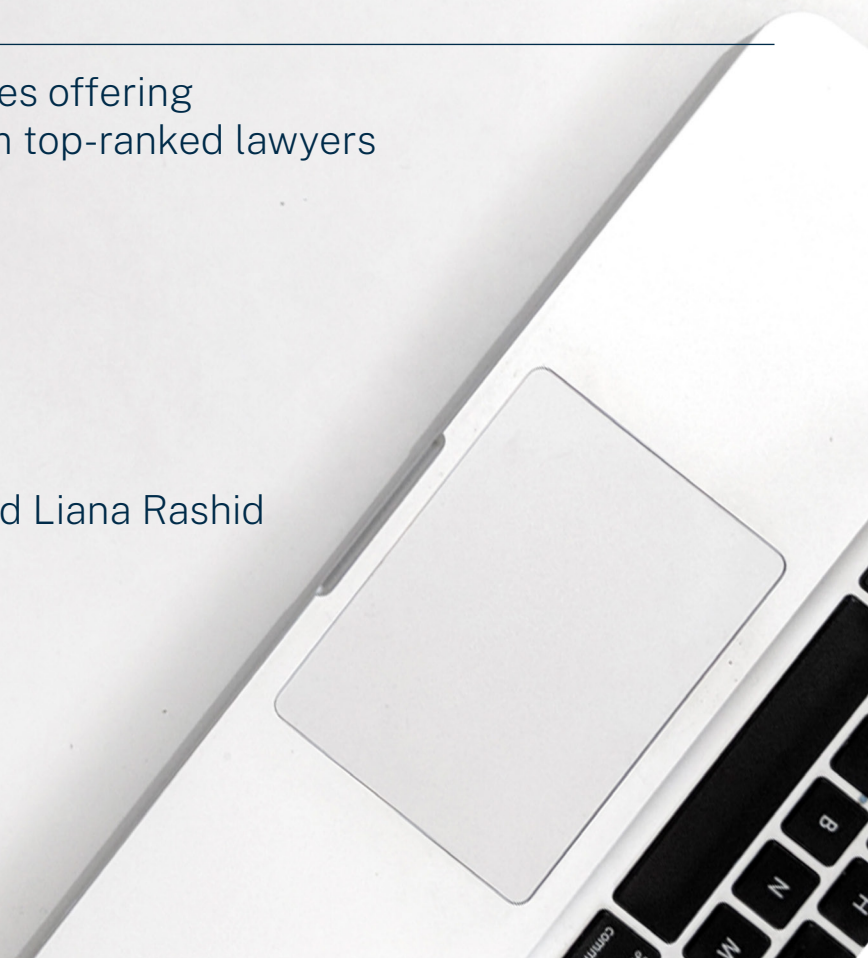
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

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



Kuwait: Law & Practice
Alex Saleh, Asad Ahmad,
Mohammad Al Awadhi and Liana Rashid
GLA & Company

KUWAIT

Law and Practice

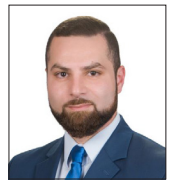
Contributed by:
Alex Saleh, Asad Ahmad, Mohammad Al Awadhi and Liana Rashid
GLA & Company

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.

Mohammad Al Awadhi is a corporate and commercial lawyer as well as a commercial and civil litigator, and represents multinational companies and joint ventures in connection with litigation and possible litigation strategies. He also regularly leads and assists GLA & Company's corporate team in the Kuwait office in their day-to-day matters, with a primary focus on legal issues arising from corporate affairs in Kuwait. Mohammed prides himself in leading the firm on acquisitions in all sectors of the Kuwait and regional market.

Liana Rashid is a trainee lawyer at GLA & Company's Kuwait office. She graduated with honours, and engaged in various university volunteering work and external events in support of good causes while completing her degree. She has practised many legal procedures and gained experience in drafting and reviewing legal documents related to M&A and commercial advisory. She volunteered for the organisation Support Through the Court, located in Sheffield, where she provided assistance to impoverished and disabled individuals with understanding and completing legal documents, attending hearings, and translating legal jargon into Arabic.

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

Legislation Currently in Place

The Electronic Transactions Law under Law No 20 of 2014 (the "E-Transactions Law") and its Implementing Regulations under Decision No 48 of 2014 (the "Regulations") currently regulate the protection of private and public data of electronic records such as signatures, documents and payments.

The E-Transactions Law applies to electronic records, documents and information linked to civil, commercial or administrative transactions conducted via electronic methods, either in part or in full. An electronic record resulting from these transactions comprises data or information that is produced, stored, extracted or copied, either entirely or partially, using electronic means on an electronic medium.

In addition, the Cybercrime Law under Law No 63 of 2015 imposes fines and penalties in relation to the illegal dealing or possession of personal and governmental data.

New Developments Regarding Data Privacy Protection Regulation

The latest amendments to Law No 42 of 2021 pertaining to the Data Privacy Protection Regulation (DPPR) were made under Decision No 26 of 2024, and have notably narrowed the legal framework of the DPPR, which now only applies to individuals and entities operating as service providers and licensees in the telecommunications sector ("Licensees"), possessing licences issued by the Kuwait Telecommunications and Information Technology Regulatory Authority (CITRA). The DPPR defines Licensees as entities or individuals that provide telecommunications services to the public, or that manage, establish or operate telecommunications networks or provide internet services for telecommunications purposes. In addition, the DPPR creates data protection obligations for Licensees engaged in the activities of collecting, processing or storing personal data – as well as the conditions necessary to engage in such activities.

Moreover, the DPPR applies to actions involved in data storage, collection and processing performed inside or outside Kuwait. The CITRA regulations grant Licensees' prospective and existing customers the right to withdraw their consent to any form of use of their personal data; upon the customer's request, the Licensees must accordingly dispose of and destroy all the associated user's data in their possession.

However, it is important to note that the regulations do not apply to the respective state security authorities that hold data for the sole purpose of monitoring and maintaining peace, controlling existing and prospective crimes, and preventing external and internal threats to public security.

Furthermore, CITRA has repealed the Data Classification Policy under Decision No 34 of 2024, which previously classified data into four distinct levels to provide guidance to entities that process, store and transfer data.

That said, the authors do not expect the current data protection landscape to remain this way. The authors understand that the Kuwaiti government has decided to narrow the scope of the DPPR due to the Google Cloud project, which was initiated in Kuwait in January 2024. The Google Cloud project in Kuwait is a collaboration between Google and the Kuwaiti government to build three data centres and a local office.

Google Cloud has formed this strategic alliance with the government of Kuwait to enhance the country's digital transformation and support its goal of becoming a data-driven economy. The partnership includes a roadmap for digitalising citizen services and increasing government employee productivity, with a focus on sectors such as healthcare, education, disaster recovery and smart living.

1.2 Regulators

CITRA and the Central Agency for Information Technology (CAIT) are the regulators responsible for overseeing data protection in Kuwait, pursuant to the E-Transactions Law and the DPPR. CITRA was established under Law No 37 of 2014 (the "CITRA Law") and CAIT was established under Law No 266 of 2006 (the "CAIT Law").

1.3 Enforcement Proceedings and Fines

The CITRA Law

The CITRA Law empowers CITRA to collect information relevant to the telecommunications and IT sectors, and to issue any reports, bulletins and guidelines to users. It also prepares the necessary media programmes to increase public awareness of the importance attached to these sectors and the extent of their influence on social and economic development in the State of Kuwait.

Pursuant to Article 15 of the CITRA Law, all Licensees must adjust their internal policies and rules to any extent necessary to achieve compliance with the provisions of the CITRA Law, no more than one year from the date of publication of the CITRA Law's Executive Regulations. However, under CITRA Decision 68 of 2022, the adjustment period was extended for another 24 months from 13 February 2022.

Pursuant to Article 49 of the CITRA Law, if CITRA receives any complaint about a Licensee's default in the performance of its obligations, a dispute between a Licensee and beneficiary users in relation to the quality and standard of the service being provided or any violations of the licence conditions, CITRA may investigate the complaint and make a decision to either keep the file or notify the Licensee to remove the violation within 90 days.

Under Article 52 of the CITRA Law, CITRA must decide with the Licensee on the procedures of any investigations into complaints, as well as the procedures for the Licensee to follow when complaints are received about it.

Under Article 54 of the CITRA Law, CITRA must ensure that the Licensee complies with all the provisions of the CITRA Law, and may take any actions it deems necessary in order to do so, such as:

- conducting physical examination(s) of the network and telecommunications devices;
- examining the Licensee's technical records to ensure invoices and records are accurate;
- assuring the quality of the services and complaint procedures provided to clients; and
- reviewing the maintenance and failure records of the Licensee to ensure the management service is efficient.

Lastly, under the CITRA Law, CITRA must also guarantee compliance with any international, regional and bilateral agreements to which Kuwait is a party.

Executive Regulations of the CITRA Law Under Decision No 933 of 2015 (the "CITRA Regulations")

Under the CITRA Regulations, CITRA may refer to other competent authorities if – following investigation(s) – there are reasons to suspect a criminal offence. Employees of CITRA are empowered to monitor the implementation of CITRA's laws and regulations. To this end, they have the right to enter places in order to inspect and control any unlicensed communications devices where the following are known or suspected to be present:

- devices or networks;
- communications facilities; and/or
- all or part of the infrastructure used in the communications service.

In the process of doing so, the employees are empowered to:

- request and examine the Licensee's licences, records and documents;
- examine and view any communications equipment related to the provision of the service; and
- view any form of information or documents related to the provision of the services.

The E-Transactions Law

Under Article 37, individuals who unlawfully access, disclose or publish any personal data registered in records or electronic processing systems of the relevant entities, related to the professional affairs, social status, health or financial status of individuals, whether registered with the entities or their employees, without the consent of the data subject or their legal representative, may face imprisonment for up to three years and a fine ranging from KWD5,000 to KWD20,000. Confiscation of the tools, programs or devices used in the commission of the offence may also be ordered.

Under Article 37, entities that collect, register or process any of the personal data stored with them on their electronic records or processing systems, using unlawful methods or without the consent of the person concerned or their representative, or that use the stored personal data for reasons other than those for which it was collected, may face imprisonment for up to three years and a fine ranging from KWD5,000 to KWD20,000. Confiscation of the tools, programs or devices used in the commission of the offence may also be ordered.

The Cybercrime Law

The Cybercrime Law addresses various forms of illegal access to electronic systems and data. It applies to individuals who unlawfully gain access to a computer, system, data-processing system, automated system or information network. The penalty for such actions can include imprisonment for up to six months and a fine ranging from KWD500 to KWD2,000, or either of these penalties. If the illegal access leads to the deletion, alteration, damage or unauthorised disclosure of data, the punishment increases to up to three years in prison and a fine between KWD3,000 and KWD10,000, especially if the data is personal (Article 2).

The law also applies to those who illegally access government systems to obtain confidential information, whether directly or via the internet or other technological means. The penalty includes imprisonment for up to three years and a fine ranging from KWD3,000 to KWD10,000, or either of these penalties. If the access results in the alteration, deletion or disclosure of the data, the punishment escalates to imprisonment for up to ten years and a fine of between KWD5,000 and

KWD20,000, or either of these penalties. This provision also covers data related to clients' bank accounts (Article 3).

Additionally, the law applies to individuals who deliberately modify or destroy electronic medical documents related to medical tests, diagnoses, care or treatment, using the internet or other information technology. Those found guilty of such actions face imprisonment for up to three years and a fine of between KWD3,000 and KWD10,000, or either of these penalties (Article 3).

1.4 Data Protection Fines in Practice

Kuwait data protection regulators do not make public the details of administrative proceedings, or the history of fines imposed on entities/individuals that violate applicable data protection regulations.

1.5 AI Regulation

To date, Kuwait has not issued any dedicated AI legislation. That said, the authors do expect Kuwait to issue new regulations in the near future upon completion of the Google Cloud project.

1.6 Interplay Between AI and Data Protection Regulations

This is not applicable, given that Kuwait has not issued any dedicated data protection legislation addressing AI issues.

2. Privacy Litigation

2.1 General Overview

Please refer to **1.1 Overview of Data and Privacy-Related Laws**, outlining the recent amendments to the DPPR under Decision No 26 of 2024, which have narrowed its scope and apply only to service providers and licensees in the telecommunications sector (specifically, those licensed by CITRA). Additionally, CITRA repealed the Data Classification Policy under Decision No 34 of 2024, which previously categorised data into four levels for processing and transfer guidance.

2.2 Recent Case Law

To date, there have been no notable ongoing litigation cases regarding enforcement of data protection laws and regulations in Kuwait.

2.3 Collective Redress Mechanisms

This topic is not applicable.

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

3.1 Objectives and Scope of Data Regulation

The DPPR applies exclusively to individuals and entities serving as providers within the telecommunications sector and holding licences issued by CITRA ("Licensees"; see **1.1 Overview of Data and Privacy-Related Laws**).

The E-Transactions Law applies to private companies, government authorities, public institutions and non-governmental organisations, and to their employees.

The Cybercrime Law applies to every identifiable natural person.

The Cloud Computing Regulatory Framework (v2.4) issued by CITRA applies to all cloud service providers licensed by CITRA with data centres in Kuwait. Although the Framework governs the licensing and other obligations of these cloud service providers, it also places obliga-

tions on individuals and on public, governmental and private entities in the State of Kuwait who subscribe to cloud services hosting certain types of data.

The CITRA Law applies to CITRA, its personnel and licensees.

3.2 Interaction of Data Regulation and Data Protection

Kuwait Law No 8 of 2016 on the Regulation of Electronic Media (the "Electronic Media Law") applies to and regulates various online platforms, including:

- electronic publishers;
- electronic journalism;
- news agencies;
- news services;
- websites offering electronic commercial advertisements; and
- the digital presence of print newspapers and satellite channels.

However, the law does not apply to personal domains, websites, outlets or electronic accounts that are not operated by individuals with specialised professional expertise. Notably, the Electronic Media Law specifies that the name of the website or media outlet must not violate public order or morals or be identical to an existing site. Thus, media regulation under Kuwaiti law seems to be restricted to media channels that are not privately owned. On the other hand, the data protection requirements under the E-Transactions Law or the DPPR would apply to both private companies and entities offering services to the public.

3.3 Rights and Obligations Under Applicable Data Regulation

The E-Transactions Law

Consent

Under Article 4, individuals are generally not obliged to deal by electronic means except with their consent, and such consent may be inferred through affirmative conduct indicating approval.

Under Article 32, when collecting data (including personal data and data related to individuals' professional affairs, social status, health status or financial status), government authorities, public authorities and institutions, companies, non-governmental entities or their employees ("Entities") are explicitly mandated to secure individuals' consent and to state the purpose behind collecting such data.

Under Articles 32 and 35, Entities must also ensure that consent is obtained when conducting any access, disclosure, sharing or processing of the collected data. These activities must be undertaken by lawful means and be limited to the stated purpose provided to data owners. This is a requirement that pertains to personal data or information stored in electronic records or processing systems that relates to the professional affairs, social status, health status or financial status of individuals that are registered with the Entities.

Data protection

Under Article 35, Entities are required to regularly verify and update the accuracy of personal data or information stored on their electronic records or processing systems. They must also implement appropriate measures to safeguard the collected or stored personal data and information stored on their electronic records or processing systems.

Under Article 2 of the Regulations, the storage and maintenance of electronic records, inclusive of personal data, must preserve their original form, encompassing all associated original data, without compromising the quality or standard of the records. In addition, the storage of electronic records, inclusive of personal data, should align with the policies and agreements established between the parties involved in electronic transactions, specifying the duration for retaining and maintaining such records.

Data subject rights

Article 33 grants specific rights to data subjects concerning their personal data stored in electronic records and processing systems maintained by Entities. Any person with personal data stored by Entities has the right to request access to, as well as a record of, the data or information maintained by that Entity.

Additionally, under Article 36, the data subject has the right to modify or delete their personal data held by any of the Entities, and may also update personal information in the event of changes. Requests for the access, modification or deletion of personal data can only be initiated by the individual to whom the data belongs or by their legal representative (Articles 25–26(1) of the Regulations).

Under Article 26(2) of the Regulations, deleting stored personal data or information is only permissible when correction is deemed necessary; in such cases, the previously stored information must be maintained without any use or handling.

User Right Protection and Regulation of Communications and IT Services ("User Guidelines")

Collection of data

Under Article 2, the Licensee must prepare relevant rules and mechanisms for the sale of its service, either through means of electronic transaction or through telephone communication. CITRA must approve the rules and mechanisms or any amendments to existing contracts of sale in advance, which includes the relevant data collection and storage. Pursuant to Article 3.16, in the case of any such amendment, the following must occur before any enforcement can take place:

- the service user must be notified of the amendment 60 days before the amendment enters into force; and
- the subscriber's written approval or e-signature (using the "Hawyti" application) must be obtained.

Under Article 3.3, the Licensee must verify the validity of the personal information provided by the users of said services; such proof of information (in the form of civil ID, passport or driving licence) may be certified by competent governmental bodies.

Under Article 3.4, before executing the service contract, the mechanism(s) for cancelling the service and any variation(s) to the contractual terms of service must be clearly stipulated.

Under Article 3.6, the Licensee must open an electronic file in which all the information, documents and complaints pertaining to any user(s) are safely stored.

Duties of the Licensee upon users' request of cancellation of service

Under Article 4, the Licensee must facilitate the mechanisms or procedures for such cancellation of service. The Licensee may bind the subscriber with a minimum limit of the service contract term, unless this is approved by the authority. Upon the subscriber's request to cancel the service, the Licensee must verify the identity of the subscriber applying for cancellation.

Dealing with data

Under Article 6, Licensees must adhere to the following requirements.

- Making no collection, use or disclosure of any personal information related to the user without their official approval.
- Not requiring information that is irrelevant in the context of providing services.
- Obtaining the approval of the user before disclosing their information to other parties.
- Taking all security measures with regard to:
  (a) protection of the user's information; and
  (b) protection against the loss, damage or disclosure of such information (or its replacement with any untrue data).

DPPR

Consent

Under Articles 2 and 4 of the DPPR, Licensees must secure user consent prior to collecting and processing their personal data, and must specify the purpose for data collection and processing both before and during the provision of services, as well as after the termination of services.

Data protection

In accordance with Article 5(1-3) of the DPPR, Licensees are required to implement robust measures for safeguarding data from unauthorised access, loss, destruction or damage, with protective measures to include encryption, confidentiality practices and disaster recovery protocols.

Under Article 6 of the DPPR, Licensees must inform both the data subject and CITRA in the case of a personal data breach.

Data subject rights

Under Article 4(3), Licensees must disclose their identity, location and contact information to their users, ensuring that users can readily recognise and reach out to them when required.

Under Article 4(10), users must also be given the right to withdraw consent or to entirely delete their personal information from the Licensee's records.

Under Article 4(11), Licensees are also obliged to notify data subjects if their personal data is to be transferred outside Kuwait.

Under Article 4(12), Licensees must afford their users the right to access or modify stored personal data that is in their possession and is stored with them.

CITRA Cloud Service Providers: Regulations and Commitments

Types of information collected by cloud service providers (CSPs)

Pursuant to the regulations concerning PaaS and SaaS model providers in Article 2, the types of information that a CSP may obtain from users can include (and is not limited to):

- name and email address;
- address;
- payment information;
- internet protocol address ("IP address"); and
- device and browser information.

Obligations in dealing with information
In accordance with the regulations concerning PaaS and SaaS model providers in Article 2, the CSP must describe to the user all information that needs to be collected and inform them as to what information will be collected automatically (as well as where to access and amend such information). Following data collection, the CSP must explain to the user where and how such information may be used.

The CSP may not use this information to locate the identity of the user. The CSP must also inform users of any third-party providers that operate certain services on their behalf – and of their privacy policies – for the purpose of maintaining transparency. The CSP commits to not share, dispose of or sell the user's information with third parties; however, for purposes of improving the service and customer experience, they may be granted access to the user's name, address, phone number and email. In any case, the user must be informed of such.

The user must be notified immediately of any data relocation to new owners as a result of M&A, liquidation or dissolution.

The CSP must be efficient, competent and equipped to detect any fraud, security threats or technical problems.

The subscriber has the right to request the amendment or deletion of their personal data available to third parties or to the CSP. The CSP must also provide clear mechanisms to users for communication regarding the privacy policy.

SaaS model providers must specify in their privacy policy the targeted age group for the collection of data. If the targeted age group is minors, the consent of their guardian must be obtained. The service must abide by any relevant child protection laws of the state.

3.4 Regulators and Enforcement
Besides CITRA and CAIT, the Electronic and Cyber Crime Combating Department (ECCCD) is a specialised department within the Ministry of Interior in Kuwait that is responsible for enforcing Kuwait's cybercrime laws and investigating cyber-related crimes. The ECCCD's main focus is to protect Kuwait's economy and national security – along with the well-being of its citizens and residents – by combating cybercrime and enhancing cybersecurity. The ECCCD is responsible for receiving complaints related to cybercrime, conducting investigations and working with other governmental and non-governmental organisations to combat cyberthreats. The department is also responsible for raising awareness about cyberthreats and providing guidance on how to stay safe online.

4. Sectoral Issues

4.1 Use of Cookies
Pursuant to the Cloud Computing Regulatory Framework, a CSP must contain a clause labelled "Cookies" in its privacy policy, which determines the mechanisms of usage when it comes to:

- log-in authentication;
- security inferences;
- advertisements; and
- personal identification.

The CSP may not use this data to locate the identity of the user and must always make available the types of cookies used by it or by external parties on any platform on which the service operates.

4.2 Personalised Advertising and Other Online Marketing Practices

Spam Messaging

In accordance with Article 12 of the CITRA Regulations, the Licensee must have a database in which the receipt of spam messages is ceased upon the request of the user. Licensees sending messages for commercial purposes must only do so between the hours of 7am and 10pm Kuwait time.

Marketing Practice

Pursuant to Article 14 of the User Guidelines, the marketing practices of Licensees must not exploit any consumer or groups on account of their weaknesses, disabilities, ages or lack of knowledge. They must also not use any means of fraud or deception in the advertising of their products and services.

When it comes to receiving marketing communications or calls, the Licensees must have duly verified the identity of the recipient user. At the beginning of the communication/call, the Licensee must:

- disclose the sender's name;
- disclose the cause for such communication/call; and
- give the recipient user the option to continue with the communication/call or not.

Regulations and Commitments of CSPs

The CSP's privacy policy must inform the user of the procedures to follow should they wish to cancel marketing communication subscriptions.

4.3 Employment Privacy Law

Monitoring of Workplace Communications

Law No 9/2001 Regarding Misuse of Telecommunications and Wiretap Sets governs the matter in question, but there is no specific rule applicable to employee monitoring.

Telephone conversations may be recorded by employers to deal with any grievances from customers or clients, in order to ensure that the calls are dealt with professionally and for the purposes of training only. In some situations, such recordings may be carried out and reproduced for legal purposes upon an order of the competent court in a situation occurring between third parties and company employees.

No applicable laws are in place for monitoring employees' emails in Kuwait. Private life cannot be violated, so the monitoring and recording of such information is considered to be an infringement of rights and a violation of confidentiality, which is guaranteed to individuals under the Kuwaiti Constitution. The courts of Kuwait aim to protect citizens and expatriates from all such violations. The employer can draw up a set of rules and regulations that may govern such monitoring for the purpose of safeguarding their interests. However, they should restrict it to the official work areas and not infringe on privacy rights, including the protection of personal emails. Such rules and regulations will need to be drawn up and made available to the employee in a handbook that is often provided to newly joined employees for them to understand and abide by.

4.4 Transfer of Personal Data in Asset Deals

The E-Transactions Law

Under Articles 32 and 35 of the E-Transactions Law, Entities and their employees are expressly required to:

- obtain individuals' consent before accessing, disclosing or sharing personal data; and

- specify the purpose for collecting and processing such personal data, including processing activities for data transfers.

These activities must be conducted using lawful means and limited to the stated purpose. This applies to personal data or information in electronic records or processing systems concerning the professional, social, health or financial status of individuals registered with these Entities. Consent may be obtained or inferred from affirmative actions indicating approval, as outlined in Article 4 of the E-Transactions Law.

DPPR and the User Guidelines

Licensees have notification obligations, including informing data subjects about personal data transfers outside Kuwait, pursuant to Article 4 of the DPPR. In addition, Licensees are required to establish and uphold a written privacy policy that elaborates extensively on their procedures concerning the collection and processing of personal data, including transfers as part of the processing activities. This policy should be publicly accessible on their website and provided to users and data subjects when entering into service contracts.

5. International Considerations

5.1 Restrictions on International Data Transfers

Please see **4.4 Transfer of Personal Data in Asset Deals**.

5.2 Government Notifications and Approvals

Private Entities covered by the E-Transactions Law typically do not need official approval for international data transfers, unless the data involves state or government-related information in Kuwait.

Licensees may require approval from CITRA to transfer user data internationally, as indicated through consultations with CITRA. However, there is a lack of specific regulations detailing the mechanisms or conditions for such data transfers.

5.3 Data Localisation Requirements

Kuwaiti law does not generally address data localisation requirements, especially after the repeal of the Data Classification Policy. However, certain sector-specific examples, such as healthcare facilities, must maintain a register and database to document patient information in either written or electronic form. The facility's management is responsible for ensuring the safety of these records, and, if the facility ceases operations or changes activities, it must provide patient files or copies upon request (Article 60 of Law No 70 of 2020 on the Medical Profession). While the law does not provide specific mechanisms for data transfers, it is understood from the E-Transactions Law that patient consent is required.

Another example of data localisation is found in Article 80 of Law No 6 of 2010 on Labour in the Private Sector (the "Labour Law"), which mandates that employers must maintain a dedicated file for each employee, containing essential documents such as the work permit, employment contract, civil ID, and records of leave, overtime, work injuries and penalties. Similar to healthcare facilities, this law does not address mechanisms for data transfers but also implies that consent may be required under the E-Transactions Law.

5.4 Blocking Statutes

Kuwait has several laws and regulations related to blocking or censoring web content, some of which concern privacy and data protection. Key examples include the following.

- The Press and Publications Law under Law No 3 of 2006 regulates the publication of printed and electronic media in Kuwait. It includes provisions related to blocking content that violates public order, morals or national security. This law gives the government the power to block websites or other media that violate these provisions.
- The Cybercrime Law criminalises a wide range of online activities, including hacking and online fraud. This law gives the government the power to block websites or other online content that violates its provisions.
- The CITRA Law regulates the telecommunications sector in Kuwait and includes provisions related to blocking or intercepting communications that violate public order, morals or national security. This law gives the government the power to block websites or other online content that violates these provisions.

Among other prohibited content, CITRA receives requests to block web content in Kuwait that violates the public interest (including public morals, Islamic faith teachings and public order). If CITRA receives a request to block or unblock web content, it will take the necessary actions to block web content that contains any prohibited content or to unblock web content in the case of an error in classifying the content as prohibited.

5.5 Recent Developments

Following the repeal of the Data Classification Policy, which previously classified sensitive data into different tiers, the regulatory framework for data storage and transfers has become less clear. Under the former policy, Tier 3 data (private sensitive data) included information such as business plans, internal reports, litigation files, medical records, and criminal fingerprints, which, if disclosed without authorisation, could damage individual privacy. Tier 4 data, considered highly sensitive, included information of a national or governmental nature, and unauthorised disclosure of such data could cause significant harm to privacy.

The Data Classification Policy required that Tier 4 data be stored within Kuwait, while Tier 3 data could be stored in hybrid clouds, both inside and outside Kuwait. Due to the repeal of the Data Classification Policy, the legislative framework surrounding the storage and transfer of sensitive data is now governed primarily by the consent provisions in the E-Transactions Law.

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