SCHLÜTER GRAF

Passion for Law

www.schlueter-graf.com

The Implementing Regulations to KSA's Personal Data Protection Law

Legal Briefing, 6 October 2023

A significant milestone for privacy and data security in *the Kingdom of Saudi Arabia (**"KSA"**)* was achieved with the entry into force of *the Personal Data Protection Law ("**DP Law**") in September 2021.*[1] *On 7 September 2023 the long-awaited Implementing Regulations of the DP Law (**"DP Implementing Regulations"**) were issued through* the Administrative Decision No. 1516/1445. The DP Implementing Regulations provide in 38 articles several clarifications on conditions and procedures regarding the new DP Law. This Legal Briefing aims to summarize the essential aspects of the DP Implementing Regulations.

A. Main Features of the DP Implementing Regulations

The DP Implementing Regulations further defines certain obligations and mechanisms under the DP Law:

1. Obligations of the Controller

Generally, the controller is obliged to take all the necessary organizational, administrative, and technical measures to ensure the security of personal data and the privacy of its subjects.

As the DP Law has included the right to request the controller to provide the data in a readable and clear format, the DP Implementing Regulations oblige the controller to execute this request within a period of not exceeding thirty days without delay. He is also obliged to adopt the necessary technical, administrative, and organizational means to ensure a prompt response. Furthermore, the controller must document and save all requests submitted by a personal data subject, including verbal requests. This means personal data owners have the right to submit their request to the controller verbally.

2. Form and Contents of a valid Consent

The controller has the option to secure the personal data subject's consent for data processing through various suitable methods, such as written or verbal agreements or electronic approaches. However, the consent must be freely given, the purpose of data processing must be clear, specific, and communicated to the personal data subject before requesting consent. Additionally, it is required that the consent is given by a legally competent person, is well documented, and obtained for each processing purpose.

Finally, personal data subjects have the right to withdraw their consent anytime. The controller must therefore establish clear withdrawal procedures and make them as easy or easier than the consent gathering process. Once the consent is revoked, the controller must immediately stop processing.

3. Legitimate Interest

The DP Law allows for data processing without consent in certain limited cases, namely based on 'legitimate interest'. According to the DP Implementing Regulations, processing for legitimate interest must meet the following criteria: The purpose of data processing may not break any of the laws in the Saudi Arabia. A balance between the rights and interests of the personal data subject and the interests of the controller must be ensured so that the interests of the controller do not infringe on the rights and interests of the personal data subject; the data processing shall not include sensitive data.

4. Direct Marketing

To engage in processing personal data for advertising and direct marketing purposes, obtaining consent is mandatory. Additionally, controllers must offer a straightforward and simplified method for data subjects to opt out of

[1] https://www.schlueter-graf.com/en/detail/ksas-new-game-changing-personal-data-protection-law/

receiving advertising and marketing materials whenever they wish.

5. Records of Personal Data Processing Activities

According to the DP-Implementing Regulations controllers are required to maintain a Record of Processing Activities (ROPA) both during the period of their involvement in the pertinent processing activities and for an additional five years after the conclusion of said processing activities. Furthermore, the DP-Implementing Regulations point out the necessary details to be included into such a ROPA-System.

6. Personal Data Breach Notification

The controller is obliged to notify the Saudi Data & Artificial Intelligence Authority (SDAIA) within a period of 72 hours upon discovery of a breach, i.e., leak or damage of personal data. The notification must contain a description of the incident, including the number of data subjects and type of personal data affected and the risks associated with the incident. Also, the controller shall, without undue delay, notify the personal data subject of the breach.

7. Data Protection Officers (DPO)

The controller must designate one or more Data Protection Officers for safeguarding personal data in any of the following scenarios: (1) If the controller is a public entity offering services that involve significant-scale data processing. (2) When the Controller's main operations involve processing activities that require constant and systematic monitoring of data subjects. (3) If the primary focus of the controller's activities is processing sensitive personal data.

B. Timeline & Next Steps

With publication on 7 September 2023, the DP Implementing Regulations have already come into force. Since the DP Implementing Regulations specify the DP Law, businesses have time to comply with the DP Implementing Regulations within a one-year grace period (till mid-September 2024).

Steps that companies must consider:

- Identify and address **compliance gaps** and associated risks.
- Evaluate current consent management, privacy, and cookie notices.
- Establish and maintain a **RoPA** process (Record of processing activities) that is compliant with DP Law.
- Review **third-party** onboarding for data privacy and security.
- Appoint a **DPO**, if necessary pursuant to to the DP Law.
- Create and develop a strategy for addressing **data breaches** and **cyberattacks**.
- Evaluate **tools** for data privacy and security compliance.
- Develop **training prAograms** to boost awareness withing the organization.

SCHLÜTER GRAF continuously monitors the legal developments related to data protection laws in KSA and the GCC. Please feel free to reach out to our dedicated KSA & data privacy team to better assist you with your queries.

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
Andrés Ring (Andres.Ring@schlueter-graf.com)
Dr. Amir Makee Mosa (Amir.Makeemosa@schlueter-graf.com)