



Assessment of [JURISDICTION]'S Data Protection Law as an Adequate or Equivalent Law recognized

by the

**Dubai International Financial Centre Authority
("DIFC" or "DIFCA")**

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.

Document Classification:
PUBLIC

Document Updated on:
DD MMMM YYYY

Date / Frequency of Review:
ANNUAL

23/01/2022 11:22
Uncontrolled copy if printed

Page
1 of 9



Table of Contents

Introduction	3
Observation 1: Basic data protection concepts and definitions	4
Observation 2: Grounds for lawful and fair processing for legitimate purposes	4
Observation 3: Existence of Data Protection Principles	4
Observation 4: Data Subjects Rights (DSR)	4
Observation 5: International Data Transfers	4
Observation 6: Security of Processing and Breach Reporting:	5
Observation 7: Accountability, principles and legitimate processing (including direct marketing or other compliance obligations required by other laws and regulations)	5
Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement).....	5
Observation 9: Existence of international commitments and conventions binding on [JURISDICTION] or its membership of any multilateral or regional organisations	5
Conclusion.....	6
Appendix 1: List of Firms Incorporated in [JURISDICTION]	7
Appendix 2: Enforcement Action.....	8
Appendix 3: Undertaking to substantially comply with Article 28 of the DIFC DP Law 2020	9

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.



Introduction

Adequacy recognition is based on an assessment of key data protection concepts and obligations found in a [JURISDICTION]'s data protection laws to ensure equivalence with the local data protection law. As such, the DIFC Office of the Commissioner of Data Protection assesses the relevant laws and regulations according to the following criteria¹:

1. Basic data protection concepts and definitions
2. Grounds for lawful and fair processing for legitimate purposes
3. Existence of Data Protection Principles
 - a. purpose limitation
 - b. data quality and proportionality
 - c. data retention
 - d. security and confidentiality
 - e. transparency
4. Data Subjects' Rights
 - a. right of access, rectification, erasure and objection
5. International / Onward Data Transfer Restrictions
6. Security of Processing and Breach Reporting
7. Accountability
 - a. Special categories of data (aka sensitive personal data)
 - b. Direct marketing
 - c. Automated decision making and profiling
8. Additional content principles for specific types of processing
9. Existence of international commitments and conventions binding on [JURISDICTION] or its membership of any multilateral or regional organisations

¹ Please see EU and UK adequacy referentials for guidance: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872231/D - Adequacy Referential.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872231/D_-_Adequacy_Referential.pdf)

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.



Summary of [JURISDICTION]'s Applicable Laws and Regulations

Observation 1: Basic data protection concepts and definitions

Please provide an overview of the basic data protection concepts and definitions captured in the relevant laws.

Summary of key obligations / changes

- **Concepts and definitions:**
- **Breach notification requirements:**
- **Enforcement powers:**
- **Notifications to the Commissioner / Supervisory Authority:**
- **Powers and objectives of the Commissioner:**

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Please provide information about the Articles of the relevant laws that provide for these obligations.

Observation 3: Existence of Data Protection Principles

- a. purpose limitation
- b. data quality and proportionality
- c. data retention
- d. security and confidentiality
- e. transparency

Observation 4: Data Subjects Rights (DSR)

Please state the relevant Articles of the applicable laws that provide for these obligations.

Observation 5: International Data Transfers

Please state the relevant Articles of the applicable laws that provide for these obligations.



Observation 6: Security of Processing and Breach Reporting:

Please state the relevant Articles of the applicable laws that provide for these obligations.

Observation 7: Accountability, principles and legitimate processing (including direct marketing or other compliance obligations required by other laws and regulations)

Please state the relevant Articles of the applicable laws that provide for these obligations.

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

Please state the relevant Articles of the applicable laws that provide for these obligations.

Observation 9: Existence of international commitments and conventions binding on [JURISDICTION] or its membership of any multilateral or regional organisations

Please state the relevant Articles of the applicable laws that provide for these obligations.



Conclusion

It is for these reasons that the DIFC Office of the Commissioner of Data Protection (“the Commissioner”) should grant adequacy recognition to [JURISDICTION]. The current [laws and regulations] align with the DIFC DP Law 2020 such that transfers to [JURISDICTION] will receive the same or substantially equivalent protection.

[Specific limitations on provision of recognition, if any, to be listed here]

The Commissioner has the right to repeal, amend or suspend its adequacy decision regarding [JURISDICTION] at any time.

Dated:



Appendix 1: List of Firms Incorporated in [JURISDICTION]

As a result of the adequacy recognition observations and recommendations above, transfers of personal data between DIFC [entities – laws to be cited depending on adequacy decision scope], and [JURISDICTION FIRMS] may occur without a requirement for additional safeguards, in accordance with DIFC DP Law 2020 Article 26 and 27, and [JURISDICTION] LAW].

A list of [JURISDICTION FIRMS] is available [Public register? List provided by written request? How best to access this information?], and may be reviewed to ensure the safety and adherence to the respective applicable data protection laws is undertaken.



Appendix 2: Enforcement Action

Data Protection Enforcement

[JURISDICTION] has undertaken the enforcement action in the form of investigations and thematic reviews for supervision purposes. Fines [are / are not] issued [how, when, why?], and [will] include:

- Warnings or admonishments or recommendations to Data Controllers issued
- Contraventions of the [JURISDICTION LAW] brought to the attention of the [JURISDICTION COURTS?]
- Directions issued to Controllers
- Investigations conducted



Appendix 3: Undertaking to substantially comply with Article 28 of the DIFC DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

[JURISDICTION] undertakes in good faith, and will ensure that [JURISDICTION ENTITIES] substantially comply with Article 28 of the DIFC DP Law 2020, to the extent possible under applicable laws and regulations to which both are subject, with respect to Personal Data transferred in accordance with the terms of adequacy recognition set out above.

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.