The Latest Developments in Data Privacy Across African & Middle Eastern Countries

2025 Joint Article by ALFA International's African & Middle Eastern Regional Group

BAHRAIN

Charles Russell Speechlys

Bahrain has the Personal Data Protection Law (PDPL) No. 30 of 2018, which came into effect on 1 August 2019.

The PDPL establishes comprehensive regulations for the processing of personal data in Bahrain, aiming to protect the privacy of individuals and ensuring the responsible handling of their personal information. The PDPL aligns with other established standards for data protection, such as GDPR, and reflects a growing emphasis on the protection of personal information.

The key aspects of the PDPL include:

- Scope & Applicability – PDPL applies to any processing of personal data within Bahrain, as well as processing outside of Bahrain if such processing is related to individuals in Bahrain;
- Data Protection Principles – these include fairness, transparency, purpose limitation, data minimisation, accuracy and security;
- Rights of Data Subjects – including the right to access their personal data, right to request correct or deletion of inaccurate data and right to object to types of data processing;
- Consent – explicit consent required for data processing of personal data (unless processing is necessary for legal compliance, legitimate interests or contractual obligations);
- Controller & Processor Obligations – responsibilities for both, including ensuring adequate measures to protect personal data and compliance with PDPL;
- Transfers – transfers are restricted unless conditions are satisfied, such as requisite levels of protection in the receiving country and obtaining data subject consent;
- DPA – the Data Protection Authority, responsible for overseeing compliance, enforcing the PDPL and handling complaints;
- Penalties – non-compliance can result in significant fines and penalties.

DUBAI

Kochhar & Co Inc.

UAE has data protection laws in place. The primary legislation governing data protection in the UAE is the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the "**PDPL**").

Additionally, certain free zones in the UAE, such as the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM), have their own data protection regulations, which align with international standards like the EU's GDPR

The PDPL establishes a comprehensive framework to ensure the confidentiality of information and protect individuals' privacy within the UAE. It outlines the governance for data management and protection and defines the rights and responsibilities of all parties involved. The law came into effect on 2 January 2022. The PDPL requires businesses to implement strong measures to protect personal data, including obtaining consent from individuals for data processing, ensuring transparency, and providing individuals with rights over their personal data, such as access, withdrawal, correction, and deletion.

The executive regulations to the PDPL ("**Executive Regulations**") were due to be published within six months of the PDPL's issuance; however, they have not yet been published. Once the Executive Regulations are issued, organizations will have a further six months from the date of issuance to adjust their operations and ensure compliance.

EGYPT

Al-Hamad Legal Group

Does the Arab Republic of Egypt have data protection laws?

Egypt Law No. 151/2020 Promulgating the Law on the Protection of Personal Data Law (PDPL), issued on the 17th of July 2020 establishes a comprehensive legal framework to protect the personal data of individuals in Egypt. It regulates data collection, processing, storage, and transfer, and creates a central authority responsible for enforcement: the **Personal Data Protection Center (PDPC)**.

The PDPL mandates that data Controllers and Processors register with the Egyptian Data Protection Authority (**DPA**). This registration requires providing details about data processing activities, which include cloud storage usage.

The PDPL has set forth that personal data cannot be processed without the explicit consent of the data subject, except in specific circumstances outlined by the law. Therefore, collecting geospatial data that includes personal information, such as street view imagery capturing identifiable individuals or private properties, requires obtaining prior consent from those individuals.

The PDP applies to any person (Egyptian or foreign) who processes personal data electronically, even outside Egypt if the data involves Egyptians or residents. However, it exempts personal and household use, statistical and legal use, journalistic use (under specific conditions), national security, judicial, and Central Bank purposes (with exceptions).

Key Provisions of Law No. 151/2020

Conditions for Personal Data Collection

Personal Data may not be collected, processed, disclosed, or revealed by any means except with the explicit consent of the Data Subject or in cases permitted by law. The Data Subject shall have the following rights:

1. Having knowledge of, reviewing, accessing, and obtaining Personal Data belonging to them which is held by any Holder, Controller, or Processor;
2. Reversing the prior consent concerning the retention or Processing of their Personal Data;
3. Rectifying, editing, erasing, adding, or updating his Personal Data;
4. Limiting the Processing to a limited scope;
5. Having knowledge of any Personal Data Breach in relation to his Personal Data; and
6. Objecting to the processing of Personal Data or its results whenever the same contradicts the fundamental

rights and freedoms of the Data Subject.

With exception to the item (5) of the previous paragraph,2 fees may apply for exercising some rights, capped at EGP 20,000.

Obligations of Controllers

The legality of the collection of Data Collection and Processing shall be deemed legitimate and legal only if the Controller does:

1. Obtain Personal Data only with the data subject's consent, or as permitted by law.
2. Ensure Data Accuracy: Data must be valid, accurate, sufficient, and relevant to its collection purpose.
3. Define Processing Standards: set clear methods and standards for data processing unless delegated to a Processor via written contract.
4. Limit Data Access: grant access to personal data only when legally permitted.
5. Implement Data Security Measures: apply technical and regulatory safeguards to prevent breaches, hacking, tampering, or illegal access.
6. Erase Data when: the processing purpose is fulfilled. If retained for legitimate reasons, data must be anonymized.
7. Correct Errors: immediately rectify any known or reported errors in the data.
8. Maintain Records including Data categories, recipients, retention periods, access rules, erasure mechanisms, and cross-border transfers. Data security protocols.
9. Obtain a License or Permit from the Data Protection Center for handling personal data.
10. Appoint a Local Representative (if the Controller is based outside Egypt), as per the Executive Regulations.
11. Cooperate with Inspections: provide proof of compliance and allow the Center to inspect operations.
12. Shared Responsibility: if there are multiple Controllers, each is individually responsible for full compliance.

Obligation of Processors

The processor of the personal data shall adhere to the following:

1. Follow Instructions - Process personal data only under written instructions from the controller or the center, and ensure processing complies with the law and is for a legitimate purpose.
2. Respect Processing Scope - limit processing to the defined purpose and timeframe and notify the Controller or data subject of the duration needed for processing.
3. Erase Data - Delete data after processing is complete or return it to the Controller.
4. No Unauthorized Access: the Processor may not grant access to personal data or processing results unless legally allowed.
5. No Purpose Deviation - the Processer may not process data beyond the Controller's intended purpose. Except processing for non-profit educational or statistical purposes, while respecting privacy rights.
6. Ensure Security by protecting processing activities, systems and devices used in handling personal data.
7. Avoid Violations by refraining from any actions that could directly or indirectly violate data subject rights.
8. Maintain Records by keeping a record of all processing activities done on behalf of Controllers, including:

- Types of data processed
- Duration and scope
- Security measures in place
- Contact details and DPO info

9. Prove Compliance by Providing evidence of compliance when requested by the Controller or the Center.
10. Obtain a License or Permit from the Data Protection Center to handle personal data.
11. Appoint a Local Representative if the Processor is based outside Egypt.
12. Shared Responsibility If multiple Processors are involved, each must comply fully unless responsibilities are assigned by agreement.

Obligations of the Data Protection Officer (DPO)

The Data Protection Officer shall be responsible for the enforcement of the provisions of this Law, its Executive Regulations, and the decisions of the Center, as well as monitoring the procedures applicable within its relevant legal entity and supervising the application of such procedures thereof, in addition to receiving requests related to Personal Data, as per the provisions of Law: The Data Protection Officer shall, in particular, undertake the following:

1. Enforce Compliance by ensuring the entity complies with the law, its executive regulations, and the Center's decisions.
2. Monitor Internal Procedures by Overseeing internal processes to ensure proper data protection measures are implemented.
3. Receive and Handle Requests to manage and respond to data subjects' requests regarding their personal data rights.
4. Perform Regular Evaluations by conducting routine assessments of the data protection system, certifying results, and recommending improvements to prevent breaches.
5. Act as Contact Point and serve as the liaison between the organization and the Data Protection Center and implement the Center's directives.
6. Enable Data Subject Rights by facilitating data subjects' ability to exercise their rights under the law.
7. Report Data Breaches by Notifying the Center of any personal data breach.
8. Handle Complaints and respond to complaints from data subjects or other concerned parties.
9. Oversee Records and Ensure the accuracy of data protection records held by the Controller or Processor.
10. Rectify Violations and Address and correct any internal data protection violations.
11. Conduct Training and organize staff training programs to enhance compliance with the law mainly Mandatory for all legal entities handling personal data. and responsible for compliance, communication with the PDPC, and managing complaints or breaches.

Sensitive Data

The enactment of Data Protection Law, Egypt Law No. 151/2020 has codified the classification of personal data in Egypt into personal data and sensitive personal data.

Personal data were defined under said Law as the data related to a particular natural person which aid in uncovering the identity of such person, in a direct or indirect means, through referring to data, such as name, voice, picture, identification number, online identifier, or any data that identifies psychological, health, economic, cultural or social identity.

On the Other hand, the law identified sensitive personal data as data related to psychological, mental, physical or genetic health, biometric data, financial data, religious beliefs, political opinions, or security situations; and personal Data relating to Children with such Data require explicit written consent and a special license from the PDPC.

Cross-Border Data Transfers

1. Prohibited unless the recipient country ensures equivalent data protection or consent is obtained.
2. Licenses or permits from the PDPC are required.
3. Some exceptions apply (e.g., medical emergencies, judicial cooperation, public interest).

Electronic Marketing

Any electronic communication for direct marketing to the Data Subject shall be prohibited unless the following conditions are met:

1. Obtaining the consent of the Data Subject.
2. The communication shall include the identity of its creator and sender.
3. The sender shall have a valid address in order to be reached.
4. The communication must indicate that its purpose is direct marketing.
5. Setting clear and uncomplicated mechanisms to allow the Data Subject to refuse electronic communication or to withdraw his consent to receiving such communication.

The sender of any electronic communication for the purpose of direct marketing shall undertake the following:

1. Specifying a defined marketing purpose.
2. Not disclosing the contact details of the Data Subject.
3. Maintain electronic records evidencing the consent of the Data Subject to receive Electronic Marketing communication any amendments thereof, or their non-objection to its continuity for a duration of 3 years from the date the last communication has been sent.

Personal Data Protection Center (PDPC)

A public economic authority, named the 'Personal Data Protection Centre', is established under the authority of the Competent Minister, and operates under the **Minister of Telecommunications and Information Technology**. The main **purpose of PDPC** is to:

1. Protect personal data.
2. Regulate data processing and access activities.
3. Develop and implement **data protection policies, strategies, and programs**.
4. Standardize data security and processing procedures across Egypt.
5. Issue decisions, regulations, procedures, and criteria for personal data protection.
6. Approve and guide **Codes of Conduct** for different sectors.
7. Collaborate with public and private entities to enforce data protection.
8. Support and train personnel across sectors.
9. Promote public awareness through **workshops, training, and publications**.
10. Issue **licenses, permits, and certifications**, and supervise compliance with the law.
11. Investigate violations and enforce legal actions.
12. Evaluate and approve **cross-border data transfers**.
13. Comment on relevant draft laws and treaties.
14. Enter **international agreements and partnerships** to enhance data protection.
15. Share knowledge and coordinate with global counterparts.
16. Publish an **annual report** on the state of personal data protection in Egypt.

Licenses and Permits

The PDPC issues Licenses, Permits, or Certifications as follows:

1. The Center shall classify and determine the types of Licenses, Permits and Certifications, and establish conditions for each type thereof, in accordance with the provisions of the Executive Regulations.
2. Issuing the License or Permit for the Controller or Processor to perform data safeguarding, handling, and Processing operations in accordance with this Law.
3. Issuing Licenses or Permits for direct Electronic Marketing.
4. Issuing Licenses or Permits for Processing of Personal Data undertaken by associations, unions, or clubs for the members of these entities and in the framework of their activities.
5. Issuing Licenses or Permits for means of visual surveillance in public places:
6. Issuing Licenses or Permits for the control and processing of Sensitive Data.
7. Issuing Permits and Certifications for individuals and entities to allow them to provide consultancy services on procedures for the protection of Personal Data and compliance procedures.
8. Issuing Licenses and Permits for the Cross-Border Movement of Personal Data.

The executive regulations shall specify the types, specifications, levels, Permits, Licenses, Certifications, procedures, and conditions of issuance and forms used, and this in return for no more than **EGP 2 million** for issuance of the License, and no more than **EGP 500,000** for issuance of a Permit or Certification

Penalties: PDPLLaw No. 151/2020 imposes custodial sentences of more than six months and severe fines ranging from EGP 50,000 to EGP 5 million against any violations of its provisions.

GHANA

Sam Okudzeto & Associates

In Ghana, the importance of protecting the data of its citizens is highly recognized and prioritized. In the year 2012, Ghana passed its primary legislation for the protection of data within the jurisdiction. The **Data Protection Act 2012** (Act 843) applies to all organizations and individuals handling personal data in Ghana and mandates that data controllers and processors register with the Data Protection Commission (DPC). Under Section 17 of the Act, it is stipulated that all persons who process data shall ensure the privacy of the individual by applying the principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, quality of information, openness, data security safeguards, and data subject participation. Under Section 35 of the Act, individuals referred to as data subjects have rights under the Act, including the right to access their data, request corrections, and object to certain processing activities.

Ghana's **Cybersecurity Act, 2020** (Act 1038) also plays a crucial role in protecting data, especially in the context of cybersecurity threats. While the Data Protection Act focuses on the lawful collection, processing, and storage of personal data, the Cybersecurity Act establishes a legal framework for securing digital systems, preventing cybercrime, and ensuring the resilience of critical information infrastructure. The Cybersecurity Act created the Cyber Security Authority (CSA), which oversees national cybersecurity efforts and enforces compliance with cybersecurity standards. The Act includes provisions on critical information infrastructure protection, incident reporting obligations, and penalties for cyber-related offenses, such as unauthorized access, hacking, and identity theft. Additionally, it provides safeguards for personal and corporate data against cyber threats, complementing the Data Protection Act by ensuring that digital information remains secure from cyberattacks. The **Electronic Transactions Act, 2008** (Act 772) is another relevant legislation that plays a role in protecting data. It regulates electronic communications and transactions, covering data privacy, electronic records, and cybersecurity. It

prohibits the unauthorized access and misuse of personal data in electronic transactions.

KENYA

Ong'anya Ombo Advocates LLP

Kenya history on Data Protection is traced from Article 31(c) and (d) of the Constitution of the Republic of Kenya (Kenya). However, Kenya's substantive Data Protection laws that are primarily enforced or implemented by the Office of the Data Protection Commissioner (ODPC) came way later in 2019. The ODPC was created via the Data Protection Act, 2019 (DPA) and formally established in the year 2020 due to the need to develop regulations that will operationalize the provisions of the DPA. The initial regulation to come into effect was the Data Protection (Civil Registration) regulations, 2020, then followed by three other regulations, which are the Data Protection (General) Regulations, 2021 (*provides for general guidelines on data collection and processing*), the Data Protection (Compliance and Enforcement) Regulations, 2021 (*outlines compliance measures and enforcement mechanisms*), and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 (*mandates the registration of entities handling personal data*). Other related laws include Computer Misuse and Cybercrimes Act, 2018, Computer Misuse and Cybercrime (the Critical Information Infrastructure and Cybercrime Management) Regulations 2024, and Gazette Notice No. 1043 (Designation of Critical Infrastructure).

The Data Protection laws provide for principles that ought to be followed by a data controller or processor when handling a data subject's personal data, and how to go about notifications during a data breach for any person that is handling personal data of a Kenyan citizen or any person within Kenya's territory. There are two models of financial or incidental costs that arise from breaching the DPA, which are statutory penalties and award for compensation to a data subject. While the latter has no statutory limitation, the former entails some statutory financial capping and imprisonment. Therefore, noncompliance with the DPA and its subsidiary legislation will result in enforcement notices or penalties not exceeding KES. 5 million or imprisonment for a period not exceeding 2 years or both. Corporate entities may be subject to administrative fines at the rate of one percent (1%) of their annual turnover, whichever is less (this is in reference to KES. 5 million general maximum administrative fine). Any person that is aggrieved with the decision of the ODPC may appeal to the High Court of Kenya.

KUWAIT

Al-Hamad Legal Group

Kuwait neither has any specific personal data protection law nor a General Data Protection Regulation (GDPR). However, Kuwait's Communications and Information Technology Regulatory Authority (CITRA) on 7 Feb 2024 issued an Administrative Decision No. 26/2024 concerning the Issuance of Data Privacy Protection Regulation (the "Regulation").

This new Regulation updates the country's data privacy framework for telecommunications and IT service providers. It replaces the previous regulation Law No. 42 of 2021 the Communications and Telecommunications Regulatory Authority (CITRA) issued Decision No. 42 of 2021 on Data Privacy Protection Regulation imposing obligations about data protection on Telecommunication Services Providers and related industry sectors.

To achieve the vision of the State of Kuwait towards developing into a financial and commercial centre (New Kuwait 2035), the Regulation applies to all licensed telecommunications and IT service providers that collect or process personal data—regardless of whether this is done inside or outside Kuwait. However, it explicitly excludes activities related to national security, law enforcement, or court orders.

The Regulation includes guidelines and better nuances to existing laws and regulations such as Law No. 20 of 2014 (Regarding Electronic Transactions) (the "ET Law") that requires that client data relating to positional affairs, personal status, health status, certain financial information, and other personal information must be retained privately and confidentially by the recipient and its employees. Such data may not be disclosed without client consent or court order.

By providing clear definitions of the terms Authority, Service Provider/Licensee, Juristic Person, Personal Data, Beneficiary/User, and third party in addition to Data Collection and Processing, Data Removal and Deletion, the main obligations for Service Providers are more specific.

Conditions for Personal Data Collecting and Processing

Before delivering any service, the Service Provider must provide:

- Clear information and explain the service terms and data-related rights (like changing or removing data) in a simple, accessible language—available in both Arabic and English
- Obtain User's consent and get the User's clear agreement to collect and process their personal data, ensuring they understand the terms, obligations, and purpose
- Explain the purpose wherein clearly state why the User's Personal Data is needed and how it will be used to provide the service

Consequently, the legality of the collection of Data Collection and Processing shall be deemed legitimate and legal only if one of the following conditions is met:

- Users consent the individual (data subject) has explicitly agreed to the collection and use of their data
- Legal obligation for the service provider to comply with legal requirements
- Data Protection – If the Data Collection is necessary to protect User data
- Identity verification - If the purposes sought by the Service Provider require determining the identity of the Data Subject
- Minor's Consent: obtaining written consent from the guardian of a minor under 18 years of age

Conditions for Data Collection and Processing

The Regulation has set forth conditions that need to be met during the provision of the Service or after its completion, wherein the Service Provider shall collect and process data in accordance with the following conditions:

- Full transparency from Service Providers, data practices, and policies to be made available and accessible
- Purpose and legal basis of collecting the data and for how long it will be kept
- Determining the identity and location of the Service Provider
- Ensuring the protection of Personal Data from unauthorized or illegal Processing and misuse
- Third-party disclosure notification to notify the Authority if User data is shared with any affiliated company or third-party and remain accountable for that data
- Using appropriate technological means that enable Users to exercise their right to directly access, review, and correct personal data
- Clearly state whether data is stored inside or outside Kuwait

- Set procedures for Users to access, correct, delete, restrict, object to, or request transfer of their data
- Notifying the data subject if the Service Provider intends to transfer his Personal Data outside the State of Kuwait
- Removing Personal Data once the User relationship ends
- Getting User consent before sharing data with third parties for marketing unrelated to the service
- Offering user-friendly ways to modify data, withdraw consent, or disable data usage/sharing
- The Service Provider shall remove the User's Personal Data if: a) Consent is withdrawn, b) Data is no longer needed for the service, c) User is no longer subscribed
- The Service Provider shall create and maintain a written privacy policy that has a clear, detailed privacy policy published online and shared with users at sign-ups.
- Notify the Authority, Users, and law enforcement of major data breaches within 72 hours
- When preparing any process, system, or procedures to provide communication facilities or services, the Service Provider must ensure privacy by service design

Security and Protection of Personal Data

Kuwait's new regulations not only focus on collecting and using data responsibly— but they also set clear expectations around keeping that data safe. Article 5 of the Regulation lays out what service providers need to do to protect personal information from leaks, hacks, or other types of misuse. The Service Provider shall take actions:

- to put strong safeguards in place and encrypt and classify data properly;
- to ensure that systems should always be secure, and stable;
- to be able to recover data whether it's a cyberattack or a natural disaster;
- to make records available for review by the Authority upon request;
- to maintain detailed records of all data handling activities;
- to ensure privacy and controls related to the design, change, or development of products, systems, and services that may affect the Processing of personal data;
- identify, train, and educate those responsible for protecting personal data;
- to set up a 24/7 channel for Users to submit complaints, ask for access to their data, or request corrections or Deletions of data;
- to notify the authority—and ideally Users to take quick action to reduce the damage; and
- conduct regular audits help make sure Service Provider is aligned with regulations.

CITRA has taken E-violations seriously and may apply penalties and fines as stipulated in Law No. 37 of 2014 that regulates information and communications amended by Law No. 98 of 2015 for violations and breaches of personal data.

MAURITIUS

YKJ Legal

Mauritius does have a comprehensive data protection legal framework governed by the *Data Protection Act 2017* (the "Act"), which came into force on 15 January 2018. The Act aligns Mauritius with international standards regarding data protection, particularly the European Union's General Data Protection Regulation (GDPR).

The Data Protection Act 2017 regulates the processing of personal data by both public and private bodies. It establishes the Data Protection Office of Mauritius and vests the Data Protection Commissioner with powers to monitor compliance, investigate complaints, and issue enforcement notices. The Act defines key concepts such as personal data, consent, data subject, controller, and processor, and sets out the rights of individuals, including the right to access, rectify, erase, or object to the processing of their personal data.

The Act requires controllers and processors to be registered with the Data Protection Office and to implement appropriate technical and organizational measures to ensure data security. It also imposes obligations regarding breach notifications, cross-border data transfers, and special categories of sensitive personal data. The Act restricts data transfers outside Mauritius unless adequate safeguards are in place. Overall, the Act seeks to strengthen individual autonomy and privacy rights while facilitating responsible data management practices.

MOROCCO

Westfield

Morocco has had data protection regulations since 2009, when the Law No. 09-08 was enacted.

Morocco's data protection framework is mainly based on Law No. 09-08. This law lays out the principles for processing personal data, which is defined as information of any kind relating to an identified or identifiable natural person, regardless of its form, including sound and images. To ensure that individuals maintain control over their privacy and identity, the law outlines their fundamental rights:

- To have their personal data corrected
- To access their personal data and the reasons for its processing
- To object to the further processing of their personal data, at any time
- To prevent processing of personal data for purposes of direct marketing
- To object to a decision based solely on automatic processing that would significantly affect the or produce adverse legal repercussions for them.

To make sure they are followed and complied with, the National Commission for the Protection of Personal Data (CNDP) was created in the same year. It plays an important role in providing guidance on data protection issues. In fact, penalties for not following data protection laws in Morocco can be quite severe. Offenses to the law are punishable by a fine ranging from MAD 10,000 to MAD 600,000 and/or imprisonment from three months to four years (from Article 52 to Article 63). Non-compliance can also lead to damage to their reputation, legal action, or even the suspension of data processing activities

The need for strong data protection in Morocco is even more important now due to the rapid growth of technology and the internet, which give more access to personal data. It's expected that lawmakers will revisit the current data protection laws to strengthen them and make them more aligned with international standards, especially as Morocco looks to improve its global trade relations. While Law No. 09-08 remains a foundational framework, it may need updates to address the challenges posed by new technologies, such as artificial intelligence and blockchain.

NIGERIA

Primera Africa Legal

The Data Protection Act, 2023

On 14 June 2023, President Bola Ahmed Tinubu signed into law, the Data Protection Act, 2023. The objective of the Act, amongst others, is to safeguard the fundamental rights, freedoms and the interests of data subjects as guaranteed under the 1999 Constitution of Nigeria. The Act establishes the Nigeria Data Protection Commission (NDPC), also referred to as the "Commission"

The Act applies to Data Controllers and Data Processors domiciled, ordinarily resident or ordinarily operating in Nigeria, or where the processing of personal data occurs within Nigeria. The Act also applies to data controllers or data processors not domiciled, ordinarily resident or ordinarily operating in Nigeria, so long as they are processing personal data of data subjects in Nigeria. In addition, the Act provides the boundaries of applicability by exempting activities carried out solely for personal or household purposes and various activities carried out by competent authorities.

Another importance of the Act is that it also emphasizes comprehensively, the rights of a data subject. It provides an avenue for aggrieved data subjects who have suffered injury, loss, or harm as a result of a violation of this Act by a Data Controller or Data Processor, to recover damages from such data controller or data processor in civil proceedings. In addition, penalties for breach of the Act have been broken down for Data controllers of major importance and Data Controllers not of major importance.

SAUDI ARABIA

Khalid Nassar & Partner Law Firm

Saudi Arabia has enacted data protection legislation. The foundation of the country's data privacy framework is the Personal Data Protection Law (PDPL), which was initially issued by Royal Decree M/19 on September 16, 2021, and amended in March 2023. The law is enforced by the Saudi Data and Artificial Intelligence Authority (SDAIA) and applies to both public and private entities that process personal data. It also extends to entities located outside of Saudi Arabia if they process the personal data of individuals residing in the Kingdom.

The PDPL governs the collection, use, disclosure, storage, and transfer of personal data. It mandates that personal data must be processed in a lawful, transparent, and secure manner, and organizations must obtain explicit consent from data subjects before processing their data unless an exemption applies. The law also establishes the rights of data subjects, including the right to access, correct, and delete their personal data.

Recent amendments introduced more flexibility regarding lawful processing bases, cross-border data transfers, and the appointment of Data Protection Officers (DPOs). The PDPL officially came into force on September 14, 2023, with a one-year grace period for organizations to comply, ending on September 14, 2024. The law is supported by implementing regulations expected to further clarify operational obligations. Organizations operating in Saudi Arabia are encouraged to assess and align their internal data governance frameworks with the PDPL requirements.

SOUTH AFRICA

Knowles Husain Lindsay Inc.

The right to privacy is enshrined in the South African Constitution, and the Protection of Personal Information Act, No. 4 of 2013 ("POPIA"), which commenced on 1 July 2020, gives practical effect to this right through setting out details and processes regarding how one's right to privacy is to be protected. Under POPIA, the personal

information of both natural and juristic persons is protected.

Among others, POPIA sets out conditions with which processing of personal information needs to comply, such as accountability, processing limitations, records retention, quality of information, openness, data subject participation and security safeguards.

Each responsible party i.e. the person (juristic or natural) who receives the personal information of others and who determines why and how to process that information is required to appoint an Information Officer and notify the Information Regulator of such appointment. Further, such responsible parties need to compile the so-called "PAIA manual", which, amongst others regulates under what circumstances third parties may request records from the responsible party, with due regard to the rights afforded by POPIA.

The name "PAIA" is an abbreviation for the Promotion of Access to Information Act, No. 2 of 2000, which Act gives effect to the constitutional right of access to information and as such compliments and limits POPIA.