NEW UAE FEDERAL DATA PROTECTION LAW

Date: 10 February 2022

UAE Data Protection, Privacy, and Security Alert

By: Mohammad Rwashdeh, Zaid Abu-Shattal

INTRODUCTION

The United Arab Emirates (UAE) has published its first Federal Data Protection Law No. 45 of 2021 (Law), which came into effect on 2 January 2022.

This alert provides an overview of the Law which will be supplemented by the expected executive regulations (Executive Regulations), as well as key aspects in comparison with other data protection frameworks such as the EU General Data Protection Regulation (GDPR).

Unless provided otherwise, capitalized terms have the meaning given to them in the Law, a list of which is provided at the end of this client alert for ease of reference.

APPLICATION OF THE LAW

Material Scope

The Law applies to:

- The processing of Personal Data of Data Subjects residing in the UAE or having a workplace in the UAE;
- Controllers or Processors established in the UAE that carry out the activities of Processing Personal Data for Data Subjects in the UAE or abroad; and
- Controllers or Processors established outside of the UAE that carry out the activities of Processing Personal Data for Data Subjects in the UAE.

Exemptions

The Law does not apply to:

- Government agencies that Process Personal Data;
- Personal Data held by security and judicial authorities;
- Data Subjects who process their Personal Data for solely personal purposes;
- Personal Data that relates to the health of a Data Subject and which is subject to specific legislation regulating the protection and processing of health data;
- Personal Data relating to banking, credit data, and information which are subject to specific legislation regulating the protection and processing of such Personal Data; or

- Companies and institutions located in free zones in the UAE which have their own legislation for the protection of personal data (i.e., these are currently the Dubai International Financial Centre and the Abu Dhabi Global Market).

GENERAL PROHIBITION ON PROCESSING WITHOUT CONSENT

The Law provides that Processing Personal Data without the Data Subject's Consent is prohibited except in certain circumstances (as further described below).

Data Subject Consent

Data Subject's Consent to the Processing of their Personal Data will be considered valid if the Controller can evidence that:

- Such Consent has been given by the Data Subject to process its Personal Data;
- The Consent was given in a clear, simple, unambiguous, and easily accessible manner, whether in writing or electronically;
- The Consent includes a statement indicating the right of the Data Subject to withdraw its Consent.

Data Subjects have a right to withdraw their Consent for the Processing of their Personal Data at any time.

As currently drafted, the Law does not expressly state that consent must be “freely given”, but this requirement is implied from the general rules of UAE law and established principles. The Executive Regulations may provide further clarifications on this aspect.

Alternatives to Consent

Processing Personal Data without obtaining the Data Subject's Consent is permitted in the following cases:

- It is necessary to protect the public interest;
- It is related to Personal Data that has been made public by the Data Subject;
- It is necessary to establish any legal claim or defense of rights and claims or in connection with judicial or security procedures;
- It is necessary for the purposes of occupational or preventive healthcare;
- It is necessary to protect public health, including protection against communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of medicines, drugs, and medical devices in accordance with the applicable legislation;
- It is necessary for the performance of a contract to which the Data Subject is a party or to take measures at the request of the Data Subject with the aim of concluding, amending, or terminating a contract;
- It is necessary for the Controller to perform specific obligations set out in other applicable legislation in the UAE; or
- Any other cases to be specified in the Executive Regulations.

In that regard, the Law encompasses all six legal basis for Processing that are already provided under the GDPR.

KEY COMPLIANCE REQUIREMENTS ON COMPANIES SUBJECT TO THE LAW

Obligations of Controllers

Personal Data must be collected for a specific and clear purpose and may not be Processed at a later time in a manner incompatible with that specific original purpose.

Personal Data must not be kept after the purpose for its Processing has ended, unless the identity of the Data Subject has been concealed using appropriate pseudonymization techniques.

In this regard, the Controller must ensure that Personal Data is accurate and, where necessary, updated.

Additionally, Personal Data must be limited to what is necessary in accordance with the purpose for which the Processing is carried out, must be stored securely and be protected against unauthorized or unlawful Processing using appropriate technical or organizational measures to be specified.

Moreover, the Law places a number of obligations that must be met by Controllers when Processing Personal Data. These include, without limitation:

- To implement necessary standards for the protection and security of Personal Data;
- To preserve the confidentiality and privacy of Personal Data;
- To ensure that Personal Data is not breached, damaged, altered, or tampered with; and
- To maintain a record of Personal Data.

Obligations of Processors

The Law also places a number of obligations on Processors. These include, without limitation:

- To process Personal Data in accordance with the instructions of the Controller and any agreement signed by the Processor and the Controller;
- To carry out Processing in accordance with the set purpose and duration; and
- To maintain a record of the Personal Data that is Processed on behalf of the Controller.

DATA PROTECTION OFFICER

The Controller and Processor must appoint a Data Protection Officer who has relevant and sufficient skills and knowledge in the following cases where the Processing:

- Creates a high risk to the confidentiality and privacy of the Data Subject's Personal Data as a result of adopting new technology or in relation to the volume of the Personal Data;
- Involves a systematic and comprehensive assessment of Sensitive Personal Data, including Profiling and Automated Processing; and
- Involves a large volume of Sensitive Personal Data.

The Data Protection Officer may be employed or appointed by the Controller or Processor and is not required to be on a UAE resident.

BREACH OF PERSONAL DATA

The Controller must inform the Emirates Data Office as soon as it becomes aware of any breach of Personal Data that would undermine the privacy, confidentiality, and security of a Data Subject. Unlike the 72-hour window mandated under GDPR, no specific timeline has currently been set. The notification must detail any preliminary investigation results as well as a statement on the nature, cause and extent of the breach. The notification must also include information on the Data Protection Officer, possible and expected effects of the breach, the procedures and measures already taken by the Controller and any additional proposed measures to counter the breach and mitigate its effects.

Additionally, the Controller must notify the Data Subject of any breach that would undermine the Data Subject's privacy, confidentiality, and security of their Personal Data, along with all information pertaining to inform any measures that were taken to address the breach.

Should the Processor become aware of any Personal Data breach, it will then have to notify the Controller of such breach as soon as it becomes aware of it.

Upon receiving a notification of Personal Data breach, the Emirates Data Office will assess the causes for such breach to determine the integrity of the security measures that were taken where the Emirates Data Office concludes that the Controller or Processor were in violation of any applicable provisions, administrative penalties may be implemented.

DATA SUBJECT'S RIGHTS

The Law offers Data Subjects a number of rights in respect to their Personal Data that is being Processed. These include the rights to:

- Access their Personal Data;
- Object to decisions issued by Automated Processing that have legal consequences or seriously affect a Data Subject including any Profiling;
- Request that their Personal Data is transferred;
- Amend or correct their Personal Data;
- Have their Personal Data erased if Processing is no longer required for the purposes for which the Personal Data was collected;
- Restrict or stop their Personal Data from being Processed in certain cases;
- Withdraw consent for Processing their Personal Data; and
- File a complaint with the Emirates Data Office.

TRANSFERRING PERSONAL DATA

Personal Data may be transferred outside the UAE to jurisdictions that have legislation for the protection of Personal Data, including provisions relating to the conditions and rules for protecting the privacy and confidentiality of a Data Subject's Personal Data, a Data Subject's ability to exercise their rights, and provisions relating to imposing appropriate measures on the Controller or Processor through a supervisory or judicial authority.

As of today, there is no specific process to assess the sufficiency of the importing-country-data–protection-framework. The Executive Regulations should provide welcomed guidance.

Personal Data may also be transferred to a jurisdiction outside the UAE where the UAE is party to a bilateral or multilateral agreement concerning the protection of Personal Data with such jurisdiction.

In jurisdictions that do not have data protection laws, parties operating in the UAE and in those jurisdictions may transfer Personal Data pursuant to an agreement that requires parties in the foreign country to apply the Law, including provisions related to imposing appropriate measures on the Controller or the Processor through a competent supervisory or judicial authority in that country.

A Data Subject may also expressly consent for their Personal Data to be transferred outside of the UAE as long as such transfer does not conflict with the public and security interest of the UAE.

A transfer of Personal Data outside of the UAE is also permitted where it is required in order to carry out obligations, establish rights before judicial authorities, defend claims, perform a contract between a Data Subject and a Controller or between a Controller and a third party to achieve the Data Subject's interest.

OTHER KEY PROVISIONS

- Controllers and Processors will have six months to comply with the Law starting as soon as the Executive Regulations are issued and come into effect.
- Any laws which would contradict the provisions of the Law will be repealed; and
- The Council of Ministers will issue a decision specifying the acts that constitute a violation of the Law and any applicable administrative sanctions and penalties (and their amounts).

KEY DEFINITIONS

- Automated Processing: Processing that takes place using a program or an electronic system that operates automatically, either completely independently without any human intervention or partially with limited human supervision and intervention.
- Biometric Data: Personal Data resulting from using specific technology relating to physical, physiological, or behavioral characteristics of Data Subject, which allows identification or confirmation of the unique identification of the Data Subject such as a facial image or fingerprint data.
- Consent: Consent that is provided by the Data Subject to a third party authorizing it to Process their Personal Data provided that this consent must be specific, clear and unambiguous as to the Processing of their Personal Data through a clear affirmative statement or action.

- Controller: The Establishment or natural person holding Personal Data, and by virtue of their activity determines the method, process and criteria for processing such Personal Data, the purpose of such processing, whether alone or jointly with other persons or Establishments.
- Cross-Border Processing: Publishing, using, displaying, transferring, receiving, retrieving, using, sharing, or Processing Personal Data outside the UAE.
- Data: An organized or unorganized set of data, facts, concepts, instructions, observations, or measurements in the form of numbers or letters, words, symbols, images, videos, signs, sounds, maps, or any other form, interpreted, exchanged, or processed by individuals or computers, including any information set out in the Law.
- Data Protection Officer: Any natural or legal person appointed by the Controller or Processor, to undertake the tasks of ascertaining that the entity to which they belong complies with the rules, conditions, and procedures for Processing Personal Data stipulated in the Law and ensuring the compatibility of such entity' systems and procedures in achieving compliance with the provisions of the Law.
- Data Subject: The natural person to whom Personal Data relates.
- Emirates Data Office: Emirates Data Office established by Federal Decree-Law No. 44 of 2021.
- Establishment: Any company registered inside or outside the UAE, including companies that are partially or wholly owned by the federal or local government.
- Personal Data: Any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, through the linking of data, by reference to an identifier such as their name, voice, picture, identification number, electronic identifier, geographical location, or one or more physical, physiological, economic, cultural, or social characteristics. Personal data includes Sensitive Personal Data and Biometric Data.
- Processing: Any operation or set of operations performed on Personal Data using any electronic means, including collecting, storing, recording, organizing, adapting, modifying, circulating, transforming, retrieving, exchanging, sharing, using, categorizing, or disclosing by transmitting, distributing, making available, formatting, merging, restricting, blocking, erasing, destroying, or creating models.
- Processor: The Establishment or natural person that processes Personal Data on behalf of the Controller under the Controller's direction and instructions.
- Profiling: A form of automated Processing that includes the use of Personal Data to assess certain personal aspects of the Data Subject. This includes analyzing or predicting the Data Subject's performance, financial status, health, personal preferences, interests, behavior, location, movements, or reliability.
- Sensitive Personal Data: Any data that directly or indirectly discloses a natural person's family, ethnic origin, political opinions, philosophical or religious beliefs, criminal record, Biometric Data or any data relating to the health of such person, including their physical, mental, genetic, or sexual health, including information relating to the provision of health care services which may reveal their health status.

This client alert is not intended to provide a comprehensive summary of all of the provisions of the Law. We recommend consulting with your lawyers to discuss the Law and the Executive Regulations (when published) and their impact on your business.

The K&L Gates Global Data Protection, Privacy and Security team remains at your disposal to analyze your data protection compliance with the Law and the Executive Regulations.

KEY CONTACTS

MOHAMMAD RWASHDEH
SPECIAL COUNSEL

DUBAI
+971.4.427.2742
MOHAMMAD.RWASHDEH@KLGATES.COM

ZAID ABU-SHATTAL
SENIOR ASSOCIATE

DUBAI
+971.4.427.2791
ZAID.ABU-SHATTAL@KLGATES.COM

