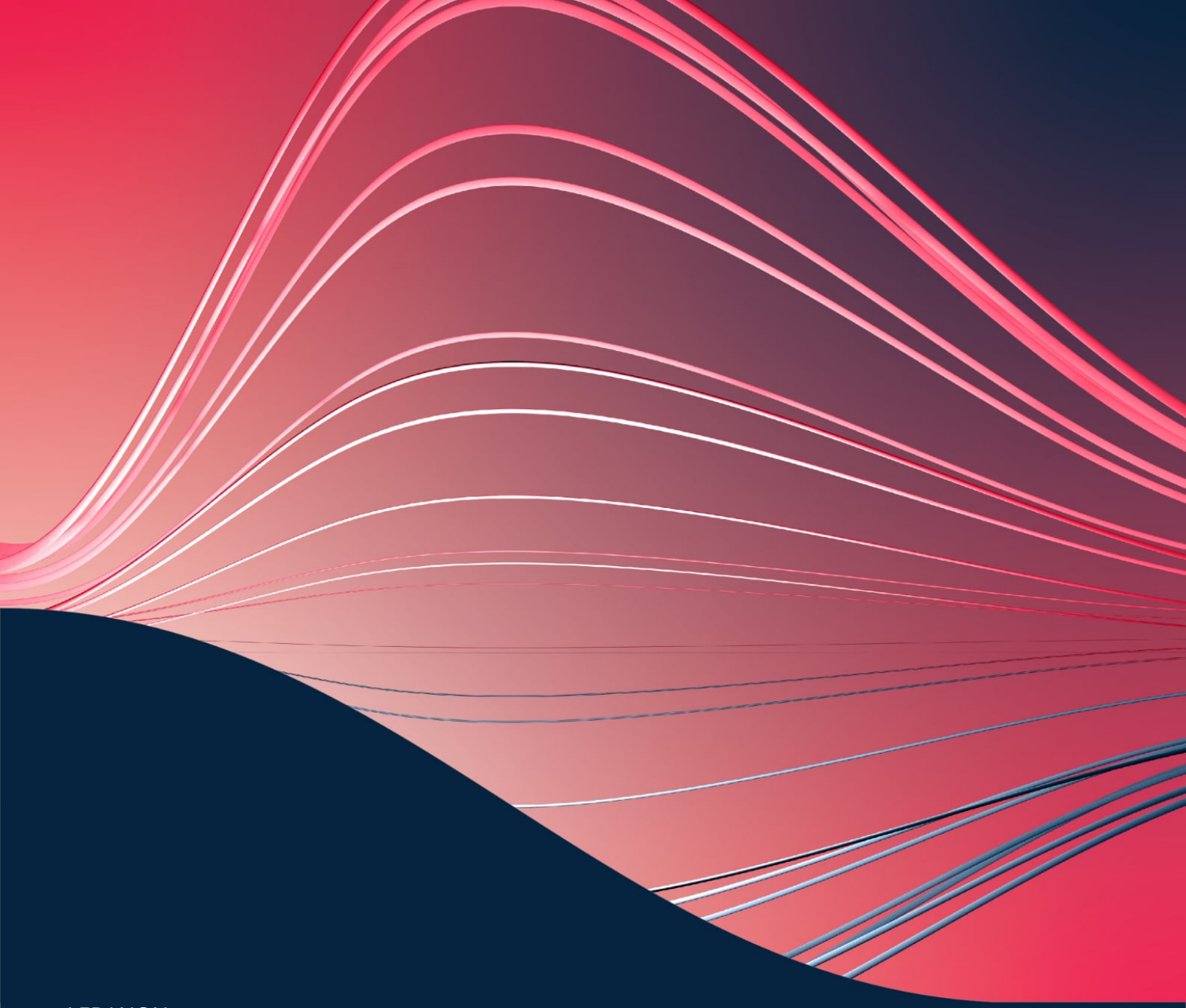


LEBANON

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.

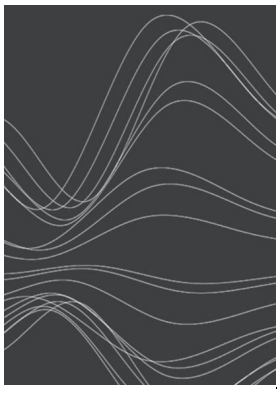
Africa key contact

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

Americas key contact

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

Asia Pacific key contact



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

Europe key contacts

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

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

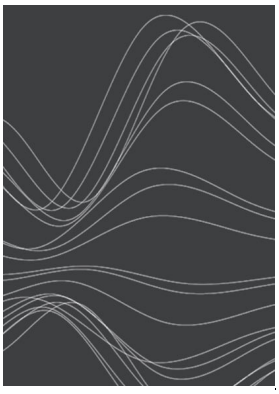
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

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

Editors

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



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

Lebanon

LAST MODIFIED 21 DECEMBER 2022

Data protection laws

Law No. 81/2018 relating to Electronic Transactions and Personal Data Law (the "**Law**").

Definitions

Definition of Personal Data

Personal Data is defined as any information relating to an individual which helps identifying such individual, either directly or indirectly, including by way of comparing or combining information of multiple sources.

Definition of Sensitive Personal Data

The Law brings no definition of sensitive personal data per se. However, it states that the processing of personal data falling within specific categories shall only be processed under a license from the Ministry of Economy and Trade (exceptions apply).

The Law does not attribute a particular name for such category of data, simply listing specific data elements falling within the above defined category, as follows:

- those related to the external and internal security of the State, under the terms of a joint decision of the Ministers of National Defence and Interior and Municipalities;
- those related to criminal offences and judicial proceedings of various natures, under the terms of a decision by the Minister of Justice;
- those related to health, genetic identity, sexual life of individuals, under the terms of a decision of the Minister of Public Health.

National data protection authority

There is no National Data Protection Authority in Lebanon.

The Ministry of Economy and Trade is responsible for issuing permits and licenses for the processing of personal data when required under the Law.

Registration

Any person or entity wishing to process personal data must file a declaration before the Ministry of Economy and Trade obtaining a permit issued against receipt of such declaration, unless:

- when the data subject has agreed in advance to the processing of their personal data.
- when processed by public authorities, within their prerogatives;
- when processed by Non-Profit Organizations in relation to the members and clients thereof, within the scope of the normal and legal exercise of their functions;
- when processed for the purpose of keeping dedicated records required under the provisions of applicable laws and regulations, for the purpose of informing the public and which data can be accessed by any person having a legitimate interest;
- when processed by educational institutions in relation to their students and pupils, for educational or administrative purposes;
- when processed by institutions, commercial companies, trade unions, associations and liberal professionals in relation to their employees and members, within limits and for the needs of exercising their activities in a legal manner;
- when processed by commercial entities, associations, organizations, trade unions and liberal professionals in relation to their clients and customers, within limits and for the needs of exercising their activities in a legal manner.

Data protection officers

The Law brings no definition of data protection officer.

Collection and processing

Processing of Personal Data is defined as any action or set of actions performed on the data regardless of the medium used, including data collection, recording, organization, storage, adaptation, modification, extraction, reading, use, transmission, copy, dissemination, deletion, destruction or otherwise disposing of it.

The Law states that personal data shall be collected faithfully and for legitimate, specific, and explicit purposes. In addition, the data must: be appropriate; not exceed the set purposes; be correct and complete; and remain on a daily basis as relevant as possible.

Data controllers, or their representatives, have an obligation to inform data subjects of the following:

- the identity of the data controller or the identity of its representative;
- the purposes of the processing;
- the mandatory or optional nature of the raised questions;

- the consequences of non-response;
- the persons to whom the data is to be sent; and
- the right to access and correct information, as well as the means provided for the same.

Transfer

The Law is silent on cross-border data transfers.

Security

The Law does not mandate specific technical security measures. Appropriate security standard is applicable.

The Law requires the data processor to take all measures, in light of the nature of the data and the risks resulting from processing thereof, in order to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorized persons.

Breach notification

Not applicable.

Enforcement

Data subjects are entitled to resort to the competent courts, especially to the Judge of Expedite Matters, for matters related to enforcement of their rights under the Law.

There are no administrative enforcement actions.

Public prosecutor and/or data subjects can start legal proceeding for enforcement of the Law.

Electronic marketing

It is forbidden to communicate unsolicited marketing and advertising emails (SPAM) using a real person's name and address, unless that person has consented to such type of advertising, except for cases where the sender of the unsolicited advertisement has legally obtained the address of such individuals through a previous engagement with them.

The Law provides that any individual shall have the right to object to the processing of their personal data for legitimate reasons, including to the collection and processing of personal data for marketing/promotion purposes (exceptions apply).

Online privacy

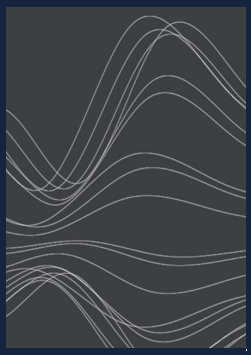
The Law does not identify classes or types of personal data, while making no specific mention to cookies/cookie identifiers or location data. Qualification of online identifiers as personal data shall be assessed by local courts.

Data protection lawyers

Leila Laila
Partner
Head of IP, Franchising and Media
leila.laila@alemlaw.com
View bio

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