SCHLÜTER GRAF

Passion for Law

www.schlueter-graf.com

KSA's New Game Changing Personal Data Protection Law

Legal Briefing, 18 January 2022

On 24 September 2021, the Kingdom of Saudi Arabia ("**KSA**") has announced its first standalone personal data protection law **("DP Law")**, promulgated by Royal Decree No. M19/1443 (Cabinet Decision No. 98/1443). This long-awaited development is in line with wider international practices in protecting the privacy of individuals and personal data and extends beyond the general principles of privacy and individuals' personal data that are outlined under Sharia law. This legal briefing shall provide an overview of the most notable features of the DP Law as well as the impact on KSA based businesses and foreign business which are processing personal data of data subjects inside KSA.

I. General

The DP Law will come into force on 23 March 2022. Implementing Regulations are due to be issued within 180 days of the date of issuance of the DP Law (i.e., by 23 March 2022).

The DP Law provides a grace period of 1 year from the effective date (i.e., 22 March 2023) for businesses to achieve compliance. It includes the option for the competent authority to extend the grace period.

The DP Law appoints the Saudi Data & Artificial Intelligence Authority (**SDAIA**") as competent authority for a period of 2 years and thereafter may transfer the supervisory function to the National Data Management Office ("**NDMO**").

In the meantime, it is not clear if the "Personal Data Protection Interim Regulations" and the "Data Sharing Interim Regulations" (both together "**Interim Regulations**"), which were published by the NDMO prior to enactment of the law, are still valid or if these were repealed by the DP Law. The Interim Regulations cover principles such as accountability, transparency, data disclosure, and data subject rights, data security, legal basis, and ethical data use.

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, address, contact number, identification number, records, personal property, bank account & credit card numbers, videos and pictures or any other data of personal nature.

It also protects "*sensitive personal data*" which is data that directly or indirectly reveals the ethnic or tribal origin of a natural person, political or philosophical opinions or religious beliefs, criminal or security records, biometric data, genetic data, health data, credit data, location data and data that indicates that both parents of an individual or one of them is unknown.

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 United Arab Emirates, the DP Law is designed to have extra-territorial reach. It shall apply to any organisation that is established in KSA

and processes personal data of data subjects inside KSA, as well as any organisation that is established outside KSA and processes personal data of data subjects inside KSA.

The DP Law last does not apply to the processing of personal data for personal and family use.

The DP Law is without prejudice to the authority of the National Cybersecurity Authority ("**NCA**"). The Council of Ministers' approval in the DP Law also notes that SDAIA will coordinate with the Saudi Central Bank and Communications and Information Technology Commission ("**CITC**") to address the application of the DP Law to regulated financial institutions and information & communication technology service providers ("**ICT**"). The DP Law further indicates that regulations will be issued in respect of the processing of "health" and "credit data".

III. Key Aspects of the DP Law

Even though the DP Law is consistent with several principles included in international data protection laws, it presents challenges to businesses operating within KSA in some major areas. Concerned businesses need to be aware of the following key aspects:

1. Data Protection Principles

The DP Law mentions certain data protection principles similar to GDPR, such as "*Purpose Limitation*", "*Relevance*", "*Fairness & Transparency*" and "*Data Minimization*".

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., **(a)** if the processing achieves a "real interest" for the data subject and communication with the data subject is otherwise impossible or difficult, **(b)** the processing is being conducted based on an agreement to which the data subject is a party, **(c)** the controller is a government entity and the processing is required for security purposes or to justify judicial requirements.

Furthermore, personal data may be collected without consent for scientific research or statistical purposes if it is anonymized.

Additionally, the DP Law stipulates that personal data shall only be collected directly from the data subject, including exemptions from this principle, e.g., **(a)** where the data subject agrees to such collection, **(b)** if the personal data is publicly available, **(c)** the controller is a government entity and such collection is for security purposes or to satisfy judicial requirements, **(d)** the data subject's vital interests would be harmed if their personal data is not collected from such other person, **(e)** the collection is necessary to protect public health or safety, or to protect the life or health of a specific individual, or if **(f)** the personal data is anonymized.

The Implementing Regulations will specify the conditions of the required consent and it is expected that the conditions will be equivalent to the definition of consent under GDPR.

As of now, "*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).

The data subject has the right to withdraw consent at any time and the Implementing Regulations will specify requirements for such withdrawal process.

3. Data Subject Rights

In line with GDPR the DP Law provides certain rights to data subjects, such as **(a)** the right to be informed, **(b)** the right to access, **(c)** the right to rectification, completion and update of personal data, **(d)** the right to erasure (destruction) of personal data (i.e., *the right to be forgotten*).

Response times to such requests will be specified in the Implementing Regulations and additional rights may be included in the Implementing Regulations. Data subjects

can file complaints with SDAIA. Controllers therefore will be required to put in place a mechanism for communicating with data subjects.

In addition, data subjects may seek compensation for violations of the DP Law for "*material or moral damage in proportion to the extent of the damage*".

4. Controller Obligations

SDAIA intends to establish a national registry of controllers. All controllers will be required to register through a publicly available portal and controllers who are private entities or private individuals will be required to pay an annual fee of a maximum of SAR 100,000.

Controllers further must provide the data subject with information related to the **(a)** legal justification for collection, **(b)** the type of data collected, **(c)** the purpose of collection, **(e)** the entities to which the personal data will be disclosed and their capacity, **(f)** whether the personal data will be transferred, disclosed, or processed outside KSA, **(g)** the collection and storage method and the means of processing, **(h)** manner by which the personal data will be destroyed and **(i)** the rights of data subjects, and details of how such rights can be exercised. This requirement can be fulfilled by providing a "privacy notice" to which the data subject must have access prior to collection of personal data.

Controllers must further **(a)** implement necessary organizational, administrative and technical measures and means to ensure that personal data is protected, **(b)** conduct privacy risk assessments ("**PRA**"), and **(c)** choose processors that are compliant with the requirements of the DP Law and constantly verify compliance of such processors, whereby the Implementing Regulations will provide further guidance and details.

The DP Law requires controllers to maintain a "**record of processing activities**" ("**RoPA**") for a period to be specified by the Implementing Regulations, which must include **(a)** the purpose of the processing, **(b)** entities to which the personal data was or will be disclosed, **(c)** whether the personal data was or will be transferred outside of KSA and **(d)** the expected retention period.
In addition, controllers are required to hold data privacy trainings for their employees.

The DP Law does not provide provisions for data processors. This may be included in the Implementing Regulations.

5. Cross-Border Transfer of Personal Data

Transfers of data or disclosure of data outside of the Kingdom may be made for limited explicit purposes, i.e., **(a)** extreme necessity to preserve the life of a data subject outside of KSA, **(b)** to prevent, examine or treat a disease; **(c)** if the transfer is in implementation of an obligation under which the KSA is a party, **(d)** to serve the interests of the Kingdom, or for **(e)** "other purposes" subject to the forthcoming Implementing Regulations.

Even if the above is met, controllers need to comply with further conditions, such as **(a)** the transfer or disclosure does not prejudice national security or the vital interests of the Kingdom, **(b)** there are sufficient guarantees for preserving the confidentiality of the personal data to be transferred or disclosed, so that the standards are not less than the standards in the DP Law and the Regulations, **(c)** the transfer or disclosure must be limited to the minimum personal data needed; and **(d)** SDAIA approves the transfer or disclosure, as determined by the Implementing Regulations.

Notably, the approval requirement goes far beyond GDPR transfer restrictions.

6. Data Protection Officer ("DPO") & Local Representative

The DP Law does not specifically mention the appointment of a DPO, however it does require controllers to appoint or assign at least one of their employees to be responsible for achieving compliance with the DP Law.

Furthermore, any foreign company without a legal presence in KSA that processes the personal data of data subjects within KSA

must appoint a local representative, licensed for that purpose. SDAIA will determine when this requirement will come into effect and this requirement can be postponed for a maximum of 5 years from the effective date of the DP Law.

7. Personal Data Breach

Breaches, leakages, or other unauthorized access to personal data must be notified to SDAIA "immediately," and, under certain conditions, to the data subjects as well.

8. Penalties

The law contains penalties for violations, including

- imprisonment of up to two years and/or a fine up to SAR 3,000,000 for anyone who discloses or publishes Sensitive Data in violation of the Law
- imprisonment of up to one year and/or a fine up to SAR 1,000,000 for anyone who violates the general prohibition on transfers of personal data outside Saudi Arabia
- a warning or fine up to SAR 5,000,000 for any other violations of the Law, which fine may be doubled if repeated

IV. Summary & Recommendations

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

The Implementing Regulations are expected to clarify various aspects, such as cross border transfer of data, registration requirements, upload of records of processing activities to the SDAIA portal etc.

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

The DP Law provides a major challenge for companies that transfer personal data outside KSA. In case the Implementing Regulations will not provide for exemptions or mechanisms (e.g., lists of approved countries with adequate level to protection or transferring personal data under a contract that applies the requirements of the DP Law) to transfer personal data outside KSA, businesses will need to evaluate the option of creating a data hub inside of KSA.

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.

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.
- 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 process** and contracts to include data privacy and security clauses and cross-border transfer provisions.
- Appointment of **DPO/Local Representative**, if necessary pursuant to the DP law;
- Develop **data breach & cyberattack response strategy**;
- 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 KSA, including the forthcoming Implementing Regulations. Our dedicated data privacy 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)