfer(s)

.....On-going as per scope of processing activities⁸

Nature of the processing

The Personal Data transferred will be subject to the following basic processing activities (please specify):

- Automated
- Semi-automated
- Fully integrated processing
- Manual

.....[Please provide details as necessary]

Purpose(s) of the data transfer and further processing

.....[Please specify]

⁸ Suggested text, please adjust accordingly to provide more details, information, etc.

Retention period for which the Personal Data will be processed, if any, and the criteria used to determine that period

- Per Importer policy
- Per Exporter policy
- Per applicable laws and regulations
- Other

.....[If "Other", please provide details as necessary]

For transfers to **(Sub-) Processors**, also specify **subject matter, nature and duration** of such further processing

.....[Please provide details as necessary]

Identify whether **any other competent supervisory authority/ies**⁹ may have jurisdiction in accordance with clause 13 of the SCCs

- EU [insert Member State]
- UK
- Other

.....[If "Other", please provide details as necessary]

⁹ For example, in addition to the DIFC Data Protection Commissioner, this could be a DP supervisory authority in an EU Member State, the UK or elsewhere.

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.

ANNEX 2 TO THE SCCS – TECHNICAL AND ORGANISATIONAL MEASURES

This Annex forms part of the SCCs and must be completed by the Parties.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with these Clauses (or document/legislation attached):

Description of the technical and organisational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures:

- Measures of pseudonymisation and encryption of Personal Data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which Personal Data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure
- Review of DIFC [EDMRI](#) and completion of [EDMRI+ due diligence tool](#) regarding importer compliance risk

For transfers to (Sub-)Processors, also describe the specific technical and organisational measures to be taken by the (Sub-)Processor to be able to provide assistance to the Controller and, for transfers from a Processor to a Sub-processor, to the Data Exporter

...[TO BE COMPLETED BY IMPORTER RE: PROCESSORS / SUB-PROCESSORS].....

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.

ANNEX 3: LIST OF PROCESSORS OR SUB-PROCESSORS

Where applicable, please list Processors or Sub-processors that the Controller / Exporter has authorised for processing operations set out in Appendices 2 and 3 above.

[IMPORTING COMPANY NAME] Record of Processing / Sub-Processing Activities

Name and contact details of the Processor its appointed DPO, where applicable, and Sub-processors, if known	Purpose(s) of the Processing	Description of the categories of Data Subjects	Description of the categories of Personal Data	Categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in Third Countries and International Organisations	Identification of the Third Country or International Organisation that the Personal Data has or will be transferred to and, in the case of transfers under Article 27, the documentation of suitable safeguards (where applicable)	Time limits for erasure of the different categories of Personal Data (where applicable)	General description of the technical and organisational security measures referred to in Article 14(2)

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 3 – Flow chart for safeguard requirements for data transfers

