SCHLÜTER GRAF

Passion for Law

www.schlueter-graf.com

UAE's New Game Changing Federal Data Protection Law

Legal Briefing, 6 January 2022

On 20 September 2021, the United Arab Emirates ("**UAE**") issued a new data protection law, Federal Decree-Law No. 45/2021 ("**DP Law**"). This long-awaited development is in line with wider international practices in protecting the privacy of individuals and personal data. Prior, the UAE did not have a comprehensive data protection law at its federal level. This legal briefing shall provide an overview of the most notable features of the DP Law as well as the impact on UAE based businesses.

I. General

The DP Law will come into force on 2 January 2022. Executive Regulations are due to be issued within 6 months of the date of issuance of the DP Law (i.e., by 20 March 2022).

The DP Law provides a grace period of 6 months from issuance of the Executive Regulations for business to comply with the regulations (i.e., 20 September 2022). It includes the option for the Cabinet to extend the grace period.

At the same time as the DP Law, UAE Federal Decree-Law No. 44/2021 related to the creation of the Emirates Data Office was also issued. The Emirates Data Office ("**Data Office**") will act as the data protection regulatory authority, operationalizing the DP Law's requirements.

II. Applicability of the DP Law

The DP Law is designed to protect "personal data", which is "any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data". This expressly includes an individual's name, voice, picture, identification number, electronic identifier, and geo location. It also protects "sensitive personal data" which is data that directly or indirectly reveals the family or ethnic origin of a natural person, political or philosophical opinions or religious beliefs, criminal record, biometric data and any data relating to a natural person's health.

The Law applies to both data controllers and data processors, whereby the definitions are in line with the **EU General Data Protection Regulation** ("**GDPR"**).

Like GDPR, the DP Law's broad definition of personal data encompasses employee data and processing in the employment context.

Similar to GDPR and the recently issued Personal Data Protection Law of the Kingdom of Saudi Arabia ("**KSA**"), the DP Law is designed to have extra-territorial reach. It shall apply to any organisation that is established in the UAE and processes personal data of data subjects inside or outside the UAE, as well as any organisation that is established outside the UAE and processes personal data of data subjects inside the UAE.

The DP Law last does not apply to government data, government entities that control or process personal data, personal data held by security and judicial authorities or any processing of personal data for personal purposes, personal banking and credit data or health data, which are covered under separate laws.

Furthermore, the DP Law does not apply to companies located in free zones that have established their own data protection regulations (i.e., DIFC and ADGM).

The Data Office will have the authority to exempt certain companies from specific requirements of the DP Law in case they do not process a large volume of personal data. This will be further specified in the Executive Regulations.

III. Key Aspects of the DP Law

In general, the DP Law is consistent with international data protection laws. Local businesses need to be aware of the following key aspects:

1. Data Protection Principles

The Law borrows heavily from GDPR, mirroring many of its key concepts including the data protection principles, i.e., **(a)** to ensure data processing is made in a fair, transparent and lawful manner which means that **(b)** the purpose of collecting personal data must be clear and specific, **(c)** the personal data must be accurate, corrected or deleted if inaccurate, **(d)** kept only for as long as required based on the specific purpose and then either deleted or anonymized and **(e)** it shall be kept securely and protected from any breach, infringement, or illegal or unauthorized processing.

2. Legal Basis for Processing Activities

The default position is that consent is required for processing personal data of the data subject, whereby the DP Law includes certain exemptions from this principle, e.g., if the processing is necessary to protect the public interest or to perform a contract to which the data subject is a party.

Consent must be given in a clear, simple, unambiguous, and easily accessible manner, whether in writing or electronic form. This is consistent to the "opt in" consent required by GDPR.

Opt-out mechanisms are now mandatory in order to allow data subjects to withdraw their consent or object to receiving marketing communications.

"*Legitimate interest*" was not included as lawful basis for processing activities by the controller, which is a common basis provided in GDPR (Article 6(1)(f) of the GDPR). However, further legal basis and exemptions shall be provided by the Executive Regulations.

3. Controller & Processor Obligations

The DP Law has introduced obligations for data controller and data processor. Key obligations of data controllers are

- taking the appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure personal data (Art. 7.1)
- maintaining a special record of personal data ("Records of Processing Activity" "**RoPA**") and its protection measures and the obligation to provide this record to the Data Office whenever requested (Art. 7.4.)
- ensuring processors provide sufficient guarantees and implement technical and organizational measures necessary to meet the DP Law requirements.

Data processor key obligations are to process personal data in accordance with the controller's instructions and on the basis of an agreement. They also must apply appropriate technical and organizational measures and maintain a special record of the personal data processed on behalf of a controller.

The Executive Regulations shall specify the procedures, controls, conditions and technical standards related to the processor obligations.

4. Privacy Impact Assessment ("PRA")

Art. 21 of the DP Law implements the processor's obligation to assess the impact of the proposed processing of personal data, when using any modern technologies that would pose a high risk to the privacy and confidentiality of the personal data of the data subject. PRA's are mandatory in certain cases as defined by the DP Law.

5. Data Subject Rights

Also in line with GDPR the DP Law provides certain rights to data subjects, such as the right to access, the right to rectification or erasure of personal data (i.e. the right to be forgotten); right to data portability; the right to object to personal data processing (e.g. for marketing purposes); the right to restrict personal data processing and the right to object to automated processing that has legal consequences or seriously affects the data subject.

Data subjects can also file complaints with the Data Office.

Controllers are required to put in place a mechanism for communicating with data subjects.

6. Cross-Border Transfer of Personal Data

The DP Law allows for the cross-border transfer of personal data but differentiates between transfer of personal data to countries with and without an adequate level of protection.

Art. 22 allows cross-border data transfer outside the UAE to countries approved by the Data Office as having an adequate level of protection or where the specific country is a party to a bilateral or multilateral agreement relating to the protection of personal data.

Art. 23 designates several cases of cross-border transfer to countries without adequate level of protection, e.g., (a) transferring personal data under a contract that applies the requirements of the DP Law, (b) by way of explicit consent of the data subject to such transfer, (c) if the transfer is necessary for the execution of a contract between the controller and the data subject, (d) if the transfer is necessary for international judicial cooperation, (e) or if the transfer is necessary to protect the public interest.

It is not clear yet, whether the Data Office will issue a list of approved countries or whether companies need to seek approval from the Data Office on a case-by-case basis. Further details are expected to be included in the Executive Regulations.

7. Data Protection Officer (“DPO”)

Controllers and processors must appoint a DPO under certain circumstances that are further specified in the DP Law. The DPO can be based inside or outside the UAE and can either be an employee or an external party.

8. Personal Data Breach

The DP Law imposes a duty on controllers to report details of any breach that compromises the privacy, confidentiality, or security of data subjects’ personal data to the Data Office as well as to the affected data subjects in certain circumstances. Timelines and details required in such notifications will be further specified in the Executive Regulations.

Under GDPR controllers are only obliged to report data breaches that are “likely to result in a high risk” to the individuals’ rights and freedoms. Such a threshold is not specified in the DP Law.

9. Penalties

The DP Law does not specify the scope and level of penalties for breaches of the provisions of the DP Law. Administrative penalties can be imposed as part of a decision by the Cabinet in response to a breach of the Law or the Executive Regulations and based on a proposal from the Data Office.

IV. Summary & Recommendations

The DP Law provides various principles and requirements that mirror GDPR with certain differences as mentioned above.

The Executive Regulations are expected to clarify various aspects related to cross border transfer of data as well as the scope and level of penalties.

Much like the GDPR, implementing the DP Law is likely to be time-consuming and it is

recommended to begin the process now to avoid facing potential administrative sanctions.

UAE based companies (or companies based outside the UAE but process personal data of data subjects located in the UAE), that have not already developed a compliance framework in line with GDPR or have not extended it to their UAE-related data processing activities, should make use of the grace period and carry out a comprehensive data protection compliance program.

First steps that may be considered by all companies affected can be:

- Identify **compliance gaps** and address the respective risks;
- Evaluate current **consent management, privacy & cookie notices** and assess if adjustments are required;
- Evaluate how to develop and maintain a **RoPA process** that is compliant to the DP Law.
- Develop a **data breach & cyberattack response strategy**;
- Check if **cross-border data transfer** occurs and how it can be managed lawfully (i.e., map data flow and include in RoPA reports);
- Review **third-party onboarding processes** and contracts to include data privacy and security clauses and cross-border transfer provisions.
- Appointment of **DPO**, if necessary pursuant to the DP Law;
- Technical and organizational measures: assess **data privacy and information security by design tools** that can be used in order to comply with the controller (and processor) obligations under the DP Law, if not implemented yet (i.e., data subject rights automation, data breach management, autonomous documented accountability, PRA automation);
- Prepare **trainings** to raise awareness within the organisation.

How we can help

SCHLÜTER GRAF will continue to monitor the developments related to data protection laws in the UAE, including the forthcoming Executive Regulations. Our dedicated Data & Digital team has in depth experience working with clients to assess and develop data protection compliance frameworks. Please contact us to discuss how we can assist you.

SCHLÜTER GRAF Legal Consultants
ONE by Omniyat, Office P501, Business Bay,
P.O. Box 29337
Dubai, United Arab Emirates
Tel: +971 / 4 / 431 3060
Fax: +971 / 4 / 431 3050
Dounia Aghdoube, Associate Partner (aghdoube@schlueter-graf.com)

SCHLÜTER Rechtsanwälte PartG mbB
Dorotheenstr. 54, 22301 Hamburg
Tel: 040 / 380 755 75
Fax: 040 / 380 756 86
Anja Christine Adam, Partner
(a.adam@schlueter-law.de)