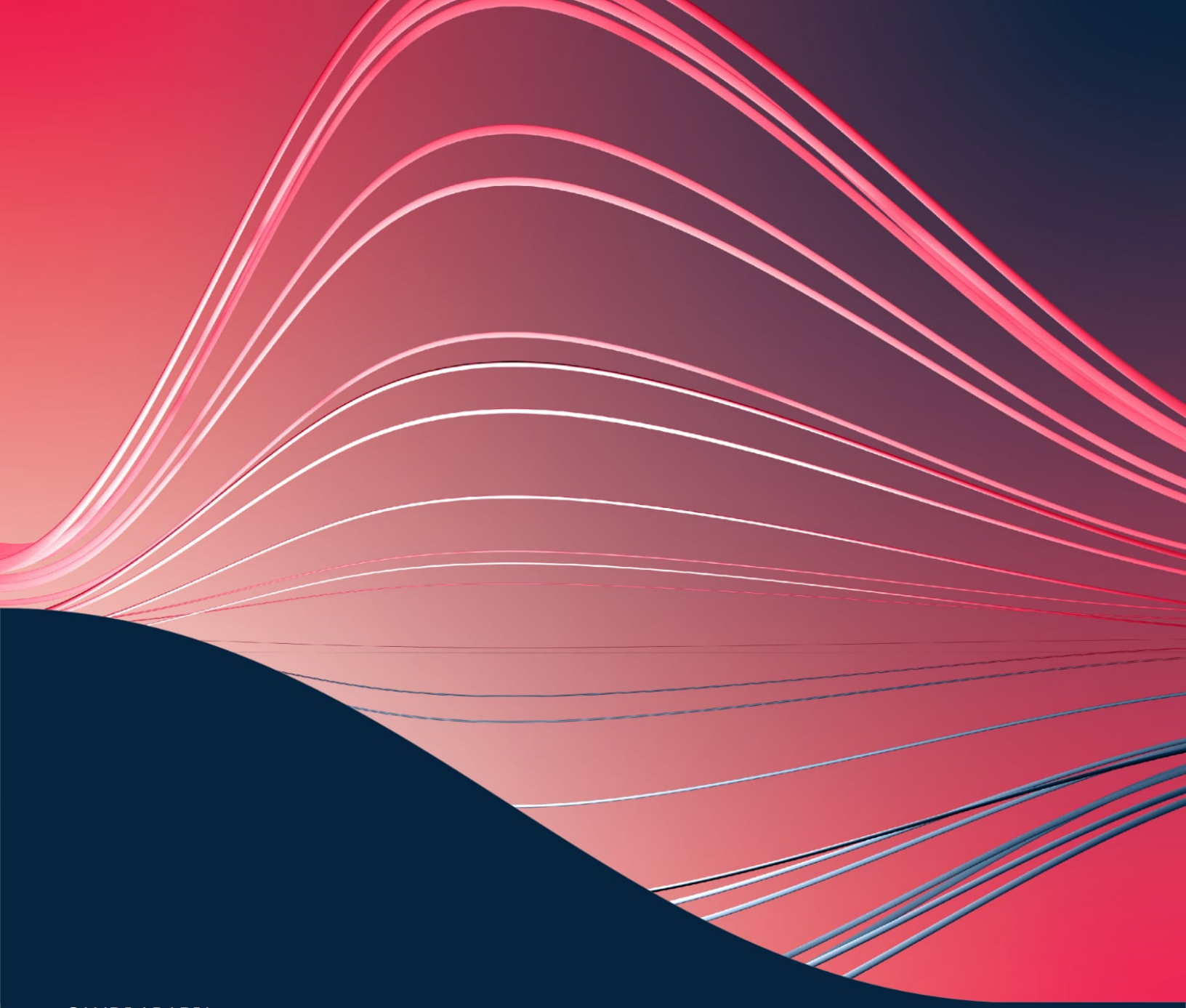


SAUDI ARABIA

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

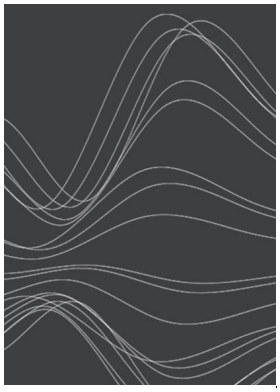
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

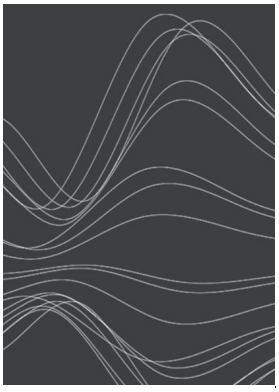
Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Saudi Arabia

LAST MODIFIED 23 FEBRUARY 2024

Data protection laws

The Personal Data Protection Law (issued pursuant to Royal Decree No. M/19 of 9/2 /1443 H (corresponding to 16 September 2021), as amended by Royal Decree No. M /148 dated 5/9/1444H (corresponding to 27 March 2023)) ("**PDPL**") came into effect on 14 September 2023, but data controllers have a further year in which to comply (although that period may be further extended for certain entities). Accordingly, businesses within the scope of the PDPL will have until 14 September 2024 to adjust their status to become compliant with the PDPL.

The Implementing Regulations are also now in force, and provide further detail and guidance on various requirements in the PDPL. It comprises of two connected regulations, with the first being the 'Implementing Regulations to the PDPL', and the second being the 'Regulations on Personal Data Transfers outside the Kingdom' ("**Transfer Regulations**").

The PDPL is a law that applies on a national level and will apply to all sectors, with certain limited exceptions. For this reason, the PDPL will need to be considered in the broader legal and regulatory framework of the Kingdom of Saudi Arabia ("**KSA**"), with other sector specific frameworks such as those issued by the Saudi Central Bank, National Cybersecurity Authority or Communication, Space and Technology Commission ("**CST**").

Definitions

Definition of personal data

Personal data is defined as "*every data – of whatever source or form – that would lead to the identification of the individual specifically, or make it possible to identify him directly or indirectly, including: name, personal identification number, addresses, contact numbers, license numbers, records, personal property, bank account and credit card numbers, fixed or moving pictures of the individual, and other data of personal nature*."

Definition of sensitive personal data

Sensitive data is defined as "*every personal data that includes a reference to an individual's ethnic or tribal origin, or religious, intellectual or political belief, or indicates his membership in nongovernmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates that both parents of an individual or one of them is unknown*."

National data protection authority

The Saudi Authority for Data and Artificial Intelligence ("SDAIA") will be the data regulator for at least two years. During this time, consideration will be given to transferring the competence to supervise the application of the PDPL (and its Implementing Regulations) to the National Data Management Office.

The Saudi Central Bank and the CST both appear to maintain their jurisdiction to regulate data protection within their remit.

Registration

The PDPL has introduced a potential requirement for data controllers to register with SDAIA. It is expected that SDAIA will issue rules regarding such registration and will specify which data controllers must register.

Data protection officers

The PDPL clarifies when a data controller must appoint a data protection officer. This includes where the data controller is a public entity that provides services involving the processing of personal data on a large scale, where the primary activities of the data controller consist of processing operations that require regular and continuous monitoring of individual also on a large scale, and where the core activities of the data controller consist of processing sensitive data.

Collection and processing

The PDPL applies to any processing of personal data related to individuals that takes place in KSA by any means, including the processing of personal data related to individuals residing in KSA by any means by any entity outside KSA.

Under the PDPL, the primary legal basis for processing of personal data is consent of the data subject. However, the PDPL also provides for circumstances where consent is not required for processing of personal data.

Transfer

There are detailed rules relating to the transfer of personal data outside of KSA. The PDPL allows for the transfer of personal data outside of KSA for several purposes (for example, if such action is taken to meet an obligation to which the data subject is a party) and subject to various conditions (for example, the transfer or disclosure must not compromise the national security or vital interests of KSA and be limited to the minimum amount of personal data needed).

Subject to such requirements and conditions, the Transfer Regulations have introduced a number of circumstances where a cross border transfer of personal data is permissible. This includes to countries with appropriate levels of protection and no less than the protections afforded under the PDPL.

However, transfers of personal data to countries which are not deemed as having an adequate level of protection may still be made where "appropriate safeguards" are put in place. If the data controller is unable to use any of the appropriate safeguards, there are still limited cases where cross border transfers are permissible. Such transfers are still however subject to various controls.

In addition, in certain contexts or sectors, specific approvals may be required - for example, in a banking context, approval from the Saudi Central Bank.

Security

Data controllers must take necessary organisational, administrative and technical measures and means to ensure personal data is preserved, including when it is transferred, in accordance with the provisions and controls specified in the Implementing Regulations.

Breach notification

The PDPL imposes data breach notification requirements on data controllers, to notify the regulator (i.e. SDAIA) and / or impacted data subjects, depending on the circumstances. Where a notification is required to SDAIA, the data controller must notify within 72 hours of becoming aware of the breach. Where a notification is required to impacted data subjects, this must be made without undue delay.

In addition, notification obligations may be triggered in specific contexts / sectors – for example, cloud service providers may be required to report security breaches to the CST depending upon the circumstances.

Enforcement

Under the PDPL, the following penalties apply with respect to violations:

- Disclosure or publication of sensitive data in violation of the PDPL with intent to harm the data subject or to achieve a personal benefit, is punishable by imprisonment for up to two years and/or a fine up to SAR 3 million;
- For other breaches of the PDPL not covered by the previous point, this is punishable by a warning or by a fine not exceeding SAR 5 million. Separately, SDAIA has the power to issue warnings / administrative fines of up to SAR 5 million for any other violation, which is appealable. This is without prejudice to any more severe penalty stipulated in another law.

Note, the competent court may double the penalty of a fine for repeat offenders (even if this results in exceeding the maximum limit(s) set out above, provided that it does not exceed double the limit(s)).

Further, the competent courts may order confiscation of funds obtained as a result of committing violations (without prejudice to bona fide third party rights). The competent courts / committee may also order publication of a summary of the judgement or decision at the violator's expense.

Any person who suffers harm as a result of violation of the PDPL has a right to claim compensation before the competent court for material or moral damage.

Electronic marketing

There are specific rules in KSA relating to the use of personal data for marketing purposes. The PDPL and its Implementing Regulations contain various conditions around when personal data may be processed for the purposes of direct marketing. Additional requirements may also apply in certain contexts – for example, in the context of e-commerce activity.

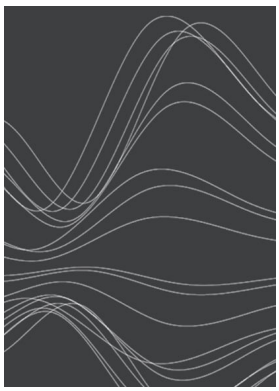
Online privacy

There is no specific legislation in the KSA that specifically regulates the use of cookies.

Data protection lawyers

Andrew Morrison
Senior Associate
DLA Piper
andrew.morrison@dlapiper.com

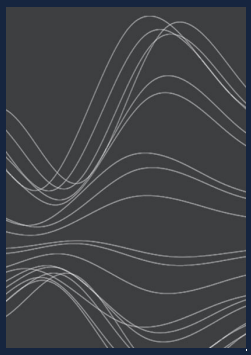
Sam O'Neill
Senior Associate
DLA Piper
sam.oneill@dlapiper.com
View bio



Paul Thevathayan
Associate
DLA Piper
Paul.Thevathayan@alshahranilawfirm.com

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com