



KUWAIT

Data Protection Laws of the World

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. In 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.

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.



Data protection laws

To date, Kuwait does not have a dedicated personal data protection law applying to all juristic or natural persons. However, legislation such as Kuwait Law No. 20 of 2014, on Electronic Transactions (the “**E-Commerce Law**”), includes provisions related to data privacy and data protection of private and public electronic records, documents, and information related to civil, commercial, or administrative transactions conducted in whole or in part through electronic means and applies to private companies, government authorities, public institutions, and non-governmental organizations, and their employees. Furthermore, Kuwait Law No. 63 of 2015, on Combating Cyber Crimes (the “**Cybercrime Law**”) imposed heavy penalties for illegal tampering with or acquisition of personal or governmental data or information.

Additionally, Kuwait Administrative Decision No. 26 of 2024 Concerning the Issuance of the Data Privacy Protection Regulation (“**Data Protection Regulation**”) by the Communications and Telecommunications Regulatory Authority (“**CITRA**”), imposes obligations in relation to data protection on Telecommunication Services Providers and related industry sectors who collect, process, or store personal data, in whole or in part. The Data Protection Regulation applies exclusively to individuals and entities operating as service providers within the telecommunications sector and holding licenses issued by CITRA, and describes the conditions for collecting and possessing personal data and the obligation of a service provider during the provision of the service or after the end thereof, in relation to the collection and processing of such data. The Data Protection Regulation provides a wider ambit of the definition of “service provider” which ranges from traditional telecommunications service providers to anyone who operates a website, smart application or cloud computing service, collects or processes personal data or directs another party to do so on its behalf through information centers owned or used by them directly or indirectly. Furthermore, the Data Protection Regulation indicates that users have a right to withdraw their consent and, consequently, the service provider must delete / destroy the information provided by the user. However, the provisions of the Data Protection Regulation do not apply to natural persons who collect and process personal and family data; or security authorities for the purposes of controlling crimes and the prevention of threats related to public security.

Definitions

Definition of personal data

The Data Protection Regulation defines personal data as information associated with a natural or juristic person whose identity is known or can be directly determined from the data. This includes personal details like name, identity, financial, health, racial, or religious information, as well as data that reveals the individual's location, fingerprint, genetic profile, or any audio file containing the person's voice. It also covers any other identifier that facilitates online interaction with the individual.

Additionally, the E-Commerce Law refers to personal data as considered to include at least personal information about a person's:

- Positional affairs;
- Personal status;
- Health status; or
- Elements of financial disclosures.

These elements are undefined, but broadly construed to encompass any personal information relating to the specified data element.

Definition of sensitive personal data

Kuwaiti law does not define sensitive personal data.

National data protection authority

There is no national data protection authority in Kuwait.

Registration

Not required.

Data protection officers

The Data Protection Regulation does not explicitly outline the mechanisms and obligations for the appointment of data protection officers, per se. However, service providers must provide CITRA with the contact details of their appointed data protection officer when reporting data breaches.

Collection and processing

The Regulation requires that prior to the provision of service, the service providers must:

- Provide all the information about the services to be provided and the terms of service in easy language both in English and Arabic;
- Clarify the purpose of collecting, and method of use of such data to the requester of service; and
- Obtain consent of the requester of service for collection and processing of data and his knowledge and acceptance of all conditions, obligations and provisions for data collection and processing.

Beside the Regulation, the E-Commerce Law includes a general obligation prohibiting Kuwaiti governmental bodies, agencies, public institutions, companies, non-governmental bodies, or employees thereof from collecting or processing any information in an illegal manner without the consent of the concerned person or his or her representative.

Additionally, The entities and individuals subject to the E-Commerce Law are obligated to regularly verify and update the accuracy of personal data and to implement appropriate measures to protect collected or stored personal data. electronic records, including personal information, must be retained in their original form and stored in accordance with the policies and agreements governing electronic transactions, which specify the storage duration. These entities must also restrict employee access to electronic records based on business requirements, ensuring adherence to personal data protection standards.

Transfer of personal data

Pursuant to the Data Protection Regulation, service providers are required to inform their users about the purposes of data processing, provide a description of the categories of data subjects and types of personal data involved, and disclose any transfer of personal data to foreign countries, specifying the names of those countries. The records must also include a general description of the technical and organizational security measures applied during processing activities, including data transfers.

The E-Commerce Law also includes a general obligation prohibiting data controllers from transferring any information in an illegal manner without the consent of the concerned person or his or her representative.

Security

No specific provisions.

Breach notification

The Data Protection Regulation mandate that service providers promptly notify data subjects and relevant authorities in the event of a data breach that may compromise the security of their users' personal data. Service providers are required to report any personal data breaches to both CITRA and the affected individuals within 24 hours of becoming aware of the breach. However, notification to the data subjects is not required if the service provider has implemented appropriate technical and

organizational protection measures, and these measures have been effectively applied to the personal data affected by the breach.

Enforcement

The Data Protection Regulation does not provide specific penalties for breach of prescribed obligations but instead it prescribes to impose penalties and fine as per the CITRA establishing Law, which lays down a range of punishments including imprisonment for a term from one to five years and fine ranging from five hundred Kuwaiti Dinars to twenty thousand Kuwaiti Dinars or a combination thereof.

Violations of the E-Commerce Law are punishable by a maximum of three years imprisonment, and fines of no less than KWD5,000 (US\$17,500) for anyone who discloses personal information without proper consent or a court order. The E-Commerce Law also provides for confiscation of tools, programs or devices used for unauthorized disclosure.

Additionally, the Cybercrime Law imposes severe penalties on anyone who unlawfully accesses a computer, its systems, a data electronic processing system, an automated electronic system, or an information network. Such individuals face imprisonment for up to six months and a fine ranging from KWD 500 (approximately \$1,625) to KWD 2,000 (approximately \$6,500), or either penalty. If the act results in the abolition, deletion, damage, destruction, disclosure, alteration, or republication of data or information, the penalty increases to imprisonment for up to three years and a fine between KWD 3,000 (approximately \$9,750) and KWD 10,000 (approximately \$32,500), or either penalty, especially if the disclosed data is personal. Furthermore, anyone who illegally accesses an information site or system, whether directly, via the internet, or through other means of information technology, to obtain confidential government data is subject to imprisonment for up to three years and a fine of KWD 3,000 to KWD 10,000, or either penalty. If such access leads to the deletion, damage, destruction, publication, or alteration of the data or information, the penalty increases to imprisonment for up to 10 years and a fine ranging from KWD 5,000 (approximately \$16,250) to KWD 20,000 (approximately \$65,000), or either penalty, and these penalties also extend to data and information related to clients' bank accounts.

Electronic marketing

No specific provisions.

Online privacy

No specific provisions.

Data protection lawyers



Alex Saleh
Managing Partner
GLA & Company
alex.saleh@glaco.com
[View bio](#)



Asad Ahmad
Legal Director
Head of Anti-Trust &
Competition
GLA & Company
asad.ahmad@glaco.com
[View bio](#)



Liana Rashid
Trainee Lawyer
GLA & Company
liana.rashid@glaco.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