SAUDI ARABIA

Law and Practice

Contributed by:
Alex Saleh, Feras Gadamsi, Ahmad Saleh and Shahad Al-Humaidani
GLA & Company

Contents

1. Basic National Regime p.5
1.1 Laws p.5
1.2 Regulators p.5
1.3 Administration and Enforcement Process p.6
1.4 Multilateral and Subnational Issues p.6
1.5 Major NGOs and Self-Regulatory Organisations p.6
1.6 System Characteristics p.7
1.7 Key Developments p.7
1.8 Significant Pending Changes, Hot Topics and Issues p.7

2. Fundamental Laws p.8
2.1 Omnibus Laws and General Requirements p.8
2.2 Sectoral and Special Issues p.11
2.3 Online Marketing p.14
2.4 Workplace Privacy p.14
2.5 Enforcement and Litigation p.14

3. Law Enforcement and National Security Access and Surveillance p.15
3.1 Laws and Standards for Access to Data for Serious Crimes p.15
3.2 Laws and Standards for Access to Data for National Security Purposes p.15
3.3 Invoking Foreign Government Obligations p.16
3.4 Key Privacy Issues, Conflicts and Public Debates p.17

4. International Considerations p.17
4.1 Restrictions on International Data Issues p.17
4.2 Mechanisms or Derogations That Apply to International Data Transfers p.18
4.3 Government Notifications and Approvals p.19
4.4 Data Localisation Requirements p.19
4.5 Sharing Technical Details p.19
4.6 Limitations and Considerations p.19
4.7 “Blocking” Statutes p.19

5. Emerging Digital and Technology Issues p.19
5.1 Addressing Current Issues in Law p.19
5.2 "Digital Governance" or Fair Data Practice Review Boards p.20
5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation p.20
5.4 Due Diligence p.21
5.5 Public Disclosure p.21
5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI) p.21
5.7 Other Significant Issues p.22

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It provides strategic, cost-effective and forward-thinking legal representation for companies seeking to do business in the Middle East. The firm boasts a diverse portfolio of clients, ranging from start-ups to global enterprises doing business in the Middle East. GLA's practice consists of a full-service law firm that handles everything from simple advisory work to complex contentious and non-contentious matters. With extensive experience advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the United Arab Emirates (UAE) – as well as in Egypt and Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area for the firm, considering the expansion and revamping of applicable laws and regulations across the GCC.

Authors

Alex Saleh is a founder and managing partner of GLA & Company and takes a leading regional role in the firm's M&A and private equity practice. With more than 25 years of experience in both the Gulf Cooperation Council and the USA, he has accumulated sizeable expertise in the areas of banking and finance, M&A, capital market deals and infrastructure projects. His experience garners praise from the leading legal directories and his transactions are regularly noted by the same institutions and organisations.

Feras Gadamsi is a partner based in the firm's Dubai office, leading GLA & Company's global technology, data and privacy practice. Feras also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations, and audits. He started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. Immediately prior to joining the firm, Feras served as Regional General Counsel at IBM. He was formerly Uber's lawyer in the MEA region, serving as General Counsel for Middle East and Africa, Oracle Cerner's Regional General Counsel, and served as CLO and Head of Policy for a Dubai-based start-up.

Ahmad Saleh is a senior associate at GLA & Company and an active member of the firm's corporate and disputes practice, where he focuses on M&A and other local and cross-border transactions. Since joining the firm, Ahmad has successfully advised multinational clients across various industries, including banking and finance, private equity and capital markets, food and retail, and government contracting. He has recently been working on complex contractual disputes for major construction projects in Kuwait, including representation as local counsel in arbitral and other ADR forums. Ahmad has co-authored numerous articles, including an overview of Data Protection & Privacy laws and regulations in Kuwait.

Shahad Al-Humaidani serves as an associate at GLA & Company's Riyadh office, with a versatile background in both governmental and private sectors within Saudi Arabia. Her expertise is particularly focused on providing support to foreign companies aiming to establish a presence in the Kingdom of Saudi Arabia (KSA). In this capacity, she navigates the complexities of regulatory frameworks, including the Saudi Arabian General Investment Authority (MISA) and the Ministry of Commerce (MOC). Shahad's keen understanding of the legal landscape ensures the smooth entry of foreign entities into the KSA market, guaranteeing compliance with local regulations and facilitating successful business operations.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait +(965) 669 55516
UAE +(971) 54 997 4040
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

1. Basic National Regime

1.1 Laws

Data Protection and Privacy (DPP) issues in the Kingdom of Saudi Arabia (Saudi Arabia) are governed by a robust set of laws, regulations, policies, procedures, standards and guidelines.

The most notable of these laws, the Personal Data Protection Law (together with the Implementing Regulations, the PDPL), came into force on 14 September 2023.

Other significant laws and regulations, inter alia, related to the protection and privacy of data in Saudi Arabia include:

- Telecommunication and Information Technology Law (the "TCIT Law");
- Electronic Transactions Law (the "ET Law");
- Anti-Cyber Crime Law (the "ACC Law"); and
- Electronic Commerce Law (the "EC Law").

The PDPL covers processing of personal data (i) that takes place in Saudi Arabia and (ii) related to individuals residing in the Kingdom, by any means by any party outside the Kingdom. The TCIT Law covers communication services and protection of client and customer data and privacy. The ET Law covers electronic transactions, creating and keeping electronic records, electronic signatures and electronic authentication certificates. The ACC Law addresses cybersecurity crimes and their punishment. The EC Law covers electronic commerce.

The policies, procedures, standards and guidelines are vast; however, most relevant to DPP are:

- general principles for protecting users' personal data privacy;
- procedures for launching services or products based on a customer's personal data or regarding the sharing of personal data;
- national data governance policies;
- data management and personal data protection standards;
- general standards for personal data transfer beyond the geographical limits of Saudi Arabia;
- children and incompetents' privacy protection policy; and
- guidelines and specifications on data management governance and personal data security.

The PDPL, and its corresponding Implementing Regulations, entered into force on 14 September 2023. Data controllers, however, have a one-year grace period (eg, 14 September 2024) to comply with the PDPL.

1.2 Regulators

The Saudi Data and Artificial Intelligence Authority (SDAIA) is the regulatory body that is empowered to supervise and enforce the implementation of the PDPL in Saudi Arabia for at least the first two years following promulgation. Consideration will be given to transferring supervising regulation and the application of the PDPL to the National Data Management Office (NDMO), the regulatory subdivision of SDAIA.

The Communications, Space and Technology Commission (CSTC, or the "Commission") is responsible for the enforcement of both the TCIT Law and ET Law. The Ministry of Commerce (MoC) is responsible for the enforcement of the EC Law. The National Cybersecurity Authority (NCA) is responsible for the enforcement of the ACC Law. Violations are reported to the Public Prosecution Office, which takes the necessary action to prosecute violators.

1.3 Administration and Enforcement Process

In respect of both the TCIT Law and ET Law, CSTC inspectors investigate, examine and collect allegations of violations of the provisions of the TCIT Law. Inspectors are tasked with inspecting sites of suspected violators of the TCIT Law and with gathering evidence in support of their investigations. Suspected violators may appeal a decision issued against them before the Administrative Court in accordance with the Law of Procedure before the Board of Grievances.

Under the ACC Law, potential penalties for the violation of any of its articles range from imprisonment of up to ten years to fines of up to SAR5 million. See **5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation** for more detail.

Under the PDPL, SDAIA is currently the competent authority and regulator in charge of administering the enforcement of the PDPL. Unless SDAIA provides exceptional approval, a data subject must submit a complaint within 90 days of an alleged incident to SDAIA. Complaints must specify:

- place and time of the alleged violation;
- name, identification, address and telephone number of the complainant;
- relevant identifying information about the entity that the complainant is lodging the complaint against;
- clear and specific description of the violation (together with any evidence and information provided with the complaint); and
- any other requirements that may otherwise be specified by SDAIA.

SDAIA is tasked with taking the necessary measures regarding the processing and decisions related to any complaints and informing the complainant of the outcome.

1.4 Multilateral and Subnational Issues

Article 3 of the PDPL stipulates that the provisions and procedures stated in the PDPL shall be without prejudice to any provision that grants a right to personal data subjects or confers better protection on personal data subjects pursuant to any other law or any international agreement to which Saudi Arabia is a party.

The PDPL does not allow for the transfer of data outside Saudi Arabia where such transfer would compromise the national security or vital interests of Saudi Arabia. In addition, a public entity may transfer data outside Saudi Arabia where to do so would be in Saudi Arabia's national security or for the public interest.

1.5 Major NGOs and Self-Regulatory Organisations

The PDPL has recently come into force in Saudi Arabia. As part of the process, Saudi Arabia solicited suggestions from the public, and industry, to enact "best in class" laws and implementing regulations from Day 1. From this perspective, Saudi Arabia's proactive approach allowed the public, and industry, to "self-regulate" the laws and regulations applicable in Saudi Arabia through a lengthy and robust review and commentary period.

In addition, many statutes developed by Saudi Arabia related to data privacy are based on "best practices" promulgated by global associations. For example, the NDMO Data Management and Personal Data Protection Standards selected the Data Management Body of Knowledge (DAMA-DMBOK Guide) as a key reference.

Although there are no official NGOs or self-regulatory organisations, or NGOs, specialised in data protection and data privacy issues operating in Saudi Arabia at the time of publication, it should be noted that Saudi Arabia is set to host the 19th edition of the Internet Governance Forum (IGF) in late 2024.

1.6 System Characteristics

The PDPL is designed with "best practices" in mind, and, after a two-year public consultation period, it was put into effect. Accordingly, it should not be surprising that the PDPL shares many of the same characteristics as other global data protection and privacy laws and regulations promulgated in other parts of the globe, most notably the EU's GDPR.

Some of these characteristics include:

- articulation of basic rights and principles;
- a heightened emphasis on sensitive personal data, including specific treatment of health and financial data;
- transparency with regard to collecting users' information (Article 4 and Article 10 of the PDPL);
- a prescribed manner for the exceptional processing of personal data for "legitimate interests" by a data controller (Article 6 of the PDPL);
- rectification and erasure of certain information at the request of the subscriber/user (Article 4.3 and Article 4.4 of the PDPL);
- disclosure to users of transfers of personal data to third countries or international organisations (Article 13.4 of the PDPL);
- circumstances for notification to the regulator of an incident within 72 hours (Article 20 of the PDPL);
- rights to lodge complaints with supervisory board (Article 34 of the PDPL); and
- penalties for violation of the Law (Article 35 of the PDPL).

1.7 Key Developments

The PDPL introduces comprehensive legislation aimed at filling gaps not previously addressed in Saudi Arabia. SDAIA also published a set of key ethical principles related to the use and deployment of artificial intelligence (AI). This publication on AI Ethics was developed to help establish policies, guidelines, regulations and frameworks with respect to the ethical deployment, and use, of AI in Saudi Arabia.

1.8 Significant Pending Changes, Hot Topics and Issues

While the coming into force of the PDPL is the most significant change in law related to DPP, the Implementing Regulations set forth more specifics as to the standards expected of companies operating under the auspices of the PDPL. Significant provisions in the PDPL include the introduction of consumer-friendly rules on the collection, storage and use of personal data, such as:

- the requirement to obtain express consent from the owner of such data and the minimum acceptable standards applicable to a controller when seeking a data subject's consent (Article 11 of the Implementing Regulations);
- the right for a data subject to withdraw consent and the minimum acceptable standards for a data subject's withdrawal of consent (Article 12 of the Implementing Regulations);
- general obligations related to rights to inform data subjects;
- minimum acceptable standards related to the appointment of data protection officers; and

- the right of consumers to conveniently demand the destruction of personal data in the possession of others subject to the PDPL.

It is worth noting that the PDPL does not supersede pre-existing laws, regulations, policies, etc, provided they do not otherwise contravene the PDPL. Moreover, the PDPL provides that sectors such as banking and state security will be among the "special" cases subject to the authority of government bodies such as the Saudi Central Bank and Ministry of Interior.

In terms of AI, the AI Ethics framework was published by SDAIA and is intended to apply to all AI stakeholders designing, developing, deploying, implementing, using or being affected by AI systems within Saudi Arabia, including but not limited to public entities, private entities, non-profit entities, researchers, public services, institutions, civil society organisations, individuals, workers, and consumers.

AI is already embedded in day-to-day life, but as the focus shifts to more user-facing applications of AI, the AI Ethics framework is intended to provide guidance in the interim as regulators and governments review the application of how existing laws and regulations will be applied to issues that will inevitably arise from AI, and whether the development of new laws and regulations will be required to tackle the unique set of issues tied to the deployment of AI use in Saudi Arabia.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The PDPL and its Implementing Regulations are considered the main source of protection for data subjects in Saudi Arabia (bearing in mind the one-year grace period for controllers to fully implement all aspects of the PDPL). This law applies, together with sector-specific regulations passed by other competent authorities (eg, healthcare sector data privacy rules and regulations codified by the Ministry of Health, financial sector data privacy rules and regulations codified by the Saudi Central Bank, etc).

Appointment of Data Protection Officers

Article 32 of the Implementing Regulations states that a controller is required to appoint a data protection officer under the following circumstances:

- a public entity that provides services involving processing of personal data on a large scale;
- the primary activities of the controller consist of processing operations that require regular and continuous monitoring of data subjects on a large scale; and/or
- the core activities of the controller consist of processing sensitive personal data.

The data protection officer may be an official, employee or external contractor of the data controller. However, further rules governing the appointment of data protection officers, which are supposed to be published and clarified by the regulator, have not yet been issued by SDAIA as of the publication date of this guide (12 March 2024). It should also be noted that sector-specific requirements from other relevant, competent authorities may require the appointment of a data protection officer and/or specify additional rules related to the data protection officer (eg, the banking sector, via the Saudi Central Bank, may issue additional rules requiring the appointment of a data protection officer or, for example, the data protection officer's physical location and/or nationality).

Requirements for the Collection, Processing and Use of Personal Data

Article 10 of the PDPL stipulates that the controller may collect personal data only from the personal data subject. Such personal data may only be processed for the purpose for which the personal data is collected. However, the controller, on an exceptional basis, may collect personal data from a person other than the personal data subject or process personal data for a purpose other than that for which the personal data is collected.

- The personal data subject consents in accordance with the provisions of the PDPL.
- The personal data is publicly available or collected from a publicly available source.
- The controller is a public entity, and the personal data was not collected, or processed, as required either for security purposes or in order to implement another law or fulfil judicial requirements in accordance with the provisions set out in the regulations.
- Compliance with this restriction may cause harm to the personal data subject or affect the vital interests of the personal data subject (as set out in the regulations).
- Collection or processing of personal data is necessary to protect public health or safety or to protect the life or health of a specific individual. The regulations shall set out the rules and procedures applicable in this respect.
- The personal data will not be recorded or stored in a form that makes it possible to identify the personal data subject directly or indirectly. The regulations set out the rules and procedures applicable in this respect.

Article 11 of the PDPL stipulates the following in relation to privacy, fairness and legitimate interest.

- The purpose for which personal data is collected must be directly related to the controller's purposes and shall not contravene any applicable legal provisions.
- The methods and means of collecting personal data must:
  (a) not conflict with any legal provisions;
  (b) be suited to the circumstances of the personal data subject;
  (c) be direct, clear and secure; and
  (d) not involve any deception, misleading or extortion.
- The content of the personal data should be appropriate and limited to the minimum amount necessary to achieve the purpose of the collection. The regulations shall set out the rules applicable in this regard.
- If the personal data collected is no longer necessary for the purpose for which it has been collected, the controller shall cease the collection and destroy the previously collected personal data.

Article 15 of the Implementing Regulations also provides specifications related to the collection of data from third parties, while Article 16 of the Implementing Regulations addresses the processing of data, other than sensitive personal data, for legitimate interests by private entities. A legitimate interest is defined as any necessary interest of the controller that requires the processing of personal data for a specific purpose, provided it does not adversely affect the rights and interests of the data subject.

Legitimate interests include, inter alia, the disclosure of fraud operations and the protection of network and information security. The controller may process personal data to achieve a legitimate interest provided that the processing purpose is legal, but in so far as the processing of data balances the rights and interests of the

data subject with the legitimate interests of the controller, and, in doing so, the controller does not adversely affect the rights and interests of the data subject. Processing shall be within the reasonable expectations of the data subject.

Internal or External Privacy Policies

Article 12 of the PDPL stipulates that the controller shall adopt a personal data privacy policy and make it available to personal data subjects for review prior to collecting personal data. The policy shall specify the purpose of collection, the personal data to be collected, the method of collection, the means of storage and processing, the manner in which the personal data shall be destroyed, and the rights of the personal data subject in relation to the personal data and how such rights shall be exercised.

Data Subject Access Rights

Article 5 of the PDPL states that a data subject has the right to access their personal data available with the controller provided that such access does not negatively impact the rights of others, such as intellectual property rights or trade secrets. Article 6 also makes it clear that, subject to certain parameters, data subjects have the right to request a copy of their personal data in a readable and clear format from the controller.

Article 13 of the PDPL stipulates that when collecting personal data directly from the personal data subject, the controller shall take appropriate measures to inform the personal data subject of the following prior to collection:

- the legal basis and valid practical reasons for collecting their personal data;
- the purpose of the collection, whether collecting some or all of the personal data is mandatory or optional, and that the personal data collected will not be subsequently processed in a manner inconsistent with the collection purpose or in circumstances other than those stated in Article 10 of the PDPL;
- the identity of the person collecting the personal data and the address of such person's representative, if necessary (unless the collection is for security purposes);
- the entities to which the personal data will be disclosed, the capacity of such entities, and whether the personal data will be transferred, disclosed or processed outside Saudi Arabia;
- the potential consequences and risks that may result from not collecting the personal data;
- the rights of the personal data subject pursuant to Article 4 of the PDPL; and
- such other elements as set out in the regulations based on the nature of the activity performed by the controller.

Use of Anonymised Data

Article 9 of the Implementing Regulations states that when personal data is anonymised by a controller, the controller must ensure the following with respect to the data that has been "converted", in terms of classification, from personal data to anonymised data:

- ensure that the re-identification of the data subject is impossible after anonymisation;
- evaluate the impact, through an impact assessment study as specified in the PDPL, of the possibility of re-identifying the data subject;
- take the necessary organisational, administrative and technical measures to avoid the risks identified in any impact assessment study, taking into account technological developments, methods of anonymisation, and updates to those methods; and

- evaluate the effectiveness of the applied techniques for anonymising personal data and make necessary adjustments to ensure that re-identification of data subject is impossible.

Article 9 also states that anonymised data shall not be considered personal data. Accordingly, data that is classified as anonymised data, even if it originally was considered personal data, can be used in any manner that is lawful under applicable law provided such data is anonymised in accordance with Article 9. Since the PDPL only applies to personal data, the PDPL would not apply to the processing of such anonymised data.

Big Data Analysis

Article 10 of the PDPL outlines potential exceptions for the use of personal data beyond the purpose for which such data was collected. This could involve big data analysis of personal data. These potential exceptions include, inter alia:

- instances where the controller is a public entity, and the collection and/or processing of the personal data is required for public interest or security purposes, or to implement another law, or to fulfil judicial requirements;
- personal data collection or processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals;
- personal data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the data subject; and/or
- personal data collection is necessary to achieve legitimate interests of the controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive personal data is to be processed.

In addition, Article 27 of the PDPL stipulates that personal data may be collected or processed for scientific, research or statistical purposes without the consent of the personal data subject if:

- the personal data does not contain information that specifically identifies the personal data subject;
- the information that specifically identifies the personal data subject is to be destroyed during the processing of such personal data prior to the disclosure of such personal data to any other entity – provided such data is not sensitive data; and/or
- the collection or processing of personal data for said purposes is required under any other law or in order to implement a prior agreement to which the personal data subject is a party.

2.2 Sectoral and Special Issues

Financial and Credit Data

Together with the PDPL, the financial data of banking, insurance and financial clients is protected by the rules of the Saudi Central Bank.

Under the PDPL, credit data is defined as any personal data related to an individual's request for, or obtaining of, financing from a financing entity, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.

Article 24 of the PDPL also sets out additional controls and procedures for the processing of credit data in a manner that ensures the privacy of the data subject. These include:

- implementing appropriate measures to verify that the data subject has given their explicit consent to the collection of the personal data, changing the purpose of the collection, or

disclosure (or publishing) of the personal data in accordance with applicable laws; and
- requiring that the data subject be notified when a request for disclosure of their credit data is received from any entity.

In addition, the Implementing Regulations specify that consent for processing and collection of credit data must be explicit, and when decisions are made solely based on automated processing of personal data, such as automated approval or denial of credit.

Communications Data

Article 23 of the TCIT Law provides for the following with regard to voice telephony, text messaging and the content of electronic communications.

- The service provider must take all measures and make all arrangements necessary to ensure the confidentiality of the user's information and personal data is maintained and to prevent accessing, reviewing and disposing of such information and data illegally. This includes preparing and submitting policies related to maintaining the confidentiality of such information and documents to the Commission for approval in accordance with the relevant legal provisions.
- The user's information or documents may only be disclosed with the user's consent, according to the relevant legal provisions.
- The service provider must take all procedures necessary for maintaining user's information and documents if they are infringed in any way and immediately inform the Commission and user of the incident's details.
- Without prejudice to the relevant legal provisions, the service provider shall keep the user's information and documents for the period that the Commission determines. In addition, such period shall be calculated as of the date of the last service provision. In the event of a dispute that may arise in connection with the service between the user and service provider, such information and documents shall be kept until the dispute is solved.

Article 6 of the ET Law addresses storing electronic records as follows.

- Without prejudice to Article 3 of the ET Law, if any law in Saudi Arabia requires for certain documents or information to be stored for any reason, such requirement shall be deemed satisfied if said documents or information is stored or sent in the form of an electronic record, subject to the following:
  (a) storing the electronic record in the form it was generated, sent or received, or in such a form that the contents thereof may be verified as being identical to the contents in which it was generated, sent or received;
  (b) storing the electronic record in a manner that allows for future use and reference; and
  (c) storing information, together with electronic records, indicating the originator and addressee (as well as the date and time of sending and receiving).
- Any person may, at their own risk, assign another person to satisfy the requirements set forth in paragraph (1) of this Article.

The regulations of the ET Law stipulate in greater detail how to preserve data and electronic records.

Health Data

The PDPL defines health data as any personal data related to an individual's health condition,

whether their physical, mental or psychological conditions, or related to health services received by that individual. Article 23 of the PDLP restricts the right to access health data (including medical files) to the minimum number of employees or workers - and only to the extent necessary to provide the required health services.

In addition, health data processing is restricted to the minimum procedures and operations required of employees and workers as necessary to provide health services or offer health insurance programmes.

Children's Data

Article 13 of the Implementing Regulations discusses legal guardians and the process for obtaining consent with respect to individuals who fully or partially lack legal capacity to exercise rights and/or provide consent with respect to the collection, processing and storage of personal data, including sensitive personal data. These include duties imposed on the controller to take appropriate measures to verify validity of guardianship over the data subject and means for a data subject to take back their individual rights when full legal capacity is gained or regained (as the case may be).

The Children and Incompetents' Privacy Protection Policy aims to protect the privacy of children and incompetent individuals in data processing activities. It mandates that the data collected must be relevant and limited, and that appropriate security measures must be implemented to protect personal data. Parental or guardian consent must be obtained before collecting, processing or transferring personal data of children and incompetent individuals. In case of a data breach, affected individuals and the NDMO must be notified. Privacy awareness must be raised among children and their guardians through education programmes and materials.

It should be noted that the PDPL makes it clear that consent to collect and process a data subject's data can only be provided by an individual who has full legal capacity to do so.

Data Subject Rights

The fundamental rights of individual data subjects are set forth in Article 4 of the PDPL and include, inter alia, the following.

- The right to be informed, which includes informing the personal data subject of the regulatory or valid practical reason for collecting their personal data, and informing the personal data subject that the data is not processed later in a way that conflicts with the purpose of collecting the data.
- The right to access their personal data held by a controller (without prejudice to Article 9 of the PDPL).
- The right to request personal data held by a controller in a readable and clear format, in accordance with the controls and procedures specified in the PDPL.
- The right to request corrections or to complete or update their personal data held by the controller.
- The right to request the destruction of their personal data held by the controller, without prejudice to the provisions of Article 18 of the PDPL.

In addition, the Implementing Regulations, and in particular Article 4 (right to be informed), Article 5 (right of access to personal data), Article 6 (right to request access to personal data), Article 7 (right to request correction to personal data) and Article 8 (right to request destruction of per-

sonal data), provide further clarification of data subjects' fundamental rights.

2.3 Online Marketing

Article 12 of the PDPL specifies that a controller shall adopt a personal data privacy policy in line with the law and make it available to personal data subjects for review prior to collecting personal data. The policy shall specify:

- the purpose of collection;
- the personal data to be collected;
- the method of collection;
- the means of storage and processing;
- the manner in which the personal data shall be destroyed; and
- the rights of the personal data subject in relation to the personal data and how such rights shall be exercised.

In addition, Article 29 of the Implementing Regulations further specifies that controllers must provide an "opt out" available to personal data subjects that is easy, straightforward, and no more difficult than the way data subjects provide consent in the first place.

Article 26 of the PDPL specifies that personal data (excluding sensitive personal data) may be processed for marketing purposes if it is collected directly from the personal data subject and the personal data subject consents to that in accordance with applicable laws and regulations.

Article 28 of the Implementing Regulations of the PDPL sets out the general rules applicable to consent and the processing of data for advertising and awareness purposes in this regard.

Article 29 of the Implementing Regulations also requires that the entity sending materials through direct marketing clearly identify themselves without anonymity. In addition, if a data subject withdraws consent, the controller shall immediately stop sending related marketing materials without undue delay.

2.4 Workplace Privacy

There are no special regulations found explicitly dealing with workplace privacy. The PDPL does not make a special distinction between the treatment of data subjects generally and that of those who are simultaneously considered employees of the controller, so, at the very least, a controller's employees should enjoy, at a minimum, the same rights and remedies under the minimum standards that a data controller uses with data subjects generally.

2.5 Enforcement and Litigation

As mentioned in **1.3 Administration and Enforcement Process**, to enforce both the ET Law and TCIT Law, the CSTC inspectors investigate, examine and collect evidence of violations of the provisions of the TCIT Law. Penalties can include issuance of a fine not exceeding SAR5 million and/or imprisonment for a period of up to five years.

The National Cybersecurity Authority is the competent authority regarding overseeing all cybersecurity matters in Saudi Arabia, according to Article 3 of the Statute of the National Cybersecurity Authority. Penalties of up to one year in prison and a fine of up to SAR500,000 apply to any person found to have committed one of the following cybercrimes:

- spying on or interception or reception of data transmitted through an information network or a computer without legitimate authorisation;
- unauthorised access with the intention of threatening or blackmailing any person in

order to compel them to take (or refrain from taking) an action, be it lawful or unlawful;
- unauthorised access to a website (or hacking a website) in order to change its design, destroy or modify it, or occupy its URL;
- invasion of privacy through the misuse of camera-equipped mobile phones and the like; and
- defamation and infliction of damage upon others through the use of various IT devices.

Article 35 of the PDPL specifies that any individual who discloses or publishes sensitive personal data either intentionally or for personal benefit may face a penalty of up to two years of imprisonment and/or a fine of up to SAR3 million without prejudice to any other harsher penalty applicable under any other law for the same act. These penalties may be doubled in the case of repeat offenders.

Article 36 of the PDPL specifies that all violations of the PDPL, other than those covered in Article 35, face penalties that range anywhere from a warning to a fine up to SAR5 million on every person with a special nature or legal capacity who violates the PDPL. This is, again, without prejudice to any other harsher penalty applicable under any other law for the same act, and the penalty may be doubled in the case of repeat offenders.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

In general, Article 15 of the PDPL specifies the exceptional basis for disclosure of an individual's personal data in connection with serious crimes. Article 15, paragraph 3 of the PDPL allows a controller to disclose a data subject's personal data in response to a disclosure request from a public entity (eg, law enforcement) provided that the collection or processing of the personal data is required for public interest (eg, law enforcement) or security purposes, to implement another law, and/or to fulfil judicial requirements.

Article 15, paragraph 4 of the PDPL also allows a controller to disclose a data subject's personal data if the disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.

Under the Implementing Regulations, transfer of a data subject's personal data is permitted outside Saudi Arabia by a controller that is a public entity, where such transfer and disclosure is necessary for the protection of the Kingdom for the investigation, or detection, of crimes, or the prosecution of their perpetrators, or for the execution of penal sanctions.

3.2 Laws and Standards for Access to Data for National Security Purposes

As mentioned in **3.1 Laws and Standards for Access to Data for Serious Crimes**, the general basis for the disclosure of a data subject's personal data for national security purposes is set forth in Article 15 of the PDPL. In addition, Article 16 of the PDPL limits the disclosure of personal data even if such disclosure is normally allowed if the disclosure represents a threat to security.

Also, under Article 6 of the PDPL, a public entity shall not be required to obtain a data subject's consent where the processing of such data is required for security purposes or to satisfy judicial requirements.

Under the Implementing Regulations, transfer of a data subject's personal data is permitted out-

side Saudi Arabia by a controller that is a public entity, where such transfer and disclosure is necessary for national security reasons or for the public interest.

It should also be noted that, pursuant to the Law of Electronic Transfer of Private Entity Client Information to the Ministry of Interior National Information Center (2013), hotels, furnished apartments, rental cars, and gold and silver stores must provide the competent security entities with their customers' information.

Privacy safeguards are included in High Order No 37194 (2016), which stipulates that:

- restrictions apply to all entities in the course of:
  - (a) gathering employees' biometrics information for the purpose of proving attendance in the workplace; and
  - (b) gathering information from members of the public who interact with said entities (eg, customers in the private sector or hospital patients) or interact with the government to obtain its services;
- the National Information Centre must provide authentication services in accordance with certain controls; and
- all entities that need to gather data from non-employees must obtain approval from the National Information Centre.

3.3 Invoking Foreign Government Obligations

The Implementing Regulations of the PDPL set forth exemptions for the transfer of personal data outside Saudi Arabia by a data controller. A controller may transfer personal data outside Saudi Arabia provided that the regulatory requirements of the country (or, in the case of world bodies, the international organisation) where such data is transferred to do not prejudice the privacy of data subjects or affect the ability of data subjects to enforce appropriate safeguards.

These safeguards may include binding common rules, standard contractual clauses, certifications of compliance with the PDPL, and/or binding codes of conduct. In all cases, the competent authority (eg, SDAIA) must certify the sufficiency of the appropriate safeguards. As of the date of publication of this guide (March 2024), the Implementing Regulations specify the minimum suitability of binding common rules, but standard contractual clauses have yet to be issued by the competent authority.

The controller may not transfer personal data outside Saudi Arabia or disclose it to a party outside Saudi Arabia unless necessary to implement an obligation under an agreement to which Saudi Arabia is a party, or to further benefit Saudi Arabia's interest, or for other reasons as determined by the regulations, and subject to compliance with the following conditions:

- such transfer shall not adversely affect the national security or vital interests of Saudi Arabia;
- sufficient guarantees are provided that the transferred or disclosed personal data is adequately secured, so that the standards of personal data protection are not less than the standards provided for by the PDPL and the regulations;
- the transfer or disclosure of personal data is limited to the minimum amount of personal data required;
- the approval of the competent authority for the transfer or disclosure in accordance with the regulations; and
- the relevant competent authority may exempt the controller from complying with the above-

mentioned conditions if the competent authority finds that the personal data will be afforded acceptable security standards outside Saudi Arabia, which shall be determined on a case-by-case basis – whether unilaterally or in conjunction with other authorities – as long as such data is not determined to be sensitive data.

Under Article 3 of the Implementing Regulations, SDAIA is tasked with assessing the sufficiency of the protection of personal data to countries, sectors or international organisations outside Saudi Arabia on a periodic basis. This assessment is based, inter alia, on previous assessments and international agreements signed between Saudi Arabia and sovereign nations and/or relevant entities.

3.4 Key Privacy Issues, Conflicts and Public Debates

The PDPL and its Implementing Regulations entered into force on 14 September 2023, but data controllers have until 14 September 2024 to update their current policies and procedures to fully align with the requirements of the law.

The PDPL does specify many "best practice" standards for controllers and public entities, including a standard for legitimate interests and fundamental rights for data subjects, which provide a legal basis for challenging the collection and processing of personal data, including when such data is collected and/or processed by public entities.

4. International Considerations

4.1 Restrictions on International Data Issues

There are restrictions on the transfer of data outside Saudi Arabia; however, the transfer of data outside Saudi Arabia for processing (including storage) of personal data is possible provided such transfer is performed in compliance with the PDPL and any other applicable law in Saudi Arabia.

Part 2 of the Implementing Regulations of the PDPL addresses the transfer of personal data to jurisdictions outside Saudi Arabia. A controller may transfer personal data outside the Kingdom, provided that the transfer or disclosure does not impact national security or vital interests of Saudi Arabia or otherwise violate any applicable law in Saudi Arabia. Any transfer should be limited to the minimum necessary to achieve the purpose of the transfer.

Any transfer should not impact the privacy of data subjects, or otherwise undermine the level of protection guaranteed for personal data under the PDPL by ensuring that the transfer will not compromise, at a minimum, the following principles:

- data subject's ability to exercise minimum rights guaranteed and specified under the PDPL;
- data subject's ability to withdraw consent;
- controller's ability to comply with requirements for notifying personal data breaches;
- controller's ability to comply with provisions, controls and procedures for disclosing personal data;
- controller's ability to comply with provisions and controls for destroying personal data; and

- controller's ability to take necessary organisational, administrative and technical measures to ensure the security of personal data.

The NDMO sets out general standards for personal data transfer beyond the geographical limits of Saudi Arabia in order to specify the terms and conditions for cross-border transfer and storage of personal data for both public and private entities while pointing out the sovereignty of personal data. The standards also stipulate the rights of personal data owners, along with general guidelines and exceptions for personal data transfer beyond Saudi Arabia's borders – thereby creating secure processing for personal data and idealising national data privacy and security (see **4.4 Data Localisation Requirements**).

4.2 Mechanisms or Derogations That Apply to International Data Transfers

Article 5 of Part 2 of the Implementing Regulations sets forth certain exemptions for international data transfers where there is an absence of adequate levels of protection for personal data outside Saudi Arabia, but appropriate safeguards are in place to protect the personal data of data subjects. Provided that the regulatory requirements in the country where data is transferred to does not bring any prejudice to the privacy of personal data subjects or the ability to enforce appropriate safeguards, a controller may transfer data if one of the following safeguards is in place.

- Binding common rules, approved by the regulator, are in place that apply to all parties involved in entities engaged in a joint economic activity, including their employees. These rules shall be approved by the competent authority in accordance with requests submitted to it separately in each case.
- Standard contractual clauses, following a standard model issued by the regulator, are in place in the controller's data policy that ensure a sufficient level of protection for personal data when transferred outside Saudi Arabia. As of March 2024, SDAIA has yet to issue the standard model.
- Certifications of compliance with the PDPL, issued by the regulator, together with the enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.
- Binding codes of conduct, which are approved by the regulator, together with the enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

Article 6 of Part 2 of the Implementing Regulations sets forth an exemption for international data transfers where there are no adequate levels of protection for personal data outside Saudi Arabia and no appropriate safeguards in place. In such cases, the transfer or disclosure of personal data outside Saudi Arabia is permitted in any of the following circumstances:

- the transfer is necessary for the performance of an agreement to which the data subject is a party;
- if the controller is a public entity and the transfer or disclosure is necessary for the protection of Saudi Arabia's national security or for the public interest;
- if the controller is a public entity and the transfer or disclosure is necessary for the investigation or detection of crimes, or the prosecution of their perpetrators, or for the execution of penal sanctions; or
- transfer is necessary to protect the vital interests of a data subject that is unreachable.

4.3 Government Notifications and Approvals

See **4.2 Mechanisms or Derogations That Apply to International Data Transfers**.

4.4 Data Localisation Requirements

The PDPL does not stipulate that data must be localised provided the transfer and processing of personal data outside Saudi Arabia is performed in accordance with the PDPL and any other applicable law or regulation applicable to such personal data in Saudi Arabia.

When transferring personal data outside Saudi Arabia, there are special rules and regulations, however, that may apply in addition to, and exclusive of, the PDPL depending on the type of data (eg, health data) or sector (eg, financial), or if the localisation of data is in the national security, or public, interest of Saudi Arabia. Under such circumstances, the transfer and/or processing of personal data may be restricted or prohibited altogether.

4.5 Sharing Technical Details

The National Cryptographic Standards issued by the National Cyber Security Authority establish the minimum technical standards for cryptography for civil and commercial use and to protect the data, systems and national network.

4.6 Limitations and Considerations

Please see **4.4 Data Localisation Requirements**.

4.7 "Blocking" Statutes

Article 24 of the TCIT Law stipulates that after co-ordinating with the competent authorities, the Commission must:

- introduce internet filtering and limit access to specific content on the internet; and
- prevent or restrict access to internet services by using internet gateways.

It is prohibited to by-pass or swindle internet filtering or to provide the means to do so. In addition, the Commission shall set the regulating controls and requirements.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

In September 2023, SDAIA published the first version of its AI Ethics Principles. These principles were issued and published with the aim of:

- supporting Saudi Arabia's efforts towards achieving its vision and national strategies related to adopting AI technology, encouraging research and innovation, and driving economic growth for prosperity and development;
- developing and establishing AI ethics policies, guidelines, regulations and frameworks;
- governing data and AI models to limit the negative implications of AI systems and potential threats;
- helping entities adopt standards and ethics when building and developing AI-based solutions to ensure responsible use thereof; and
- protecting the privacy of data subjects and their rights with respect to the collection and processing of their data.

The AI Ethics Framework applies to all AI stakeholders designing, developing, deploying, implementing, using or being affected by AI systems within Saudi Arabia, including, without limitation, public entities, private entities, non-profit entities, researchers, public services, institutions,

civil society organisations, individuals, workers and consumers.

Seven principles are addressed in the framework:

- fairness;
- privacy and security;
- humanity;
- social and environment benefits;
- reliability and safety;
- transparency and explainability; and
- accountability and responsibility.

In addition, in November 2023, the government announced the establishment the International Centre for Artificial Intelligence Research and Ethics, which aims to advance competencies and legislative frameworks in the field of AI and other advanced technologies.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Other than SDAIA's mandate, there is no specific fair data practice review board. The general rules for digital governance are laid out in the PDPL.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

As mentioned in **1.3 Administration and Enforcement Process**, to enforce the TCIT Law, CSTC inspectors must jointly or severally investigate and examine control violations of the provisions of the TCIT Law, by-laws and regulatory decisions. In addition, without prejudice to the relevant legal provisions, the inspectors must:

- inspect the sites of the persons suspected of violating the provisions of the TCIT Law or by-laws during working hours;
- review and take a copy of the documents, systems and databases; and
- ask, when needed, for the help of competent security agencies to enable them to implement their tasks.

To enforce the ET Law, the CSTC – in co-operation and co-ordination with competent authorities – are in charge of recording and inspecting violations and making a record thereof. The Commission may seize the equipment, systems and programs used in committing the violation until such violation is decided.

According to Article 20 of the EC Law, any person may appeal a decision issued against them pursuant to the EC Law before the administrative court in accordance with the Law of Procedures before the Board of Grievances.

For the ACC Law, penalties to the violation of any of its articles may range between imprisonment for a period not exceeding one year and a fine not exceeding SAR500,000 to imprisonment for more than 10 years and a fine not exceeding SAR5 million.

Article 35 of the PDPL specifies that any individual that discloses or publishes sensitive personal data either intentionally or for personal benefit may incur a penalty of up to two years of imprisonment and/or a fine of up to SAR3 million without prejudice to any other harsher penalty applicable under any other law for the same act. These penalties may be doubled in the case of repeat offenders.

Article 36 of the PDPL specifies that all violations of the PDPL, other than those covered in Article 35, face penalties that range anywhere from a warning to a fine up to SAR5 million on every person with a special nature or legal capacity

who violates the PDPL. This is, again, without prejudice to any other harsher penalty applicable under any other law for the same act, and the penalty may be doubled in the case of repeat offenders.

5.4 Due Diligence

The PDPL lays out the standards for transferring data outside Saudi Arabia. These standards are evaluated by the regulator, SDAIA, working with the various concerned authorities in each sector. The criteria used to evaluate the sufficiency of transfer of personal data outside Saudi Arabia to a third country include:

- existence of laws that ensure protection for personal data and the preservation of rights of data subjects, at a level of protection no less than that guaranteed under the PDPL;
- rule of law to ensure the rights of data subjects and to preserve their privacy;
- effectiveness of the implementation of personal data protection laws and regulations;
- ability of data subjects to exercise their rights and the availability of the necessary means to file complaints or claims related to the processing of their personal data;
- existence of a supervisory authority responsible for monitoring the compliance of controllers with sufficient minimum personal data protection requirements;
- willingness of the data protection authority to co-operate with SDAIA in matters related to personal data protection; and
- clarity and appropriateness of regulatory requirements with respect to the disclosure of personal data to governmental or supervisory authorities.

The evaluation of these standards may be conducted by SDAIA on the basis of a specific country, sector or international organisation.

The procedures for launching services or products based on customers' personal data or sharing personal data now include the "Privacy Impact Assessment". Before launching a service or product that involves personal data or sharing personal data, the service provider conducts a study to evaluate the impact of the service or product on the privacy of new or existing customers. This study involves identifying and assessing privacy risks, specifying required data, explaining the purpose of data processing, and developing treatment plans. Moreover, the CSTC justifies the need for the Privacy Impact Assessment in each case and has the right to intervene based on the results of said assessment.

5.5 Public Disclosure

Article 20 of the PDPL does specify that a controller must notify the regulator, and individuals affected, of any breach, damage or illegal access to personal data. Although the Implementing Regulations specify what information should be communicated in the case of a breach, there is no specific obligation of disclosure to publicise the breach.

Subject to data qualifying as anonymised data under the PDPL, public disclosure of anonymised data is permitted because the PDPL does not apply to anonymised data.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

As of March 2024, Saudi Arabia has not yet implemented any laws or policies specifically addressing the convergence of privacy, competition and consumer protection in connection with the regulation of tech companies, digital technology or data practices.

5.7 Other Significant Issues

SDAIA is the competent authority to enforce the PDPL for at least the first two years after coming into effect; after this preliminary two-year period, an overview will be conducted to decide if the task of overseeing the enforcement of the PDPL will remain with SDAIA or be transferred to the NDMO.

The National Cybersecurity Authority shall remain the competent authority when it comes to overseeing all cybersecurity matters in Saudi Arabia.

SDAIA and various public entities still need to finalise all applicable rules and regulations that will apply from sector to sector in addition to, and exclusive of, the PDPL. This is particularly true of sectors where sensitive personal data, such as credit data and health data, are collected.

The non-exhaustive list of public entities includes the Ministry of Communications and Information Technology, Ministry of Foreign Affairs, CSTC, Digital Government Authority, NCA, Saudi Health Council, Saudi Central Bank, etc. While some of these have already been concluded with SDAIA, as of March 2024, others in key sectors are pending.

Sector-specific rules and regulations, together with the PDPL and its Implementing Regulations, are required so that industry players are aware of all unique and specific rules and regulations related to data privacy for data subjects in their sector and adapt accordingly.

In addition, SDAIA, as of March 2024, has yet to set forth the standard contractual clauses (Implementing Regulations, Part 2, Chapter 3, Article 5, paragraph 1(b)) or the specifics on the nationality/residency status of a data protection officer, particularly in sectors where big volumes of data are collected and processed or in sectors where high volumes of sensitive personal data are handled.

Trends and Developments

Contributed by:
Alex Saleh, Feras Gadamsi, Ahmad Saleh and Rana Moustafa
GLA & Company

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It provides strategic, cost-effective and forward-thinking legal representation for companies seeking to do business in the Middle East. The firm boasts a diverse portfolio of clients, ranging from start-ups to global enterprises doing business in the Middle East. GLA's practice consists of a full-service law firm that handles everything from simple advisory work to complex contentious and non-contentious matters. With extensive experience advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the United Arab Emirates (UAE) – as well as in Egypt and Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area for the firm, considering the expansion and revamping of applicable laws and regulations across the GCC.

Authors

Alex Saleh is a founder and managing partner of GLA & Company and takes a leading regional role in the firm's M&A and private equity practice. With more than 25 years of experience in both the Gulf Cooperation Council and the USA, he has accumulated sizeable expertise in the areas of banking and finance, M&A, capital market deals and infrastructure projects. His experience garners praise from the leading legal directories and his transactions are regularly noted by the same institutions and organisations.

Feras Gadamsi is a partner based in the firm's Dubai office, leading GLA & Company's global technology, data and privacy practice. Feras also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations, and audits. He started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. Immediately prior to joining the firm, Feras served as Regional General Counsel at IBM. He was formerly Uber's lawyer in the MEA region, serving as General Counsel for Middle East and Africa, Oracle Cerner's Regional General Counsel, and served as CLO and Head of Policy for a Dubai-based start-up.

Contributed by: Alex Saleh, Feras Gadamsi, Ahmad Saleh and Rana Moustafa, **GLA & Company**

Ahmad Saleh is a senior associate at GLA & Company and an active member of the firm's corporate and disputes practice, where he focuses on M&A and other local and cross-border transactions. Since joining the firm, Ahmad has successfully advised multinational clients across various industries, including banking and finance, private equity and capital markets, food and retail, and government contracting. He has recently been working on complex contractual disputes for major construction projects in Kuwait, including representation as local counsel in arbitral and other ADR forums. Ahmad has co-authored numerous articles, including an overview of Data Protection & Privacy laws and regulations in Kuwait.

Rana Moustafa is an associate at GLA & Company with extensive experience in international and domestic commercial disputes. Rana's experience spans across the GCC and Europe, representing clients in Kuwait, Lebanon, Qatar, United Arab Emirates, Saudi Arabia, Egypt and France. She has experience in international and domestic arbitration, working on matters held under the auspices of ICC/DIFC-LCIA/CRCICA/DIAC/ICSID and CAS. Rana extended her experience in data protection while working on matters related to data protection disputes, data protection framework at the workplace and data protection policies for clients. She is a member of the Egypt Bar Association and is currently studying for the French Barreaux.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait +(965) 669 55516
UAE +(971) 54 997 4040
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

Digital Transformation in Saudi Arabia

As part of Saudi Arabia Vision 2030 ("Vision 2030"), Saudi Arabia has fully embraced the digital age, and the country's digital transformation is leaving a lasting impression on its citizens, residents, visitors and outside observers globally.

At the heart of Saudi Arabia's digital transformation is a multifaceted approach that spans various sectors. The government's commitment to incorporating technology into its operations has been a driving force behind this evolution. From implementing smart city initiatives to digitising public services, Saudi Arabia has demonstrated a vision beyond mere modernisation. The digital revolution seeks to create a more efficient, responsive and interconnected administrative framework.

In the private sector, Saudi Arabia has been equally proactive in leveraging technology to drive innovation and economic growth. Initiatives that incentivise and nurture the development of tech start-ups and foster an ecosystem conducive to digital entrepreneurship have positioned Saudi Arabia as a regional leader in the digital landscape, from fintech to the automotive industry.

However, Saudi Arabia's digital transformation is not solely about technological advancements; it is fundamentally about improving the quality of life for its citizens. Technology integration aims to simplify processes, reduce bureaucratic hurdles, and enhance overall efficiency.

Saudi Arabia's digital transformation is also about the establishment of bodies within the country that specialise in developing the rules and regulations required to integrate technological advancements into society in a responsible manner. Initiatives like the establishment of the Saudi Data and Artificial Intelligence Authority (SDAIA) and the National Transformation Programme (NTP) have laid the groundwork for a comprehensive and strategic approach to digital evolution.

This chapter of the guide will explore some key legal and regulatory milestones that have played a pivotal role in shaping Saudi Arabia's digital landscape, including personal data and the development and deployment of artificial intelligence (AI) in Saudi Arabia. It will also explore what Saudi Arabia is doing to ensure that the legal regime and the regulators tasked with monitoring further developments stay ahead of and in line with the advancement and use of technology in Saudi Arabia.

Significant developments in the regulatory landscape in Saudi Arabia

On 14 September 2023, the Personal Data Protection Law (PDPL) came into effect. In addition, SDAIA issued the Implementing Regulations of the Personal Data Protection Law (the "Regulations") and the Regulations on Personal Data Transfer outside the Geographical Boundaries, which came into effect concurrently with the PDPL. Companies have a one-year grace period from the effective date to align their existing privacy policies with the PDPL and the Regulations.

The PDPL and the Regulations govern all aspects of processing personal data, including sensitive personal data. The law also addresses the processing of special types of data such as health data, genetic data, credit data, and data of minors. Much like the GDPR, it provides companies with rules related to the requirement for consent and circumstances for offshore data transfer.

The responsibilities outlined in the PDPL apply to all entities operating in Saudi Arabia or those processing the personal data of Saudi citizens, residents and visitors, excluding individual and non-commercial entities. Under the PDPL and the Regulations, data controllers must adhere to the provisions of the PDPL. Data controllers are permitted to collect personal data only in compliance with the PDPL, and they must ensure that all personal data processing, whether conducted internally or through a third-party processor, aligns with the PDPL regulations.

The concept of processing under the PDPL is comprehensive, covering any action applied to personal data, whether manual or automated. As a result, the PDPL applies to all personal data processing activities within Saudi Arabia and the processing of personal data related to individuals accessing data in Saudi Arabia by foreign entities.

The primary beneficiaries of the PDPL are the individuals from whom the personal data is derived. The law is designed to protect the privacy rights of Saudi residents, ensuring that their personal data is handled responsibly and in accordance with established regulations.

SDAIA AI Ethics Framework

SDAIA has been instrumental in setting guidelines and policies to govern the ethical use of artificial intelligence (AI). This reflects Saudi Arabia's awareness of the need for responsible development and deployment of advanced technologies.

Before 2023, Saudi Arabia had yet to have a comprehensive national AI-specific regulatory framework, but there were discussions about developing guidelines and policies to govern the ethical use of AI.

On 14 September 2023, SDAIA published its AI Ethics Framework version 2.0 (the "Framework"), which focused on helping entities develop responsible AI-based solutions that limit the negative implications of AI systems while encouraging innovation. AI is defined under the Framework as "a collection of technologies that can enable a machine or system to sense, comprehend, act, and learn".

AI has rapidly become an integral part of various sectors and industries. Society's rapid deployment and adoption of AI are influencing decision-making processes and helping to reshape both existing and future interactions between technology and society. As AI systems continue to advance, it is crucial to prioritise the principle of fairness to prevent bias, discrimination and stigmatisation in their design, development, deployment and use. This commitment to fairness is essential to avoid perpetuating historical disadvantages and to ensure that AI benefits all segments of society.

The Framework developed by SDAIA is, in part, issued to ensure fairness in AI systems as these systems are developed and deployed in Saudi Arabia. The Framework's evolution, as AI is used more in day-to-day life in Saudi Arabia, revolves around the following key principles and axes.

- *Inclusive standards* – When designing and developing AI systems, the Framework emphasises that it is paramount to establish just, fair and non-biased standards. These standards should be objective and representative of the diversity present in society. The functionality of AI systems should not be confined to specific groups based on characteristics such as gender, race, religion, disability, age, etc.

- *Transparent motivations* –AI system owners must clearly articulate the purpose of utilising sensitive personal data, highlighting potential risks and benefits. Transparent communication about the motivations, intent and use of sensitive personal data helps build trust and ensures that the deployment of AI systems aligns with ethical considerations.
- *Cleansed and representative data* –To foster fairness and inclusiveness, AI systems should be trained on datasets free from bias and representative of all affected minority groups.
- *Non-correlative algorithms* –Algorithms form the backbone of AI systems, and it is imperative to construct them in a manner that avoids bias and correlation fallacies. Developers should be vigilant in building algorithms free from inherent biases and that do not contribute to reinforcing stereotypes or discriminatory practices.
- *Humanity* – The humanity principle advocates for an ethical methodology in building AI systems rooted in fundamental human rights and cultural values. The goal is to generate a positive impact on individuals and communities through a human-centric design approach.
  (a) *Reliability and safety* – AI systems must adhere to set specifications, ensuring consistent behaviour as intended by designers. Reliability is measured by consistency, instilling confidence in the system, while safety ensures that AI systems do not pose risks to society or individuals.
  (b) *Accountability and responsibility* – Aligned with the fairness principle, accountability holds all stakeholders responsible for ethical decision-making in AI systems. This principle emphasises the need for mechanisms and controls to prevent harm and misuse, making designers, vendors, developers and assessors ethically liable for potential risks and adverse effects.

One of the key ethics and standards stated in the Framework and the list above, and worthy of discussion, is *algorithm auditing* development.

As algorithms increasingly influence decision-making processes in various domains, the need for transparency, accountability and fairness has given rise to algorithm auditing.

Algorithm auditing involves a systematic evaluation of algorithms to ensure they meet predefined ethical and performance standards. This process is essential for uncovering biases, discrimination and unintended consequences that may arise from algorithmic decision-making. With algorithms influencing areas ranging from finance and hiring to criminal justice, the significance of algorithm auditing cannot be overstated.

One of the primary motivations behind algorithm auditing is identifying and mitigating biases present in algorithms. Bias can inadvertently be introduced during the development process or be learned from historical data, leading to discriminatory outcomes. By conducting thorough audits, organisations can uncover and rectify biased decision-making, promoting fairness and equity in algorithmic systems.

Algorithm auditing contributes to transparency, allowing stakeholders and the public to understand how algorithms function and make decisions. Transparency is crucial for building trust, especially when algorithms impact individuals' lives. Moreover, auditing enhances accountability by holding developers and organisations responsible for the consequences of algorithmic decisions.

As AI applications become more sophisticated, the ethical implications of algorithmic decision-making become more pronounced. Algorithm auditing plays a pivotal role in ensuring that AI systems adhere to ethical standards and do not compromise privacy, security or human rights. By scrutinising algorithms, auditors can identify and rectify ethical lapses before they result in adverse outcomes.

In response to the growing importance of algorithmic transparency and accountability, regulatory bodies in the country, such as SDAIA, are beginning to enact laws requiring organisations to audit their algorithms. Compliance with these regulations is not only a legal requirement but also a demonstration of commitment to responsible AI practices.

Algorithm auditing is not without its challenges. The dynamic and evolving nature of algorithms and sheer complexity of AI systems makes auditing a demanding task. The lack of standardised auditing procedures and tools further complicates the process. However, ongoing research and collaboration within the industry are working towards establishing best practices for algorithm auditing.

Development of AI recruitment tools

AI tools are increasingly being used for automated screening of resumes and applications. These tools can analyse and match candidate profiles with job requirements, streamlining the initial stages of the recruitment process.

Chatbots powered by AI are utilised for initial candidate interaction. They can engage with applicants, answer queries, and collect preliminary information, providing a more efficient and responsive recruitment experience.

Nonetheless, AI tools are incorporating predictive analytics to assess the likelihood of a candidate's success in a particular role. This involves analysing historical data to predict future job performance and cultural fit. Further, AI tools are being developed with a focus on mitigating biases in the recruitment process. This includes addressing gender, ethnic and other biases to promote diversity and inclusivity.

Given the rise of remote work, AI tools are facilitating remote hiring processes. This includes virtual interviews, online assessments and collaborative tools for remote team evaluation.

AI Trust, Risk and Security Management (TRiSM)

In the swiftly digitising landscape of Saudi Arabia's economy, AI TRiSM emerges as a safeguard for trust and security within AI systems. As the Vision 2030 initiative propels the nation towards technological leadership, the imperative of ensuring transparency, fairness and security in AI becomes crucial. With generative AI anticipated to revolutionise 70% of new web and mobile app development by 2026, the role of AI TRiSM becomes indispensable in steering this transformative journey.

Metaverse-related projects

The Saudi Central Bank was involved in Project Aber, which concentrated on assessing the viability of digital currencies for facilitating cross-border payments with the United Arab Emirates. It is likely that the Saudi Central Bank will continue to be involved as the United Arab Emirates introduces its digital currency. Reports indicate that Saudi Arabia has allocated a substantial investment of USD1 billion in projects associated with the metaverse. This underscores the jurisdiction's evident comprehension of the piv-

otal role the digital economy is poised to play within the framework of Vision 2030.

Conclusion

Saudi Arabia is actively navigating the evolving landscape of data protection and AI with a keen eye on rapidly satisfying, and perhaps exceeding, international trends and developments. Saudi Arabia recognises the critical importance of safeguarding personal data and fostering responsible AI practices, and it is putting together a regulatory and legal scheme that is nimble enough to pivot at the pace of business while simultaneously safeguarding the balance between individual and commercial interests. The implementation of comprehensive data protection laws aligns with global efforts to empower individuals with greater control over their personal information.

The active participation of Saudi institutions, such as the Saudi Central Bank, in initiatives like Project Aber and investments in metaverse-related projects, underscores Saudi Arabia's strategic goals for being at the forefront of technological innovation. As Saudi Arabia progresses on its transformative journey as outlined in Vision 2030, the harmonisation of AI advancements with robust data protection measures plays a pivotal role in shaping a digitally resilient, and ethically grounded, future for the nation.