waystone | Compliance Solutions

Data protection regimes: KSA, ADGM, DIFC and onshore UAE – a comparison

A key consideration for United Arab Emirates ("UAE") firms with a presence in the Kingdom of Saudi Arabia ("KSA"), is understanding the difference between the data protection regimes.

In the UAE, firms may be required to comply with the Abu Dhabi Global Market Data Protection Regulations 2021 ("ADGM DPR"), the Dubai International Financial Centre Data Protection Law (DIFC Law No. 5 of 2020) ("DIFC DPL") or the UAE Federal Decree Law No. 45 of 2021 on Personal Data Protection ("UAE PDPL"), amongst other UAE laws related to data protection and privacy.

There remains a question mark around the UAE PDPL; while it came into force on 2 January 2022, the Executive Regulations are yet to be released and, therefore, it is not possible to assess the details at this stage. Once the Regulations are released, firms will have six months to comply.

Firms crossing multiple jurisdictions will need to conduct a comprehensive gap analysis. As a starting point, we have set out below a high-level overview.

The KSA Personal Data Protection Law ("KSA PDPL") was released in September 2021, and amended in March 2023 following a public consultation. The Implementing Regulations released on 7 September 2023 set out the details which entities processing personal data must abide by. The KSA PDPL and Implementing Regulations are collectively referred to throughout as KSA PDPL.The Saudi Data & Artificial Intelligence Authority ("SDAIA") is the regime's supervisory body, however, there are interactions with several other government bodies.

The Saudi Data & Artificial Intelligence Authority ("SDAIA") is the regime's supervisory body, however, there are interactions with several other government bodies.

14 September 2024 deadline

The effective date of the regulations is 14 September 2023, and a one-year grace period has been granted for entities to comply with the law and regulations. Firms with a presence in KSA should be aware of the impending deadline of 14 September 2024.

As detailed in the Implementing Regulations, further rules are expected concerning the appointment of Data Protection Officers ("DPOs"). We should also expect the release of the list of jurisdictions considered to have an adequate level of protection for personal data when it is transferred outside the Kingdom and the Standard Contractual Clauses ("SCC").

A public consultation was released by SDAIA on 19 March 2024 proposing amendments to the Regulation on Personal Data Transfers outside of KSA. The amendments aim to clarify the provisions and detailed procedures concerning personal data transfers outside of KSA. The deadline for the public to respond to the proposals is 18 April 2024, therefore we can expect the release of the updated Implementing Regulations during Q2 or Q3 of 2024.

Similarities between the regimes

When global jurisdictions update their existing data protection regimes, they often follow well-known international standards such as the General Data Protection Regulations ("GDPR") in Europe. The KSA PDPL is no different, containing similar concepts to those seen in the GDPR, making the KSA PDPL, ADGM DPR, and DIFC DPL very similar.

While we cannot go into the details of the UAE PDPL at this stage, we can advise that the Law borrows heavily from the GDPR, reflecting many of its key concepts including the data protection principles.

Key differences to be aware of

Records of Processing Activities ("ROPA")

The KSA PDPL outlines the information to be included in a ROPA, such as the purposes of the data processing and the description of the data categories being processed, amongst other information that we would usually expect to be included.

However, unlike other data protection regimes, the KSA PDPL specifies that a data controller must keep a ROPA during the period that it engages in the relevant processing activities and a further five years from the date of completion of the processing.

Data subject rights

The right to be informed, to access, to correct, to delete and to restrict are consistent across the three regimes. The following rights are not mentioned within the KSA PDPL:

- right to object
- right to data portability
- right to not be subject to fully automated decision-making, including profiling
- right to non-discrimination.

Data subject requests

As with the DIFC DPL, under the KSA PDPL data controllers are obligated to act on a request from a data subject within 30 days. The initial period can be extended up to an additional 30 days should the response require disproportionate effort, or if the controller receives multiple requests from the data subject.

Under the DIFC DPL the extension may be for a further 60 days where the request is particularly complex, or requests are numerous.

The ADGM allows an initial period of 60 days, with an extension of 30 days for complex requests or where the controller is handling numerous requests, whether related or not.

In all jurisdictions there is the option to refuse to act on a request where necessary, and where the rules allow for this, for example, where a request is repetitive, manifestly unfounded, or requires disproportionate efforts.

Legal basis

One of the key differences we observe between the regimes is in relation to the legal bases available for processing data. The KSA PDPL has fewer legal bases to choose from and the definition of legitimate interest is narrower. A legitimate interest impact assessment must also be completed if relying upon this.

In general, the KSA PDPL requires that consent be obtained from a data subject prior to processing their data, unless a suitable exception can be relied upon. These exceptions include situations where:

- the processing of the data would result in an actual interest to the data subject and the data subject cannot be practically or possibly contacted
- the processing is mandated by law or by a prior agreement to which the subject is a party
- the data controller is a public entity, and the processing of data is essential for security or judicial purposes
- the processing is necessary and in the legitimate interests of the data controller or another party, provided that it does not prejudice the rights of data subjects.

The KSA PDPL distinguishes between situations requiring 'explicit consent' and those requiring 'implied consent' based on the types of data collected and the processing purposes. Implied consent is required to process personal data for direct marketing purposes. Explicit consent is required by controllers who wish to process sensitive data, as well as for automated processing.

Data processors and transfers

Each of the regimes requires controllers who engage data processors to enter into appropriate agreements with those processors. However, unlike the DIFC DPL and ADGM DPR, the processor must confirm that they are not subject to any other regulations in any other countries that impact their ability to comply with the PDPL. If a processor violates the instructions issued by the data controller or the processing agreement, the processor shall be considered a data controller and held directly accountable.

The regimes are aligned in considering countries as either adequate or non-adequate in terms of the level of protection offered to personal data. If a transfer is made to a non-adequate jurisdiction, further safeguards are required such as binding common rules, standard contractual clauses, certifications of compliance and binding codes of conduct. In addition to these safeguards, derogations are also available which can be relied on to make cross-border transfers to non-adequate countries.

The amendments proposed by the SDAIA to the Regulation on Personal Data Transfers outside of KSA focus on the following topics:

- alternative purposes of transfer or disclosure of personal data to entities outside KSA
- procedures and standards for assessing the protection level for cross-border personal data transfers
- scenarios in which where controllers may be exempt from safeguarding and minimising personal data transferred

- subsequent transfer of personal data
- cases where the Competent Authority might revoke a previously issued exemption granted to a data controller
- assessment of risks of transferring/disclosing personal data to an entity outside KSA.

We will provide further analysis on any updates to the implementing regulations in due course.The proposed amendments can be found here. Feedback via this link is encouraged until 18 April 2024.

Data breach notifications

In line with the ADGM DPR, the KSA PDPL requires data controllers to notify personal data breaches to the supervisory authority within 72 hours of becoming aware of the breach and must notify data subjects without undue delay.

This differs slightly to DIFC DPL, which does not specify a 72-hour time frame but requires that the supervisory authority be notified as soon as practicable in the circumstances. However, in keeping with the above, the breach should be communicated to an affected data subject as soon as practicable.

The threshold for reporting a breach to the supervisory authorities appears to be similar; a breach is reportable to the supervisory authority and data subjects where it may cause harm to the personal data, or conflicts with their rights or interests.

Advertising and direct marketing

This area is one of the significant differences between the regimes. The KSA PDPL confirms that consent is required to process personal data for advertising and direct marketing purposes. Controllers must also provide an easy and simplified mechanism to enable data subjects to stop receiving advertising and marketing materials at any time. We expect that further guidance will be provided in due course to clarify the distinction between advertising under Article 28 and direct marketing under Article 29.

DPO appointments

The KSA PDPL and ADGM DPR are largely aligned when it comes to the mandatory appointment of a DPO. DPOs must be appointed by public bodies and where the core/primary activities of the data controller consist of processing that requires:

- regular and systematic monitoring of individuals on a large scale
- processing of sensitive personal data.

A further significant point is that the ADGM DPR states that with ‘large scale’ processing of special category data the rules relate to both data processors and controllers, whereas the KSA PDPL DPO requirement relates only to data controllers.

The DIFC DPL requires DIFC bodies to appoint a DPO. Data controllers and processors performing High-Risk Processing Activities (as per the DIFC DPL definition) on a systematic or regular basis, must also appoint a DPO.

In all cases, entities may choose to appoint a DPO internally or to engage a third-party company that provides DPO services. The Competent Authority, currently the Saudi Data & AI Authority (“SDAIA”), shall issue rules for the appointment of the DPO, which shall include the circumstances under which a DPO shall be appointed.

What changes do businesses need to implement:

- **training –** ensure all employees involved in processing operations are trained on the KSA PDPL so that they are aware of their obligations
- **gap analysis –** assess your current data processing activities to understand the impact of the KSA PDPL and what changes within the business would need to be taken to ensure compliance with the law
- **develop policies and procedures –** this may mean adapting your existing framework or introducing new policies and procedures
- **DPO –** consider whether you are required to appoint a DPO; many firms choose to appoint a DPO voluntarily to manage the data protection function, ensuring compliance with the law
- **transfer assessments –** where controllers will be transferring personal data outside of the business, they will need to consider whether that third country is an adequate country, whether safeguards will need to be implemented, or if an exemption is available
- **monitor and review –** additional clarification and sectoral laws are expected to be published as the grace period comes to a close and it is therefore critical for businesses to continue to monitor developments within this space.

How Waystone Compliance Solutions can help

Waystone has assisted many clients with their data protection requirements, including implementing complex, multi-jurisdictional data protection frameworks, advising on cross-border transfers, incorporating data protection principles, and drafting suitable documentation as per the relevant data protection regulations and laws.

Waystone is well-positioned to support you in implementing or maintaining a compliant data protection framework. We can also, where required, provide experienced, outsourced DPOs, or educate and train your in-house DPO on the regulatory requirements. If you would like to find out more about how we can assist your firm, please reach out to your usual Waystone representative, or contact us below.

Contact Us