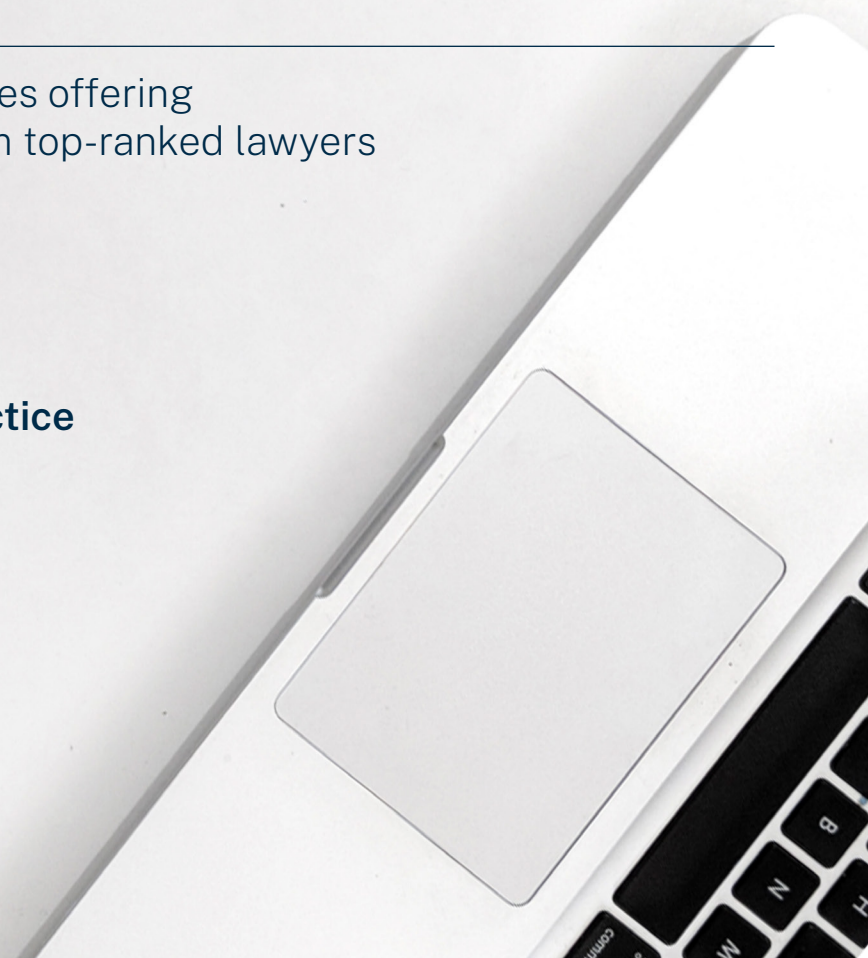
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Saudi Arabia: Law & Practice
Alex Saleh, Asad Ahmad,
Shahad Al Humaidani
and Khaled Al Khashab
GLA & Company



SAUDI ARABIA

Law and Practice

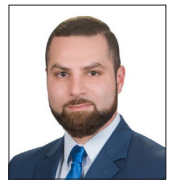
Contributed by:
Alex Saleh, Asad Ahmad, Shahad Al Humaidani and Khaled Al Khashab
GLA & Company

Contents

GLA & Company is a regional law firm based in the UAE, and 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. 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 in advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the UAE – as well as in Egypt and Bahrain – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy is an area of particular focus 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.



Asad Ahmad is the legal director and head of the antitrust and competition practice at GLA & Company, and leads the firm's regional practice across Kuwait, Saudi Arabia, Qatar, the UAE, Egypt, and COMESA. He advises clients on merger control, competition compliance and regulatory matters, securing major clearances and handling high-profile investigations. Asad also leads GLA's data privacy team, guiding multinational clients on regulatory compliance and data protection strategies. A dedicated mentor and thought leader, he contributes to legal publications, conducts webinars and actively engages with competition regulators, reinforcing GLA's reputation as a leader in antitrust and competition law.

Shahad Al Humaidani is an associate at GLA & Company's Riyadh office. Shahad has worked in both the governmental and private sectors in KSA, and has experience in advising on capital market, corporate and commercial transactional and advisory matters, including due diligence exercise, corporate governance and mergers and acquisitions.

Khaled Al Khashab is an associate of GLA & Company. He fulfils a role within the GCC-focused M&A, capital markets and finance teams. Khaled's experience with high-profile clients in different sectors includes F&Bs, hospitality, pharmaceuticals, technology and banking. He also acted as a counsel for the multimillion-dollar start-up Trella, a fast-growing trucks and shipment management tech company.

GLA & Company

Alex Saleh
Managing Partner

Tel: +965 669 55516
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

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

The most notable of these laws is the Personal Data Protection Law, issued by Royal Decree M/19, and its amendments (together with the Implementing Regulations, the PDPL), which came into force on 14 September 2023.

Other significant laws and regulations related to the protection and privacy of data in KSA include:

- Telecommunications and Information Technology Law No M/160 of 1443 (the "TCIT Law");
- Electronic Transactions Law No M/18 of 1428 (the "ET Law");
- Anti-Cyber Crime Law No M/17 of 1428 (the "ACC Law"); and
- Electronic Commerce Law No 125 of 1440 (the "EC Law").

Also, in August and September 2024, the Saudi Data & AI Authority (SDAIA) issued several new regulations to enhance and streamline the data privacy framework in KSA. These regulations include:

- regulation on personal data transfer outside KSA;
- rules for appointing personal a data protection officer;
- a data sharing policy;
- elaboration and developing privacy policy guidelines;
- minimum personal data determination guidelines;
- guidelines for binding common rules (BCR) for personal data transfer;
- standard contractual clauses for personal data transfer;
- personal data destruction, anonymisation and pseudonymisation guidelines;
- guidelines on personal data disclosure cases;
- guidelines on personal data-processing activities records; and
- a procedural guide for personal data breach incidents.

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

The policies, procedures, standards and guidelines are vast. However, the most relevant to data protection and privacy 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 KSA;

- children's and incompetents' privacy protection policy; and
- guidelines and specifications on data management governance and personal data security.

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

1.2 Regulators

The SDAIA is the regulatory body 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 regulations and the application of the PDPL to the National Data Management Office (NDMO), the regulatory subdivision of the SDAIA.

The Communications, Space and Technology Commission (CSTC, or the "Commission") is responsible for the enforcement of both the TCIT Law and the 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 Enforcement Proceedings and Fines

In respect of both the TCIT Law and the 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.

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

- the place and time of the alleged violation;
- the name, identification, address and telephone number of the complainant;
- relevant identifying information about the entity that the complainant is lodging the complaint against;
- a 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 the SDAIA.

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

1.4 Data Protection Fines in Practice

The PDPL has been in full effect since 14 September 2024, after the elapsing of the grace period mentioned in **1.1 Overview of Data and Privacy-Related Laws**. The PDPL establishes a framework for data protection within KSA, outlining specific penalties for non-compliance. Notably, the PDPL prescribes fines of up to SAR3 million and potential imprisonment for up to two

years for the unauthorised disclosure or publication of sensitive data with intent to harm the data subject, or for personal gain. Further, an SAR5 million fine shall be imposed on every person with a special natural or legal capacity who violates any of the provisions of the PDPL. The fine penalty may be doubled in the event of a repeat violation, even if it results in exceeding its maximum limit, provided that it does not exceed double this limit.

Given the recent implementation of the PDPL, there is limited publicly available information regarding notable administrative proceedings or fines imposed by the SDAIA to date. PDPL cases are expected to occur in the coming years, which will provide clearer insights into the regulatory landscape and the practical application of the PDPL.

1.5 AI Regulation

In September 2024, the SDAIA published the AI Adoption Framework, offering a guiding framework that provides a comprehensive roadmap for the adoption of AI in all sectors. This framework represents a strategic step towards building a knowledge-based society founded on innovation and continuous development. Its goal is to provide necessary guidance and instructions, outline critical steps and procedures, and align with best practices to ensure optimal and responsible AI adoption, thus achieving successful milestones in the transformation towards AI within the ecosystem.

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

- supporting KSA'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 Principles apply to all AI stakeholders designing, developing, deploying, implementing, using or being affected by AI systems within KSA, 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 environmental benefits;
- reliability and safety;
- transparency and explainability; and
- accountability and responsibility.

In addition, in November 2023 the government announced the establishment of 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.

1.6 Interplay Between AI and Data Protection Regulations

Please see **1.5 AI Regulation**.

2. Privacy Litigation

2.1 General Overview

As of January 2025, privacy-related litigation in KSA is still in its infancy. There have been no notable lawsuits related to the PDPL. However, complaints and regulatory actions related to data breaches or violations of consent are starting to emerge.

Currently, most actions related to privacy protection are managed by the SDAIA and the NDMO, which investigate complaints and enforce compliance with the PDPL. Instead of litigation, regulatory fines and investigations have been the primary mechanisms used to address violations.

As data protection awareness continues to rise and the enforcement of the PDPL strengthens, it is likely that litigation will increase. Businesses are expected to face greater scrutiny regarding data breaches and violations of data subject rights, which may lead to more litigation related to compensation or damage claims in the future.

The SDAIA handles all complaints related to the PDPL, and its role will be critical in shaping the future of privacy-related litigation in KSA.

The PDPL aligns with global privacy standards, particularly the GDPR, ensuring protection for cross-border data transfers. KSA's data protection framework reflects international norms, ensuring that data processed within and outside KSA is appropriately safeguarded. The influence of the GDPR can be seen in how Saudi laws regulate data processing and the security of data transfers internationally.

In addition, KSA's Anti-Cybercrime Law, enacted in 2007, plays a significant role in privacy protection. Recent trends under this law highlight an increased focus on privacy protection in the digital space. This includes heightened penalties for privacy violations, and the law continues to evolve in line with technological advancements. In 2024, the government enhanced its monitoring of online platforms, with an increasing number of cases involving cybercrime, such as hacking, illegal data interception and online harassment.

2.2 Recent Case Law

Since the PDPL was enacted in 2023, there has not yet been a significant body of related case law in KSA. Data privacy litigation remains relatively sparse at this stage. The SDAIA has primarily been handling regulatory enforcement, such as investigations and fines related to data breaches and violations of consent. As a result, administrative actions have been the dominant approach to addressing privacy violations, rather than court rulings.

However, as businesses fall under more scrutiny for data protection compliance and data subject rights, it is expected that privacy-related lawsuits will increase. This could mirror trends seen in the EU with the GDPR, where Articles 82 and 83 have shaped jurisprudence concerning compensation for violations. As more cases are brought before the courts in KSA, a similar approach to compensation and penalties may be seen, particularly in relation to data subject harm.

For now, regulatory bodies such as the SDAIA and NDMO continue to enforce the law, and

litigation remains an emerging aspect of the PDPL's development.

2.3 Collective Redress Mechanisms

Currently, KSA does not have formal collective redress mechanisms for privacy-related violations, such as the class action system seen in some EU jurisdictions. The PDPL, which was enacted in 2023, provides a robust framework for individual data protection, but does not currently include provisions for collective actions or class actions for data privacy violations.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

The PDPL seeks to regulate the collection, processing and storage of personal data in KSA, ensuring data privacy and security. This applies to all personal data, including data generated by Internet of Things (IOT) services. IOT is defined as the sensors and devices (things) that are connected to the internet and/or other networks, which helps to create value based on exchanged data, such as easing jobs functions per the NCA's Cybersecurity Guidelines for Internet of Things (the "IOT Guidelines").

The IOT Guidelines aim to provide a comprehensive framework for organisations utilising IOT technologies to mitigate cybersecurity risks. The primary objective is to ensure that IOT systems are secure, resilient and compliant with relevant laws and regulations. These guidelines are designed to address the growing cybersecurity threats associated with the widespread adoption of IOT devices and services, which are increasingly integrated into critical sectors such as healthcare, smart cities and transportation. By establishing best practices across four main domains –cybersecurity governance, cybersecurity defence, cybersecurity resilience, and third-party and cloud computing cybersecurity – the guidelines seek to enhance the overall security posture of IOT ecosystems.

The scope of the IOT Guidelines applies to all organisations in KSA that use IOT technologies, as well as IOT manufacturers developing products and services. The guidelines are non-mandatory but strongly recommended minimising cybersecurity risks. They emphasise the importance of embedding cybersecurity into the governance, development, maintenance and management of IOT systems. The IOT Guidelines also encourage IOT manufacturers to adopt secure-by-design principles and provide consumers with transparent information about the cybersecurity features of their products. This dual focus on both users and manufacturers ensures a holistic approach to IOT cybersecurity.

Data holders – such as organisations that collect, store and process data through IOT devices – are obligated to implement robust cybersecurity measures to protect the confidentiality, integrity and availability of data. This includes maintaining an accurate inventory of IOT assets, enforcing strong identity and access management, and conducting regular vulnerability assessments and penetration testing. Data holders must also ensure compliance with national laws and regulations, such as the PDPL, and adopt privacy policies that inform data subjects about how their data is collected, used and protected. Additionally, data holders are required to establish incident response plans and to ensure business continuity in the event of a cybersecurity breach.

3.2 Interaction of Data Regulation and Data Protection

IOT service providers must ensure that users are informed and give explicit consent before their personal data is collected through IOT devices. The PDPL requires that individuals have the right to access their data and request corrections.

Both IOT providers and data processors must implement robust security measures to protect data against breaches and unauthorised access, as stipulated in the NCA's guidelines. These obligations align with the PDPL's security provisions for preventing data breaches.

The PDPL mandates that personal data be destroyed when it is no longer necessary, which interacts with IOT providers' obligations to ensure that devices or systems do not retain unnecessary data.

The interaction ensures that data protection is not overlooked as IOT technologies expand, balancing innovation with the protection of individuals' rights to privacy and security.

3.3 Rights and Obligations Under Applicable Data Regulation

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 it is collected. However, the controller may, on an exceptional basis, 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, as follows.

- Where the personal data subject consents in accordance with the provisions of the PDPL.
- Where the personal data is publicly available or collected from a publicly available source.
- Where 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 to fulfil judicial requirements in accordance with the provisions set out in the regulations.
- Where 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).
- Where 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.
- Where 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 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 must 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 should be within the reasonable expectations of the data subject.

Internal or External Privacy Policies

Article 12 of the PDPL stipulates that the controller should adopt a personal data privacy policy and make it available to personal data subjects for review prior to collecting personal data. The policy should 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 with the controller, provided that such access does not negatively impact on 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 should 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 KSA;
- 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.

3.4 Regulators and Enforcement

The enforcement of data regulations in KSA involves several regulatory bodies. The primary body responsible for overseeing compliance with data protection laws is the SDAIA, which supervises the implementation of data protection practices. Additionally, the CSTC regulates IOT services related to communications technologies and ensures compliance with related laws.

The NCA ensures that cybersecurity measures are in place to protect data, especially in IOT devices. The MoC enforces data protection laws related to electronic commerce, which also includes services that utilise IOT technology. These regulators collaborate to ensure that IOT providers comply with data protection and cybersecurity requirements.

4. Sectoral Issues

4.1 Use of Cookies

To date, no specific requirements are imposed in KSA for the use of cookies. For the general rules as regards gaining consent in relation to cookies, please see under **Requirements for the Collection, Processing and Use of Personal Data** in **3.3 Rights and Obligations Under Applicable Data Regulation**.

4.2 Personalised Advertising and Other Online Marketing Practices

In relation to marketing purposes, Article 10(2) of the PDPL permits the collection of personal data from publicly available sources without the data subject's consent, as long as the collection and processing are necessary to achieve legitimate interests of the controller, and provided that this does not prejudice the rights and interests of the data subject and that no "sensitive data" is processed. Sensitive data is defined under the PDPL as:

- personal data revealing racial or ethnic origin, or religious, intellectual or political belief;
- data relating to security, criminal convictions and offences;
- biometric or genetic data for the purpose of identifying the person;
- health data; and
- data that indicates that one or both of the individual's parents are unknown.

In such a context, for a legitimate interest to be established, it must outweigh any potential harm to the data subject's rights and freedoms. This is outlined in Article 6(4) of the PDPL. Also, the controller must inform the data subject about the processing activities, including the legal basis for processing, the purpose of processing and the types of data collected; this is required under Article 12 of the PDPL. Accordingly, the data subject has the right to object to the processing of their personal data.

Otherwise – and if the processing for the above purpose cannot be justified under legitimate interests – consent from the data subject is required. Such consent must be informed, meaning the data subject is fully aware of the nature, purpose and consequences of the data

processing activities. This is specified in Article 6(1) of the PDPL.

Informed consent is comprised of the following elements:

- freely given – consent must be freely given without coercion, as outlined in Article 6(1) of the PDPL;
- specific and explicit – consent must be specific to the processing activities and must be explicitly granted, as required by Article 6(1) of the PDPL;
- consent should be given by a person who has full legal capacity; and
- consent should be documented by means allowing future verification.

4.3 Employment Privacy Law

No special regulations explicitly deal 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, a controller's employees should enjoy (at a minimum) the same rights and remedies as under the minimum standards that a data controller uses with data subjects generally. Accordingly, the PDPL does not adversely affect how employment relationships develop in KSA.

4.4 Transfer of Personal Data in Asset Deals

Please see **3.3 Rights and Obligations Under Applicable Data Regulation**.

5. International Considerations

5.1 Restrictions on International Data Transfers

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

The NDMO sets out general standards for personal data transfer beyond the geographical limits of KSA, in order to specify the terms and conditions for cross-border transfer and storage of personal data for both public and private entities, and 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 KSA's borders – thereby creating secure processing for personal data and idealising national data privacy and security.

The Regulation on Personal Data Transfer Outside the Kingdom (the "Transfers Regulation") imposes several restrictions on the international transfer of personal information to ensure that such transfers comply with KSA's data protection standards. According to Article 29 of the PDPL, personal data may only be transferred outside the Kingdom if the receiving country or entity provides an appropriate level of protection that meets or exceeds the standards set by Saudi law.

This requirement is further detailed in Article 3 of the Transfers Regulation, which mandates that the competent authority publish and maintain a list of countries or international organisations that meet these protection standards. If the receiving country is not on this list, the transfer

is generally prohibited unless specific appropriate safeguards are implemented, such as standard contractual clauses, binding common rules, or approval certificates from a licensed body as outlined in Article 4. These safeguards ensure that the data is protected at a level consistent with Saudi regulations, even when transferred internationally.

Before transferring personal data outside the Kingdom, controllers are required to conduct a risk assessment under Article 7 of the Transfers Regulation. This assessment is mandatory for transfers involving sensitive data or when the transfer is made under the exemptions specified in Article 4 of the Transfers Regulation. The risk assessment must evaluate several factors, including the purpose and legal basis for the transfer, the nature of the data and the appropriate safeguards in place to protect the data. Additionally, the assessment must consider the potential material or moral effects of the transfer and the likelihood of risks to data subjects. This ensures that controllers carefully weigh the necessity of the transfer against the potential risks to individuals' privacy and data security. The risk assessment requirement underscores the importance of ensuring that international transfers are conducted responsibly and in compliance with the Transfers Regulation.

Furthermore, the Transfers Regulation allows for exemptions from the general restrictions on international data transfers in specific cases, as outlined in Article 4(2). For example, transfers are permitted for central operations within multinational entities, scientific research or to provide services to data subjects, provided that the appropriate safeguards are in place. However, even in these cases, the data must be limited to the minimum amount necessary to achieve the intended purpose, and the receiving entity must ensure compliance with Saudi data protection standards. If the competent authority determines that the safeguards are inadequate, the transfer may be halted, and the controller must notify the relevant entities under Article 6 of the Transfers Regulation. These restrictions and requirements ensure that international data transfers are conducted in a manner that prioritises the protection of personal data and aligns with KSA's legal and regulatory framework.

5.2 Government Notifications and Approvals

Government approval for certain international data transfers is required under the Transfers Regulation. Transfers to countries or organisations on the competent authority's approved list under Article 3(1) do not need additional approval, but transfers to non-listed countries require appropriate safeguards, such as standard contractual clauses or binding common rules, which may need to be reviewed or approved. As of January 2025, such a list of countries is yet to be published.

For specific cases such as scientific research or providing services to data subjects, the receiving entity must hold an approval certificate from a licensed body under Article 4(2)(E), provided that the transferred data is not sensitive data. Additionally, controllers must conduct a risk assessment for sensitive data transfers as per Article 7.

While not all transfers require explicit approval, the Transfers Regulation ensures oversight through conditions such as exemptions from such approvals and the potential revocation of such exemptions if the stated safeguards are inadequate. Controllers must ensure compliance with the Regulation, which may involve notifying or seeking approval from the competent authority, particularly for sensitive data or transfers to

non-approved jurisdictions. This framework prioritises data protection while allowing international transfers under strict safeguards.

5.3 Data Localisation Requirements

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

When transferring personal data outside KSA, special rules and regulations apply; however, these 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 KSA. Under such circumstances, the transfer and/or processing of personal data may be restricted or prohibited altogether.

From a PDPL perspective, per the August 2024 Regulation on Personal Data Transfer Outside Saudi Arabia, there are no distinct rules for transferring data related to particular sectors; instead, certain types of data are categorised as sensitive, and are subject to stricter transfer requirements. Otherwise, data transfers outside KSA may be permitted subject to certain circumstances. For example, Article 4(2)(C) allows the transfer of sensitive data for central operations within multinational entities, provided that the controller adheres to binding common rules or standard contractual clauses to ensure data protection. Similarly, Article 4(2)(E) permits the transfer of sensitive data for scientific research and studies, but only if the data is limited to the minimum amount required and if the receiving entity has an approval certificate from a body licensed by the competent authority.

Additionally, Article 7 addresses the transfer of sensitive data on a continuous or widespread basis, requiring controllers to conduct a risk assessment before such transfers. This risk assessment must evaluate the purpose and legal basis of the transfer, the nature of the data and the appropriate safeguards in place to ensure compliance with the Regulation. While the Regulation does not explicitly differentiate between sectors, it imposes stricter requirements for sensitive data, which often includes sector-specific information such as health records or financial data. By requiring standard contractual clauses, binding common rules or approval certificates, the Regulation ensures that all sensitive data, regardless of its sector, is transferred outside KSA only under conditions that guarantee an appropriate level of protection.

5.4 Blocking Statutes

KSA has various relevant legal authorities on internet censorship, which are primarily aimed at controlling online content to align with the country's cultural, religious and legal norms. Key legislation on web censorship are as follows.

- ACC: Article 6 prohibits, and prescribes imprisonment and fines as penalties for, the publication, dissemination or promotion of content deemed offensive to public order, religious values or national security. This includes content related to pornography, gambling, blasphemy, defamation and political dissent.
- TCIT Law: Article 24 stipulates that after coordination with the competent authorities the Commission must:
  - (a) introduce internet filtering and limit access to specific content on the internet; and
  - (b) prevent or restrict access to internet services by using internet gateways.

It is prohibited to bypass or deceive internet filtering or to provide the means to do so. In addition, the Commission shall set the regulating controls and requirements.

5.5 Recent Developments

There have been few significant changes to KSA's data protection laws and regulations since 2023, with the primary framework still largely being governed by the PDPL, which was designed to align with international data protection standards. Nevertheless, the most notable development in KSA's data protection regime occurred on 14 September 2024 when the PDPL finally became fully enforceable, marking a significant milestone for businesses operating in KSA. This full enforcement deadline required organisations to ensure compliance with the law's provisions, including implementing robust data protection measures, appointing data protection officers and adhering to strict data transfer requirements.

While no further changes or material effects occurred or have been announced since the full enforcement date, the full implementation of the PDPL represents a critical step forwards in strengthening data privacy and security in KSA.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com