DATA PROTECTION LAWS OF THE WORLD

UAE - Abu Dhabi Global Market Free Zone

DLA PIPER

UAE - ABU DHABI GLOBAL MARKET FREE ZONE

Last modified 9 January 2024

LAW

Note: Please also see UAE – General, UAE – DIFC, UAE – DHCC.

The Abu Dhabi Global Market ("**ADGM**") is a financial freezone in Abu Dhabi emirate. The ADGM has powers to issue laws regarding its governance. On 14 February 2021 the ADGM issued the ADGM Data Protection Regulations 2021 ("**DPR**").

An important feature of the new framework is the establishment of an independent Office of Data Protection, headed by a Commissioner of Data Protection.

In order to assist businesses in understanding the requirements DPR, and how those should be applied to their activities, in August 2021 the Office of Data Protection issued a suite of eight guidance documents which cover the following topics:

1. General overview;
2. Data subject rights
3. Data protection by design and default, fees, record of Processing activities (“**ROPA**”), data protection officers (“**DPOs**”) and Processor obligations;
4. Data protection impact assessments (“**DPIAs**”);
5. Security of Processing and data breaches;
6. International transfers;
7. Codes of conduct and the role of the Commissioner of Data Protection and the Office of Data Protection; and
8. Individual Rights and Remedies.

DEFINITIONS

Definition of Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Definition of Processor

A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

Definition of Data Subject

An identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Personal Data

Any information relating to a Data Subject.

Definition of Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Definition of Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Definition of Special Categories of Personal Data

- Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- Genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data Concerning Health or data concerning a natural person's sex life or sexual orientation; and
- Personal Data relating to criminal convictions and offences or related security measures.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection performs his functions with the support of the Office of Data Protection. Those functions include the following:

- exercising investigative powers, where necessary;
- monitoring and enforcing the application of the DPR;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to Processing;
- advising and issuing opinions to the ADGM Board of Directors, Registration Authority, Financial Services Regulatory Authority, ADGM Courts, and other institutions and bodies on legislative and administrative measures relating to the protection individuals rights with regard to the Processing of Personal Data;
- promoting the awareness of Controllers and Processors of their obligations under the DPR. The Commissioner may also engage in outreach programmes to raise awareness and increase understanding DPR;
- providing the public with opportunities to provide views on the activities of the Office of Data Protection;
- handling complaints lodged by individuals, and investigating, to the extent appropriate, the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation is necessary;
- cooperating with, including sharing information and provide mutual assistance to, other data protection authorities with a view to facilitating the effective enforcement of legislation for the protection of Personal Data worldwide;
- monitoring relevant developments insofar as they have an impact on the protection of Personal Data, in particular the development of information and communication technologies and business practices;
- adopting standard contractual clauses (as per Sections 26(6) and 42(2) DPR);
- publishing and maintaining a list as to the types of Processing operations which typically require a DPIA (as per Section 34 (4) DPR);
- approving codes of conduct and certification criteria (as per Sections 38(1) and 39(1) DPR);
- authorising contractual clauses and provisions referred to in Section 42(4) DPR;
- approving binding corporate rules pursuant to Section 43 DPR;

- issuing guidance and publishing standard forms (e.g. The August 2021 Guidance and the template DPIA);
- keeping records of non-compliance by those entities caught by the DPR, as well as any measures taken as a result of such non-compliance; and
- collecting data protection fees and renewal fees.

The contact details for the Office of Data Protection are as follows:

The Office of Data Protection
Authorities Building
ADGM Square
Al Maryah Island
Abu Dhabi
UAE

Email

Data.Protection@adgm.com

There is also a “Make An Enquiry” form available on the Office for Data Protection’s website.

REGISTRATION

Data protection fee

Section 24 DPR requires Controllers to pay a data protection fee to the Commissioner of Data Protection before, or as soon as reasonably practicable after, they start Processing Personal Data under the DPR.

It is also necessary to provide the Commissioner of Data Protection with:

- name and address (which, in the case of a registered company, will be its registered office); and
- Data Controllers must also establish and maintain records of any Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.

All licensed entities in the ADGM would have already provided much of the necessary information to the Commissioner of Data Protection during the company incorporation and registration Process. The date of incorporation is also the date the Controller may commence Processing Personal Data, such as the Personal Data of directors, shareholders and other statutory role holders. Each year, within one month of the expiry of the anniversary on which a Controller commenced Processing Personal Data under the DPR it is also necessary to pay the renewal fee.

The amounts payable are set out in the Data Protection Regulations 2021 (Fees) Rules 2021.

As per Section 28 DPR each Controller and Processor to which the DPR applies must maintain a record of Processing activities in writing. This can be in electronic form, but it does not necessarily need to be. The record of Processing activities must be made available to the Commissioner of Data Protection upon request.

DATA PROTECTION OFFICERS

Controllers and Processors must appoint a DPO where:

- the Processing is carried out by a public authority, except for courts acting in their judicial capacity;
- the core activities of the Controller or the Processor consist of Processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of Data Subjects on a large scale; or
- the core activities of the Controller or the Processor consist of Processing on a large scale of special categories of Personal Data.

COLLECTION & PROCESSING

Data Controllers may Process Personal Data when any of the following conditions are met, as per Section 5(1) DPR:

- the Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes. There are detailed conditions for consent set out under Section 6 DPLs;
- Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the Controller is subject under Applicable Law;
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person;
- Processing is necessary for the performance of a task carried out by a public authority in the interests of ADGM, or in the exercise of (i) ADGM’s; (ii) the Financial Services Regulatory Authority’s; (iii) the ADGM Court’s; or (iv) the Registration Authority’s functions or in the exercise of official authority vested in the Controller under Applicable Law (as defined under the DPR);
- Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, except where such interests are overridden by the interests or rights of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a Child.

Data Controllers may Process Special Categories of Personal Data when any of the following conditions are met:

- the Data Subject has given explicit Consent to the Processing of their Special Categories of Personal Data for one or more specified purposes;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment law, provided that when the Processing is carried out, the Controller has an appropriate policy document in place in accordance with Section 7(3) DPR;
- Processing is necessary to protect vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
- Processing is necessary for health purposes, including preventative or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health care or treatment or the management of health care systems or services or pursuant to a contract with a health professional provided that Processing is by or under the responsibility of a health professional subject to the obligation of professional secrecy or duty of confidentiality;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- Processing is necessary for Archiving and Research Purposes in accordance with Applicable Law;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body including religious, cultural, educational, social or fraternal purposes or for other charitable purposes and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside that body without the Consent of the Data Subjects;
- Processing relates to Personal Data which is intentionally made public by the Data Subject;
- Processing is required for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- Processing is necessary for reasons of substantial public interest, provided that (unless specified otherwise) the Controller has, when the Processing is carried out, an appropriate policy document in place in accordance with Section 7 (3), where it is necessary for:
    - the exercise of a function or requirement conferred on a person by Applicable Law;
    - the exercise of a function of the Board, Abu Dhabi or United Arab Emirate government;
    - the administration of justice;
    - equality of opportunity or treatment provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual; and it does not relate to an individual who has given written notice to the Controller not to Process their Personal Data;
    - diversity at senior levels of organisations, where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject and is not aware of the Data Subject withholding Consent provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual;
    - the prevention or detection of an unlawful act or omission where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose; and if the Processing relates to the disclosure of Personal Data to a relevant public authority an appropriate policy document in accordance with Section 7(3) need not be in place for the Processing to be lawful under these Regulations;
    - the protection of the members of the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a company, body or association, or failures in services provided by a company, body or association where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose;
    - compliance with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or omission, or been involved in dishonesty, malpractice or other seriously improper conduct where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject to the Processing;
    - the prevention of fraud in connection with Processing of Personal Data as a member of, or in accordance with arrangements made by, an antifraud organisation;
    - the disclosure in good faith to an appropriate public authority regarding suspected terrorist financing, to identify terrorist property or in relation to suspected money laundering, in accordance with Applicable Law; or
    - the publication of a judgment or other decision of a court or tribunal or if the Processing is necessary for the purposes of publishing such a judgment or decision.

TRANSFER

International transfers

The DPR restricts the transfer of Personal Data out of the ADGM to a jurisdiction outside of the ADGM, or to an international organisation. 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 includes transfer to onshore UAE based recipients.

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

1. transfer on the basis of an adequacy decision. The list of adequate jurisdictions can be found on the ADGM website. 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 Section 41(2) DPR;

2. 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);

    iii. standard data protection clauses adopted by the Commissioner of Data Protection (available online). Those are broadly based on the recently issued EU SCCs;

    iv. a Commissioner approved code of conduct pursuant to Section 37 DPR 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; or

    v. a Commissioner approved certification mechanism pursuant to Section 39 DPR 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'.

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).

3. where the Commissioner has given its approval to:

    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

4. transfers made on the basis of the set out under Section 44 DPR (some of which are subject to additional qualifications):

    i. the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

    ii. the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

    iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

    iv. the transfer is necessary for important reasons of public interest;

    v. the transfer is required by law enforcement agencies of the UAE in accordance with Applicable Law (as defined under the DPR);

vi. the transfer is necessary for the establishment, exercise or defence of legal claims (including judicial, administrative, regulatory and out-of-court procedures); or

vii. the transfer is necessary in order to protect the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving consent.

SECURITY

The obligation to provide appropriate technical and organisational (security) measures for Personal Data applies to both Controllers and Processors. The DPR do not specify any particular security measures, rather it is up to the organisation to judge what is appropriate in the circumstances taking into account:

- the state of the art (i.e. the current state of technological development as appropriate to the context including: industry practice; the type and scale of the Processing; and the availability of a product or solution in the market);
- the costs of implementation;
- the nature, scope, context and purposes of the Processing; and
- the likelihood and severity of risks to Data Subjects’ rights (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data).

Controllers must only use Processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their Processing will meet the requirements of the DPR and protect Data Subjects’ rights. Controllers are primarily responsible for overall compliance with the DPR, and for demonstrating that compliance. If this isn’t achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures (see “Enforcement” below).

BREACH NOTIFICATION

In the event of a breach of any Personal Data held by a Data Processor, the Data Processor shall inform the Data Controller of the incident without undue delay after becoming aware of the Personal Data Breach (Section 32(2) DPR).

If a Data Controller becomes aware of a Personal Data Breach, the Data Controller must inform the Commissioner of Data Protection of the incident without undue delay, and where feasible, not later than 72 hours after becoming aware of it (Section 32 (1) DPR).

When the Personal Data Breach is likely to result in a high risk to the rights of natural persons, the Controller must communicate the Personal Data Breach to the Data Subject without undue delay.

ENFORCEMENT

Investigation and enforcement

The Commissioner has broad investigative powers under the DPR. Those include the power to:

- order, by notice in writing, Controllers and Processors to provide any information it reasonably requires for the performance of its duties and functions;

- initiate investigations into a Controller’s or Processor’s compliance with the DPR;

- it also has the power to access any equipment used to Process Personal Data (such as computers) and to take possession of any relevant documentation or information. The Commissioner must give written notice of the decision to investigate unless it believes that would likely result in the investigation being frustrated;

- carry out investigations in the form of data protection audits;

- carry out a review on certifications issued pursuant to Section 39 DPR;
- notify Controllers and Processors of any alleged contravention; and
- obtain, by notice in writing, from Controllers and Processors, access to all Personal Data and to all information reasonably necessary for the performance of its duties and functions.

From an enforcement standpoint, the Commissioner has the power to:

- issue and publish directions and warnings and make recommendations to Controllers and Processors that intended Processing operations are likely to contravene the provisions of the DPR;
- issue and publish directions and reprimands to Controllers and Processors where Processing operations have already contravened provisions of the DPR;
- order Controllers and Processors to comply with an individual's requests to exercise his or her rights pursuant to the DPR;
- order Controllers and Processors to bring Processing operations into compliance with the provisions of the DPR, where appropriate, in a specified manner and within a specified period;
- order a Controller to communicate a Personal Data Breach to the individual, where it has not done so already;
- impose a temporary or permanent limitation (including a ban) on Processing;
- order the rectification or erasure of Personal Data or restriction of Processing pursuant to Sections 14, 15 and 16 DPR and the notification of such actions to Recipients to whom the Personal Data has been disclosed, pursuant to Sections 15 (2) and 17 of the DPR;
- withdraw a certification if the requirements for the certification are not or are no longer met;
- impose an administrative fine pursuant to Section 55 of the DPR, in addition to, or instead of, any of the other measures set out under the DPR.

When considering whether to issue a fine the Commissioner will consider the circumstances on a case by case basis. For particularly serious breaches the Commissioner may well issue a fine and issue an order for the infringing party to resolve its infringement moving forwards;

- order the suspension of data flows to a recipient inside or outside of ADGM or to an international organisation; and
- where appropriate, refer contraventions DPR to the attention of the court and where appropriate, commence legal proceedings, in order to enforce the provisions DPR.

The DPR also provides a mechanism for Data Subjects to lodge complaints with the Commissioner (Section 57 DPR), and bring claims for compensation where they have suffered “*material or non-material damage*” as a result of a contravention DPR by a Controller or Processor (Section 59 DPR).

Notably the Commissioner has started to publish enforcement decisions, which are available upon the ADGM website.

ELECTRONIC MARKETING

According to Part 2 of the Commissioner’s Guidance, it is not always necessary to seek consent under the DPR to conduct direct marketing activities, such as sending marking emails. In many cases, it will be possible to rely upon legitimate interests (Section 5(1)(f) DPR) as the relevant legal basis for Processing. If relying on legitimate interests, it is important to ensure

that individuals are given the right to object both at the point at which their Personal Data is collected for direct marketing purposes, and within each communication (for example, by way of an “unsubscribe link” in an email). A pre-ticked box may be sufficient when offering the right to object at the point of data collection.

Whenever are relying on legitimate interests as the legal basis for Processing for direct marketing, consider whether the legitimate interests in conducting the marketing are overridden by the interests or rights of the Data Subject. Depending on the context of the direct marketing activities (for example, if the content of those marketing communications relates to products or services which are sensitive in some way, such as health related services), there may be instances where it will not be appropriate to rely on this as the relevant legal basis and consent would be more appropriate. Controllers must also ensure that they continue to meet their obligation to comply with the principles of transparency and fairness under Section 4 DPR by clearly describing their direct marketing activities in the applicable privacy notice.

ONLINE PRIVACY

The DPR does not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. Note that “online identifiers” fall within the definition of Personal Data. In addition, as UAE criminal law applies in the ADGM, the privacy principles laid out therein may apply (see UAE – General).

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.