SCHLÜTER GRAF

Passion for Law

www.schlueter-graf.com

Data Protection in Saudi Arabia: An Overview of the New Rules for Appointing Data Protection Officers (DPOs)

Legal Briefing, 11.09.2024

Introduction

In line with the rapid global developments in data protection and privacy regulations, Saudi Arabia has introduced a comprehensive framework through its Personal Data Protection Law ("PDPL"; Saudi Arabia Cabinet Decision No. 98/1443; Saudi Arabia Royal Decree No. M19/1443 on the Approval of the Personal Data Protection Law and Saudi Arabia Cabinet Decision No. 604/1444 on the Approval of the Amendments to the Personal Data Protection Law). Following the publication of the Implementing Regulations of the PDPL (Saudi Arabia Administrative Decision No. 1516/1445), the Saudi Data & AI Authority ("SDAIA") has now issued specific rules for appointing Data Protection Officers ("DPO") under Article 30 (2) of the PDPL (the "Rules"). These Rules are aimed at enhancing personal data protection and ensuring compliance with local and international standards. This article provides an in-depth overview of these Rules, including their purpose, scope, and the critical requirements for appointing a DPO in Saudi Arabia.

Purpose of the Rules

The Rules issued by SDAIA serve several crucial objectives. First and foremost, they establish minimum requirements for the appointment of a DPO. In addition to setting qualifications, the Rules offer clarity on the circumstances in which the appointment of a DPO is mandatory. Furthermore, they define the roles and responsibilities of the DPO, ensuring organizations implement the PDPL and its accompanying regulations effectively.

The overall aim is to create a system of accountability and compliance in the processing of personal data, ensuring that data controllers (organizations handling personal data) have professionals in place to oversee and protect the privacy rights of data subjects.

Key Definitions

As per Article 1 of the Rules, the terms and phrases mentioned adhere closely to the definitions laid out in Article 1 of the PDPL. This ensures that the regulations are synchronised and prevents contradictions. Some of the key terms include:

- **Competent Authority**: The Saudi Data & AI Authority (SDAIA), which is responsible for overseeing the implementation and enforcement of the PDPL.
- **Data Protection Officer (DPO)**: A person appointed by the data controller to oversee compliance with the law and handle matters related to personal data protection. This individual can be an employee or an external contractor.
- **Core Activities**: Refers to the activities essential to achieving the primary objectives of the controller, particularly when these involve the processing of personal data.

These definitions form the foundation of the Rules and are essential for understanding the appointment process of a DPO.

Scope of Application

The Rules apply as per Art. 3 of the Rules to all data controllers ("Controller") governed by the PDPL and its implementing regulations. A Controller, in this context, refers to any entity or organization that determines the purpose and means of processing personal data. This includes both public and private entities, depending on the nature and scale of their operations. The Rules explicitly mention that organizations must appoint DPOs when engaging in certain types of data processing activities.

Mandatory Appointment of a DPO

In particular, the Rules outline three specific cases in which a data controller must appoint a DPO. As per Article 5 of the Rules, the Controller shall appoint one or more individuals to be responsible for protection of personal data in any of the following cases:

1. **Public Entities**: If the controller is a public entity and processes personal data on a large scale, it must appoint a DPO. The question of what constitutes a 'large scale' depends on the circumstances of the individual case. It can be determined by factors such as the number of data subjects, the volume of personal data processed, and the geographical scope of the processing activities.

2. **Core Activities Involving Regular and Systematic Monitoring**: If the organization's core activities involve regular and systematic monitoring of data subjects, a DPO is required. This includes activities like tracking personal data through wearables or monitoring behavioural patterns through cookies and location tracking technologies. Relevant industries are e.g. telecommunications, health services or insurance, where large amounts of personal data are routinely processed.

3. **Sensitive Data Processing**: If the core activities involve processing sensitive personal data (such as health, financial, or genetic information), a DPO must be appointed. In contrast to point 2, no regular and systematic monitoring is necessary here, so the one-time processing of sensitive data within the meaning of Art. 5 of the Rules is sufficient to make the appointment of a DPO necessary.

Requirements for Appointing a DPO

Furthermore, to ensure a high standard of personal data protection, the Rules mandate that DPOs meet the following qualifications as stated in Art. 4 of the Rules:

The DPO must possess appropriate academic qualifications and experience in personal data protection. Again, it will depend on the circumstances of the individual case to decide whether the qualification or professional experience is sufficient.

The DPO should be also proficient in risk management practices, particularly in managing personal data breaches and several other incidents. In addition, sufficient understanding of the regulatory landscape is essential, including both the PDPL and any other relevant laws. Furthermore, the DPO should be of high integrity, without any prior convictions related to dishonesty or breach of trust.

An important sentence is contained in Art 4 (2) of the Rules: The DPO can be an internal employee of the controller or an external contractor. This flexibility allows organizations to hire experts either within or outside their operational structure, depending on their size and resources.

Lastly, the appointment must also be documented, both when appointing an internal DPO and when appointing an external DPO, Art. 6 of the Rules. If the DPO is an internal employee, their appointment must be

documented, while external contractors must sign a formal agreement. Moreover, organizations are required to notify SDAIA of the DPO's contact details upon appointment through the National Data Governance Platform.

Roles and General Responsibilities of the DPO

In terms of content, it is important to understand what the tasks and responsibilities of a DPO regarding the Rules are. The DPO's primary responsibilities extend beyond simply ensuring compliance. The DPO plays a pivotal role in aligning the organization's operations with the PDPL and international best practices, especially as Saudi Arabia integrates more deeply with global data protection standards and cross-border data transfers. Rather, as per Art. 8 of the Rules they are required to:

- **Provide support and advice** on all aspects of personal data protection, including the development of internal policies and procedures.
- **Conduct awareness and training** programs for employees, ensuring they understand the principles of data protection and the ethical handling of personal data.
- **Review incident response plans**, ensuring that data breach response mechanisms are effective and up to date.
- **Prepare reports** on data protection activities within the organization, providing recommendations to ensure ongoing compliance with the PDPL and the Implementing Regulations.
- **Monitor regulatory developments** and inform relevant departments within the organization of any changes that may affect compliance.

The Rules also contain in Art. 9 general provisions aimed at ensuring the effective operation of the DPO. These additional regulations ensure that the DPO carries out its work properly and that the objectives of the PDLP, the Implementing Regulations and the Rules are realised. Regarding this, the following points should be noted:

- **Independence**: The controller must ensure that the DPO's tasks are independent and free from conflicts of interest.
- **Training and Development**: Organizations are encouraged to provide continuous training and professional development to their DPOs to enhance their efficiency.
- **Periodic Reviews**: Organizations must periodically assess whether they are still required to have a DPO, as their operations evolve.

Responsibilities of DPO in Cross-Border Data Transfers

In addition to the above, one of the most significant responsibilities of a DPO is overseeing cross-border data transfers, which are also heavily regulated under the PDPL. Saudi Arabia's approach to cross-border data transfers mirrors comparable data protection regulations such as the General Data Protection Regulation (GDPR) in Europe. Like there, companies and organizations in Saudi-Arabia are also to be instructed to implement appropriate safeguards when transferring personal data outside the country. This is especially important for multinational corporations and companies with international operations, as the movement of data between jurisdictions is often necessary for business operations.

The DPO is tasked with ensuring that any cross-border data transfer complies with the conditions set forth in the PDPL, which may include obtaining the consent of the data subject or ensuring that the receiving country has adequate data protection laws in place. In cases where these conditions are not met, the DPO must take measures to implement

additional safeguards, such as binding corporate rules or standard contractual clauses, to ensure the security and privacy of personal data being transferred abroad. This responsibility places the DPO at the center of the organization's global data strategy, making their role even more critical in ensuring compliance with both local and international regulations.

Penalties for Non-Compliance

Failure to nominate a DPO or incorrect nomination in accordance with the above requirement will result in a breach of the Rules and the PDPL. This non-compliance can result in significant financial penalties, reputational damage, and legal consequences. The PDPL allows SDAIA to impose fines for breaches of the law, and organizations that fail to appoint a DPO may face severe repercussions.

Additionally, businesses that engage in high-risk data processing without a DPO may be subject to heightened scrutiny from regulatory authorities. This could result in audits, investigations, or even the suspension of certain data processing activities until compliance is achieved. To avoid these outcomes, businesses must take proactive steps to comply with the DPO appointment Rules and ensure that their data protection frameworks are fully aligned with the PDPL.

Conclusion

The appointment of a Data Protection Officer is now an integral part of ensuring compliance with Saudi Arabia's Personal Data Protection Law. These new Rules set a robust framework for safeguarding personal data, reinforcing Saudi Arabia's commitment to aligning with global data protection standards. By clearly defining the roles, qualifications, and responsibilities of DPOs, SDAIA provides tools to navigate the complex landscape of data privacy. As organizations in Saudi Arabia grow increasingly data-driven, the role of the DPO will become ever more crucial in upholding the values of transparency, accountability, and respect for individual privacy.

SCHLÜTER GRAF Legal Consultants LLC
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
Julian Steimer, Associate (julian.steimer@schlueter-graf.com)