ABU DHABI GLOBAL MARKET

Guidance on the Data Protection Regulations 2021

Part 6: International Transfers

Office of Data Protection

TABLE OF CONTENTS

1. INTRODUCTION

Introduction to this Guidance

1.1 This is Part 6 in the series of guidance (Guidance) on the Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021). It covers international transfers of personal data.

2. INTERNATIONAL TRANSFERS

2.1 General

The DPR 2021 restricts the transfer of personal data out of the ADGM to a jurisdiction outside of the ADGM, or to an international organisation[1]. This is because individuals whose personal data would ordinarily be protected by the DPR 2021 may no longer have the same protections where their personal data is processed outside of the ADGM.

The DPR 2021 does not prohibit data exports altogether. It allows for personal data to be exported where individuals' rights may be protected using some other mechanism, or where one of the exceptions applies.

2.2 What does it mean to "transfer" personal data?

Transfer is interpreted broadly and covers not only an act of sending, but also making available personal data to an individual or organisation in another jurisdiction. This could be, for example, by uploading personal data to a portal or system and granting access to an individual in another jurisdiction access to that portal or system. A transfer may be made where sending, or granting access to, personal data either to a third party, or to another organisation within your group, where the other organisation is based outside of the ADGM.

Example:

The marketing team at a consultancy based in the ADGM shares a document which lists all of their contacts for clients in the UAE with the marketing team at the company's office in France, so that they can identify any overlaps in personnel and opportunities.

This would constitute an international transfer.

Example:

The local HR team at a FinTech company uses an online, cloud based platform to store personal data relating to employees.

HR operations are managed centrally from the UK, meaning that the HR team in London requires access to the platform to view the information stored in relation to ADGM based employees.

Granting access to the HR team in the UK would constitute a transfer.

[1] Under the DPR 2021 'International Organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

2.3 Would onshore United Arab Emirates count as a non-ADGM jurisdiction?

Yes, it would.

2.4 Is there a de-minimis rule which applies?

No. Any transfer of personal data outside of the ADGM, however small, must be made in accordance with Part V of the DPR 2021. Many businesses will put in place framework agreements to cover regular sharing of personal data.

2.5 Consider whether it is necessary to make an international transfer

Before making any international transfer of personal data, consider whether it is necessary to make that transfer. Transferring personal data is a processing activity in its own right and is subject to the necessity principle (see section 4(1)(c) of the DPR 2021).

If the same purpose can be achieved by anonymising personal data before making a transfer, you should consider whether this is a viable alternative to sharing the personal data in identifiable form.

2.6 How can personal data be legitimately transferred outside of the ADGM?

There are various ways in which personal data can be legitimately transferred outside of the ADGM. Those are as follows:

a. transfer on the basis of an adequacy decision (see paragraph 2.7 below);

b. transfer on the basis of appropriate safeguards without the need for Commissioner approval for the transfer. Those include the following (provided always that the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available):

   i. a legally binding and enforceable instrument between public authorities;

   ii. binding corporate rules (BCRs) (see paragraph 2.9 below);

   iii. standard data protection clauses adopted by the Commissioner of Data Protection (Commissioner) (see paragraph 2.10 below);

   iv. a Commissioner approved code of conduct pursuant to section 37 of the DPR 2021 together with binding and enforceable commitments of the controller or processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards data subjects' rights (see paragraph 2.10 below); or

   v. a Commissioner approved certification mechanism pursuant to section 39 of the DPR 2021 together with binding and enforceable commitments of the controller or processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards Data Subjects' rights (see paragraph 2.11 below);

The Commissioner does not require exporters relying on (i) – (v) above to conduct a detailed analysis of the laws of the importing jurisdiction, but recommends that exporters conduct due diligence on importing entities to ensure that they are capable of meeting their commitments under (i) – (v) above (as applicable).

c. where the Commissioner has given its approval:

i. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data outside of ADGM or the international organisation; and

ii. provisions to be inserted into administrative arrangements, including regulatory memorandums of understanding between public authorities or domestic or international bodies which include enforceable and effective data subject rights; or

d. transfers made on the basis of the derogations (see paragraph 2.12).

2.7 Adequacy decisions

The Commissioner has the power to designate certain jurisdictions, sectors within jurisdictions and / or international organisations as ensuring an adequate level of protection. This means that the Commissioner has taken the view that transferring personal data from the ADGM to those jurisdictions can be done without putting in place any additional safeguards. The rationale is that the laws or rules which apply to such transfers are sufficient to protect the rights of the data subjects whose personal data is being transferred.

The list of adequate jurisdictions can be found at: https://www.adgm.com/operating-in-adgm/office-of-data-protection/jurisdictions. Note that these may be updated from time to time as the Commissioner will monitor for any changes in law which could impact an adequacy decision. When making its assessment the Commissioner will take account of the factors set out at 41(2) of the DPR 2021.

It will however still be necessary for the transferor to satisfy itself that it has a legal basis to make the transfer (transfer being a processing activity) under section 5 (and 7, if the personal data is special category data) of the DPR 2021.

In addition, if a controller is transferring personal data to a processor in an adequate jurisdiction, it would still be necessary for the controller to enter into a contractual arrangement which meets the requirements of section 26 of the DPR 2021 (unless relying upon the standard contractual clauses, which meet these requirements – see paragraph 2.9 below).

2.8 Binding corporate rules

Businesses can make a restricted transfer within their international organisation if both transferor and the transferee (i.e. All the relevant group entities, if more than two) have signed up to BCRs which have been approved by the Commissioner. The BCRs must be legally binding and apply to and are enforced by every member concerned of the group, including employees.

There are detailed requirements at section 43(1)(a) and 43 (2) of the DPR 2021 which BCRs must meet. The Commissioner may also approve BCRs where those have been approved by another another supervisory authority[2]. When BCRs are submitted to the Commissioner for approval, the Commissioner will consider whether those requirements are all met and may require adjustments to be made where they are not, prior to granting approval.

[2] "Supervisory Authority" is defined as: (a) an independent authority which has been established pursuant to Article 51 of the GDPR, which includes, for these purposes, the United Kingdom's Information Commissioner's Office; or (b) an independent authority with responsibility for ensuring and enforcing compliance with the data protection rules that is established in a jurisdiction which the Commissioner of Data Protection has decided ensures an adequate level of protection in accordance with section 41(3) of the DPR 2021.

2.9 Standard data protection clauses

The Commissioner has published a set of standard contractual clauses (SCCs) on its website. The SCCs are based on the current standard contractual clauses issued by the European Commission and will cover each of the following scenarios through various "modules":

a. controller-to-controller transfers, for when a controller based in the ADGM is transferring personal data to a controller outside of the ADGM;

b. controller-to-processor transfers, for when a controller in the ADGM is transferring personal data to a processor outside of the ADGM. The SCCs will contain provisions which meet the requirements under section 26(3) of the DPR 2021, although it is acknowledged that under certain circumstances the parties may agree a separate set of terms which meet the section 26(3) requirements and which may be negotiated (e.g. In the body of a services agreement);

c. processor-to-processor transfers, for when a processor in the ADGM is transferring personal data to another processor outside the ADGM; and

d. processor-to-controller transfers, for when a processor in the ADGM is transferring personal data to a controller outside the ADGM.

The SCCs place obligations on both data exporters and data importers and give data subjects the right to enforce those against either party.

Example:

A financial institution in the ADGM relies on third party software hosted in Australia to make certain transactions. The party which provides the software requires limited access to certain personal data held within the platform, primarily to provide support services to the financial institution.

As the platform provider has access to the personal data, there will be an export of personal data from the ADGM to Australia. As Australia is not an adequate jurisdiction, the parties agree to enter into the SCCs to ensure that the transfer is made in compliance with the DPR 2021. The transfer in question would likely be made on a controller to processor basis, provided that the platform provider does not determine the means and purposes of processing.

2.10 Approved code of conduct

International transfers can be made under a Commissioner approved code of conduct. At present the Commissioner has not approved any codes of conduct.

For further guidance on codes of conduct, please refer to paragraph 2 of Part 7 of this Guidance.

2.11 Certification

International transfers can be made under a Commissioner approved certification scheme.

2.12 Derogations

In accordance with section 44 of the DLR 2021, personal data can also be exported from the ADGM under the following circumstances:

Data subject consent

Any such consent should meet the conditions set out under section 6 of the DPR 2021. It is important to recognise that consent cannot be bundled within contracts or privacy policies for transfers generally. Any consent must be specific and limited.

Data subjects should be informed of:

- the identity of the recipient (or the category which it falls in);
- the location(s) of the recipient;
- reason for the transfer;
- the types of data being transferred;
- their right to withdraw consent; and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. For example, you may inform data subjects that their data subject rights may not be exercisable in the receiving country, or that public bodies have unfettered access to their data.

Consent can also be withdrawn, which reduces its usefulness as a legal basis for transfer.

The Commissioner's expectation is that consent is unlikely to be a common legal basis for transfer given the informational requirements and the right to withdraw. Its utility is likely to be limited to certain one off situations where no other legal basis is available. It is recommended that wherever an alternative legal basis for transfer is available, that alternative legal basis is used.

Consent cannot be relied upon by public authorities as the legal basis for transfer.

Transfer is necessary for the performance of a contract (between data subject and controller) or implementation of pre-contractual measures taken at the data subject's request

Example:

An individual books a holiday in the Kingdom of Saudi Arabia via a travel booking platform which is run from the ADGM. As instructed by the individual, the platform sends the individual's personal data to:

1. the airline, prior to the booking being made, to see if the individual can use his or her rewards points to upgrade to business class (i.e. pre-contractual measures); and

2. the hotel in the Kingdom of Saudi Arabia once the booking has been made, so that the hotel can log the booking on its own systems (i.e. necessary for the performance of a contract).

This basis cannot be relied upon by public authorities as the legal basis for transfer.

Transfer is necessary for the performance of a contract between controller and third party (in the interests of the data subject)

Example:

An individual is applying for a role at a company based in the ADGM. For regulatory reasons, before offering the individual the role, the ADGM company requires a criminal record check issued in the country in which the individual has lived for the past 5 years, Nigeria. The ADGM company engages a criminal background check provider in Nigeria to provide this. It provides the provider with the name, date of birth and passport number of the individual.

The transfer is necessary for the third party to provide the ADGM company with its services, as per the contract in place between the ADGM based company and the service provider in Nigeria. That transfer is clearly in the interests of the data subject, as it is necessary for him or her to secure the role that he or she is applying for.

This basis cannot be relied upon by public authorities as the legal basis for transfer.

Transfer is necessary for important reasons of public interest

Note that the public interest reason must be recognised in applicable law (as defined in the DPR 2021) to which the controller is subject.

Example:

An ADGM based Fintech company wishes to share its data pool with a think tank in Russia to enable the think tank to develop an artificial intelligence tool which will help the poorest in society better manage their finances.

Whilst the transfer is arguably in the public interest, as that public interest is not recognised under applicable law (as defined under the DPR 2021), the transfer would not be permitted under the public interest derogation.

UAE law enforcement agencies

Example

The UAE public prosecution may request an ADGM based company to provide it with information in accordance with its powers under Federal Law No. 35/1992 Concerning the Criminal Procedural Law (as amended).

Note that this derogation would not extend to cover requests from law enforcement agencies outside of the UAE.

Establishment, exercise or defence of legal claims (including judicial, administrative, regulatory and out-of-court procedures)

The transfer must be necessary, so there must be a clear nexus between the need for the transfer and the relevant legal claim.

Example:

A competition authority in the U.S. is bringing an action against a group of individuals on the basis that they colluded to keep the price of a certain good high. In the course of that investigation that competition authority requests information from a company in the ADGM where one of those individuals used to be a director. It is clear that the information requested is fundamental to the action being brought.

Whilst this isn't a civil claim (in the sense of one party claiming damages from another) it is a "regulatory" procedure and the transfer of personal data to the U.S. would therefore be legitimate.

You cannot rely on this exception if there is only the slight possibility that a legal claim or other formal proceedings (whether judicial, administrative, regulatory and out-of-court procedures) being commenced.

Vital interests

This derogation applies in a medical emergency where the transfer is needed in order to give the medical care required. The imminent risk of serious harm to the individual must outweigh any data protection concerns.

2.13 Will permits issued under the Data Protection Regulations 2015 remain valid?

Yes. Permits previously issued by the Commissioner will remain valid until their expiry, or until those are expressly revoked by the Commissioner (whichever is sooner).

For more information, you may contact the Commissioner of Data Protection of Data Protection on:

Telephone No.: 00 971 2 3338888

Email: Data.Protection@adgm.com

Address: ADGM Building, Abu Dhabi Global Market Square, Al Maryah Island, Abu Dhabi, United Arab Emirates.

Disclaimer

This Guidance is a non-binding indicative Guidance and should be read together with the Data Protection Regulations 2021 and any other relevant regulations and enabling rules, which may change over time without notice. Information in this Guidance is not to be deemed, considered or relied upon as legal advice and should not be treated as a substitute for a specific advice concerning any individual situation. Any action taken upon the information provided in this Guidance is strictly at your own risk and the Office of Data Protection, Registration Authority and ADGM will not be liable for any losses and damages in connection with the use of or reliance on information provided in this Guidance. The Office of Data Protection, Registration Authority and ADGM make no representations as to the accuracy, completeness, correctness or suitability of any information provided in this Guidance.