KUWAIT

Law and Practice

Contributed by:
Alex Saleh, Feras Gadamsi, Asad Ahmad and Liana Rashid
GLA & Company

Contents

1. Basic National Regime p.5
1.1 Laws p.5
1.2 Regulators p.5
1.3 Administration and Enforcement Process p.7
1.4 Multilateral and Subnational Issues p.8
1.5 Major NGOs and Self-Regulatory Organisations p.8
1.6 System Characteristics p.8
1.7 Key Developments p.9
1.8 Significant Pending Changes, Hot Topics and Issues p.10

2. Fundamental Laws p.10
2.1 Omnibus Laws and General Requirements p.10
2.2 Sectoral and Special Issues p.14
2.3 Online Marketing p.16
2.4 Workplace Privacy p.16
2.5 Enforcement and Litigation p.17

3. Law Enforcement and National Security Access and Surveillance p.18
3.1 Laws and Standards for Access to Data for Serious Crimes p.18
3.2 Laws and Standards for Access to Data for National Security Purposes p.18
3.3 Invoking Foreign Government Obligations p.18
3.4 Key Privacy Issues, Conflicts and Public Debates p.18

4. International Considerations p.19
4.1 Restrictions on International Data Issues p.19
4.2 Mechanisms or Derogations That Apply to International Data Transfers p.20
4.3 Government Notifications and Approvals p.20
4.4 Data Localisation Requirements p.21
4.5 Sharing Technical Details p.21
4.6 Limitations and Considerations p.21
4.7 “Blocking” Statutes p.21

5. Emerging Digital and Technology Issues p.22
5.1 Addressing Current Issues in Law p.22
5.2 "Digital Governance" or Fair Data Practice Review Boards p.22
5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation p.23
5.4 Due Diligence p.23
5.5 Public Disclosure p.23
5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI) p.23
5.7 Other Significant Issues p.23

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It 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 doing business in the Middle East. GLA is 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 Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area 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' experience in both the GCC and the USA, he has accumulated extensive 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.

Feras Gadamsi is a partner in GLA's Dubai office and leads the global technology, data and privacy practice. He was previously Uber's lawyer in the MEA region, and served as Regional General Counsel at IBM, as Oracle Cerner's Regional General Counsel from 2010–2014, and as CLO and Head of Policy for a Dubai-based start-up. He has advised several technology and payments companies throughout the EMEA region. Feras started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. He also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations and audits.

Asad Ahmad is a senior associate at GLA & Company and has been involved in a number of transactional and advisory works in various industries, including logistics, construction, finance, healthcare and education. His practice has involved comprehensive representation with regard to M&A, conducting extensive due diligence exercises in relation to complex transactions, as well as distribution and agency arrangements. Asad has an extensive background in advising on the marketing of securities, corporate governance issues, policies and regulatory compliance, and he has expanded his expertise to include advising on data protection and regulation.

Liana Rashid is a trainee lawyer at GLA & Company. While completing her degree, she undertook numerous volunteering roles both at the university and for external events in aid of a good cause. Liana has a diverse range of experience in the Kuwaiti legal field, including advising on corporate commercial matters and representing high-profile clients in arbitration and litigation proceedings. She also has extensive legal research experience and has already assisted in various high-level corporate transactions taking place in the GCC area.

GLA & Company

Arraya Tower II
36th and 37th Floors
Al Shuhada Street
Sharq
Kuwait
Tel: +965 2291 5800
Web: www.glaco.com

1. Basic National Regime

1.1 Laws

Legislation Currently in Place

The Electronic Transactions Law under Law No 20 of 2014 ("E-Transactions Law") and its Implementing Regulations under Decision No 48 of 2014 ("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 the Data Privacy Protection Regulation (DPPR) Decision No 42 of 2021, introduced by Decision No 244 of 2023, 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 issued the Data Classification Policy ("Policy") under Resolution No 95 of 2021, which classifies data into four distinct levels to provide guidance to entities that process, store and transfer data. It also provides specific guidelines regarding the dealing and storing of said data, depending on its classification level and sensitivity.

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 ("CITRA Law") and CAIT was established under Law No 266 of 2006 ("CAIT Law").

Furthermore, 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 combatting 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.

Relevant Provisions in Relation to Audits and Investigations

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 it receives any complaint about a Licensee's default in the performance of its obligations or 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 upon 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 party.

Executive Regulations of the CITRA Law under Decision No 933 of 2015 ("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.

1.3 Administration and Enforcement Process

Chapter 6 of the CITRA Regulations delineates the conditions and processes necessary for the investigation of grievances or disputes submitted to CITRA, by forming a Dispute Resolution Committee.

Formation of the Dispute Resolution Committee

Under Article 33 of the CITRA Regulations, the chair of the Authority must form a committee from outside the Authority ("Committee") to resolve disputes between Licensees and beneficiaries and decide on the grievances and complaints submitted to CITRA (including those in relation to other Licensees).

Conduct of the Committee

Under Article 34 of the CITRA Regulations, the Committee must conduct its activities in accordance with the following rules:

- one registrar must be appointed and designated to record the disputes received by CITRA and another one must be appointed to record the grievances;
- grievances must be submitted within 30 days of the date of notification of the action or decision by the Licensee to which the grievance relates;
- a grievance/dispute writ must comprise the details of the grievance/dispute, the grievant/claimant and the respondent; and
- the secretary must present the writ on the dispute to the chair of the board to set a hearing date to consider such.

Decision of the Committee

Pursuant to Article 35 of the CITRA Regulations, CITRA – following the direction of the Committee – must decide on the disputes or grievances presented before it by coming to a reasoned decision within one month of the date of submission of the dispute (if it did not escalate to the Committee) or grievance/dispute writ. The Authority must then notify the parties concerned of its decision within a week of the date of its issue.

Appeal and Referral to Judiciary

Under Article 37 of the CITRA Regulations, if a CITRA decision is challenged before the judiciary, the relevant competent department at CITRA must prepare a technical report on the

dispute or grievance to be submitted to the chair of the board of directors for approval before the conclusion of the report.

It is worth noting here that Article 55 of the CITRA Law makes the decisions of the Committee binding on the parties involved in the dispute/grievance. In addition, grievances against decisions may be referred to the judiciary, but not before resorting to the Committee first - with the objectionable issues submitted before the judiciary attached to the technical report concluded by CITRA.

E-Transactions Law

Articles 40–42 of the E-Transactions Law confer exclusive investigative and prosecutorial authority to the Kuwaiti Public Prosecution for all crimes outlined in the E-Transactions Law and related offences.

Designated personnel appointed by CAIT are granted judicial officer status to oversee the enforcement of the E-Transactions Law, the Regulations and associated decisions. They are empowered to compile reports in case of violations and forward them to the Public Prosecution for further action. The Public Prosecution may consider a reconciliation request from a first-time offender of the specified crimes, provided the accused submits the request and pays KWD1,000 to the court treasury before the case is formally referred for prosecution.

Cybercrime Law

Under Article 17 of the Cybercrime Law, the Kuwaiti Public Prosecution has the exclusive authority to investigate, take action and prosecute all crimes outlined in the Cybercrime Law.

Article 12 allows the court to exempt offenders from punishment if they voluntarily report the crime to competent authorities before its execution, with a conditional exemption for a crime that is reported after discovery but before the investigation only if the reporting aids in apprehending other culprits in a case with multiple offenders.

1.4 Multilateral and Subnational Issues

GDPR and Impact on Kuwait Companies

By virtue of the CITRA Law, CITRA shall also guarantee compliance with any international, regional and bilateral agreements to which Kuwait is party. This means that companies operating in Kuwait that process, store or collect personal data that is EU-based may also be subject to the General Data Protection Regulation (GDPR).

Besides the above-mentioned overlap between the DPPR and the GDPR, the authors are not aware of any efforts towards the implementation of any relevant multilateral obligations.

1.5 Major NGOs and Self-Regulatory Organisations

At the time of writing, data protection NGOs and industry self-regulatory organisations are not present in Kuwait; all regulatory authorities in this respect are governmental.

1.6 System Characteristics

Similarities with the GDPR

It should first be noted that, in most material respects, the E-Transactions Law and the DPPR loosely resemble the EU's GDPR in the following respects.

- Transparency in collecting users' information:
  (a) PaaS and Saas Regulations located under Article 2 of CITRA's Cloud Service Providers Regulations and Commitments

– sub-section 5.6, in particular – relate to the use of third-party services; and
(b) Article 32 of the E-Transactions Law.

- Rectification and erasure of certain information at the request of the subscriber/user:
  (a) Article 4 of the User Rights and Data Protection Law of CITRA; and
  (b) Article 36 of the E-Transactions Law and Article 25-26(1) of the Regulations.
- Disclosure to users of transfers of personal data to third countries or international organisations (data protection classification and the need to disclose to users the transfer of information to new entities as a result of acquisitions or mergers):
  (a) Article 4.2 of the Cloud Computing Regulatory Framework ("Framework"); and
  (b) Article 32 of the E-Transactions Law.
- Rights to lodge complaints with the supervisory board: Chapter 6 of the CITRA Regulations.
- Penalties for violation(s) of the CITRA Law:
  (a) Chapter 10 of the CITRA Law; and
  (b) Chapter 8 of the E-Transactions Law.

1.7 Key Developments

Users' Rights and Data Protection Under the Data Protection Regime

The issuance of the DPPR, which applies to Licensees in Kuwait, has been a much-needed milestone in the area of data protection in relation to Licensees. The provisions adopted under the CITRA Law use the guidance of internationally approved standards in regulating the relationship between the Licensee and the user, which was otherwise non-existent in Kuwait.

Such needed provisions include the regulation and conditions of spam messaging and marketing methods adopted by Licensees, dealings in and the protection of personal data (particularly from third parties), the use of cookies, unfair contract terms and complaint procedures - to name a few.

Framework

The issuance of the Framework was also an important achievement in the field of Kuwaiti data protection. This Framework brought about definitions for types of cloud computing service providers (CSPs), data classification, cybersecurity and the main jurisdiction location(s) of data storage, among other things.

CITRA Regulations to Protect the Rights of Technology Users

In late April 2022, CITRA issued guidelines regarding the protection of users' rights and regulation of communications and IT services. Pursuant to these guidelines, users must give explicit oral, electronic or written consent to receiving messages or communications when subscribing. The Licensee must keep a record of the subscriber's consent to promotional messages, and must keep a database to regulate unwanted messages by the subscriber(s) upon request(s) of such.

Emergence of National Cybersecurity Centre

Decision No 37 of 2022 on the establishment of The National Cybersecurity Centre involves the creation and organisation of a resilient national cybersecurity system to shield the State of Kuwait from cyberthreats. The Centre is dedicated to effectively addressing these threats, ensuring operational sustainability and upholding national cybersecurity. Its scope encompasses safeguarding vital interests in the digital realm, overseeing the development of specialised national capabilities in cybersecurity, nurturing a cybersecurity culture to promote secure electronic space use, and monitoring and protecting critical assets, infrastructure, national information and the state's information network.

Furthermore, the Centre facilitates collaboration, co-ordination and the exchange of information among diverse local and international entities within the cybersecurity sphere.

1.8 Significant Pending Changes, Hot Topics and Issues

Kuwait's Digital Transformation

CAIT recently launched the Kuwait Information Network Project. Distributed across multiple centres in Kuwait, the network devices connect 95 government agencies through high-speed fibre-optic cables and prioritise security with firewalls, encryption devices and continuous monitoring services. Security and confidentiality devices equipped with programs to combat cyberthreats are strategically placed to protect information transfer points.

Noteworthy achievements include connecting more than 90 government agencies, implementing hosting environments for business continuity, and linking the network with other countries in the Gulf Cooperation Council (eg, Bahrain, Oman, Qatar, Saudi Arabia and the United Arab Emirates).

The network also facilitates electronic messaging, system activation and continuous development in line with international standards. Preparations are underway to integrate the latest global technologies for data and information transfer.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

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 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 infor-

mation 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 case of any such amendment, the following must occur before any enforcement can take place:

- the service user must be notified of the amendment(s) 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; and
- 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).

Policy

Pursuant to the Policy, guidance is provided to public and private sector entities to classify their data in accordance with its sensitivity, including any personal data of any individuals in their possession.

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 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 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 and Regulations and Commitments

Types of information collected by 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 located 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 (and 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 names, 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, then the consent of their guardian must be obtained. The service must abide by any relevant child protection laws of the state.

Framework

Dealing with data

Under Article 4, Tier 3 and Tier 4 data may not be stored outside the state of Kuwait, and CSPs may not use a shared or hybrid cloud to store this type of information, unless such is licensed by the Authority. CSPs must also notify users of a security breach within no more than 72 hours and, accordingly, must have established safeguard mechanisms in place with regard to disaster recovery and risk management. Under the same provision, the CSP must give its users the technical means through which to access the given information and the process by which to amend such.

Under Article 6, the service contract must clearly stipulate the protocol of action and notification in the event that a security breach occurs.

Cancellation of service

Under Article 6, the CSP must include certain clauses in its service contracts that relate to the cancellation of the user's service. The user must be provided with a copy of their cloud computing content saved at the time of termination; otherwise, upon the request of the user, their content may be transferred to their other chosen CSP. Upon such handover of the transferral of

content, the CSP must delete any and all content or information related to the user present on its own platform(s).

Unfair contract terms

Under Article 7, CSPs may not exclude any liability (extending to actions by individual employees) in their service contract in relation to the damage or loss of, or tampering with, the user's information and content – unless it is stipulated that this may happen unintentionally or in the event of a security breach.

Disclosure of data

Under Article 4.3.4, the CSP may only disclose the user's content or data by:

- responding to an official request by security or intelligence authorities; or
- obtaining consent of the user, provided that:
  (a) the data is not classified as Tier 3 or 4; and
  (b) the user may withdraw their consent to such disclosure in the future.

The CITRA Law and the CITRA Regulations

Regulations

Under Article 51, telephone calls and private communications are classed as confidential matters that may not be violated. The only exception to this is by an approval solely granted by a competent judicial authority in the state of Kuwait.

The CITRA Law

Under Article 46, the trade, sale or display for sale of bugging devices is strictly prohibited. The only exception to this is that governmental authorities (as defined by a decree) are permitted to own bugging devices for the purpose of maintaining national security and peace. Even in such circumstances, the delegated authorities may only use these devices if consent has been granted by the public prosecutor's office in accordance with the terms, conditions and procedures set forth in the Kuwaiti Procedures Law.

2.2 Sectoral and Special Issues

Policy

The governing regulation is CITRA's Policy, which classifies different types of data according to the sensitivity of its content.

Classification of data and specifics

The First Tier

"Public Data" refers to unclassified data that is available to the public or to data that is not subject to protection from public access under any law, regulation or contract. Examples include:

- open data such as policies, regulations and laws published on websites, daily newspapers, magazines or other publications;
- self-service forms made available to individuals and authorities; and
- any data and information made publicly available on websites.

The Second Tier

"Private Insensitive Data" refers to data owned by the public and private sectors, or at a personal level. It is data that indicates the identity of the data owner, although unauthorised disclosure does not lead to any damage to the privacy of the person's data. Examples include:

- first or last name;
- job title, job duties and employer name;
- email address;
- civil ID number;
- gender;
- age; and
- academic qualification.

The Third Tier

"Private Sensitive Data" refers to data owned by the public and private sectors, or at a personal level. It is data indicating the identity of the data owner and may encompass a mix of sensitive and insensitive data. The unauthorised disclosure of such data may damage the privacy of the person's data. Examples include:

- the minutes of meetings and business plans;
- internal project reports;
- legal notes and opinions issued by legal offices;
- medical records; and
- criminal fingerprints and DNA fingerprints.

The Fourth Tier

"Highly Sensitive Data" refers to private data of a very sensitive nature, the unauthorised disclosure of which may result in great damage to the privacy of the person/entity's data. Such data may be owned by government or private sector entities but relate to highly personal information. This data must have high encryption requirements and requires the highest levels of protection means. Examples include:

- encryption keys;
- political documents, international negotiations or international relations; and
- sensitive information of a military nature or in relation to state security.

Data storing methods

As previously mentioned, under Article 3, the owner of the data is encouraged to classify such data into at least four different levels, according to its contents. If a separate classification system is used, it must be unified to match the data classification tier outlined earlier. Governmental entities are exempt from this and may choose to classify data in any manner they see fit.

The data owner is free to choose their data protection methods according to their data classification, retention, collection and processing schemes. The data owner must also ensure the availability and adoption of certain safeguards and protections necessary for the storage of such data – specifically, data labelled under Tier 3 and Tier 4.

The owner of the data is also encouraged to create a data catalogue that contains standards of data storage in a unified format. However, the data owner must encrypt all data classified under Tier 3 and Tier 4 when transferring such data from one governmental authority or private entity to another (or across geographical locations). Classified data under the aforementioned tiers must be transferred or removed before the data server is disposed of.

Obligations of CITRA

Lastly, under Article 3, CITRA is obliged to encourage and provide guidance for private and public entities' compliance with the Policy. It is also empowered to request periodic reports from CAIT. Such reports must contain a catalogue of all the types of data in its possession, the approved tier classification system of data and reasons for adopting such, and the locations of the stored data according to the adopted classification tiers.

Regulations and Commitments of Cloud Service Providers

The use of cookies

The 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.

2.3 Online Marketing

User Guidelines

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 07:00 and 22:00 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 advertisement 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 Cloud Service Providers

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

2.4 Workplace Privacy

Please see **2.1 Omnibus Laws and General Requirements** (E-Transactions Law: Consent).

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 the event of a situation occurring between third parties and company employees.

There are no applicable laws in place for monitoring employees' emails in Kuwait. Private life cannot be violate, 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.

2.5 Enforcement and Litigation

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 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 CITRA Law

Violations of CITRA Law and Regulations

Under Article 61 of the CITRA Law, if a CITRA inspection determines that a violation – or suspected violation – of its laws has been committed, then CITRA must instruct the public prosecutor's office to adopt the appropriate measures. However, under Article 63, the board of CITRA may accept reconciliation of the violations of its laws or regulations and accept a cash penalty of no less than twice the amount of the fine(s) stipulated in the CITRA Law before a referral to the public prosecutor's office. Such violations include:

- using bugging devices (punishable by either imprisonment for no more than one year or a fine of no more than KWD5,000 and no less than KWD500); and
- illegally using a private or public telecommunications network (punishable by either two years in prison or a fine of no more than KWD20,000 and no less than KWD500).

Claim for compensation (Article 81)

It should be noted that the above-described penalties do not prejudice any person to claim for direct compensation as a result of such actions. Due to the CITRA Law and CITRA Regulations being so new, the procedure has yet to be tested in the courts.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Under Article 70 of the E-Transactions Law, using telecommunications to send threats, immoral or humiliating messages, or made-up events for the purpose of causing panic is punishable either by imprisonment of no more than two years or by a fine of no more than KWD5,000. In addition, intentionally defaming anyone by engaging in non-consensual capturing or usage of pictures or videos (or the falsifying of such) is punishable either by a prison term of no more than two years or by a fine of no more than KWD5,000

and no less than KWD500. Furthermore, sending immoral or indecent materials by any means (eg, messages, videos or pictures) will be punished by either a prison term of no more than three years or a fine of no more than KWD5,000 and no less than KWD500.

If any such acts are accompanied by blackmail in relation to the above-mentioned materials, it is punishable by either up to ten years in prison or a fine not exceeding KWD10,000.

3.2 Laws and Standards for Access to Data for National Security Purposes

Please see **3.1 Laws and Standards for Access to Data for Serious Crimes**.

Usually, governmental agencies – in particular, law enforcement agencies – do not require any judicial approvals to access individuals' data for intelligence, anti-terrorism or other national security purposes. Moreover, most of the data is retained in centralised systems to which the agencies already have access. There are no specific requirements to obtain any judicial approvals for governmental agencies to request data from other governmental agencies. There are no specific laws that govern this particular scenario.

Please note that, depending on the sensitivity of the information (ie, Tier 3 and Tier 4), certain approvals may be required.

3.3 Invoking Foreign Government Obligations

The laws in Kuwait do not consider a foreign government access request to be a legitimate basis for transferring personal data. The situations in which personal data may be transferred outside Kuwait are discussed in **4. International Considerations**. It is generally not permissible for an organisation to invoke a foreign government access request as a legitimate basis upon which to collect and transfer personal data – unless there is a legal basis under the local laws for such transfer.

Kuwait has not participated in any Cloud Act agreements with the USA to date.

3.4 Key Privacy Issues, Conflicts and Public Debates

Like many other countries, Kuwait faces several conflicts and public debates concerning government access to personal data. The key issues in relation to privacy include the following.

Civil ID Cards

The Kuwaiti government has mandated the use of a national ID card for all citizens and residents. However, there have been concerns about the amount of personal information collected on the card and the potential for misuse of this information.

Health Data Collection

The collection of health data is generally governed by Kuwait Law No 70 of 2020 On the Practice of the Medical and Paramedical Professions, the Rights of Patients and Health Facilities ("Health Data Law"), which applies to the Kuwait Ministry of Health and its personnel, and to any individual possessing a university degree granted by a medical or dental faculty accredited and endorsed by the relevant authorities in the State of Kuwait.

Under Article 60 of the Health Data Law, every Healthcare Facility (defined in Article 1 as every place specifically designated to offer medical or healthcare services to individuals for purposes such as disease diagnosis, treatment, prevention, health enhancement, rehabilitation or convalescence) must establish a register and data-

base to record all patient information in either written or electronic form. The management of the Healthcare Facility is responsible for maintaining and safeguarding these files to prevent damage or loss. If the Healthcare Facility ceases operations or undergoes a change in activity, it is obliged to deliver the patient files or copies upon request to the patient or their family. In addition, under Article 13(5), written consent is required from a patient before disclosing their secrets and health information, and patients have a right to request a detailed summary or report of their health files (Article 28 of the Health Data Law).

The Kuwaiti government has also been collecting health data from citizens and residents, particularly during the COVID-19 pandemic. Although this data can be useful for public health purposes, there are concerns about the privacy implications of such data collection.

Conflict With Human Rights

The collection and use of personal data by the government in Kuwait has been seen as potentially being in conflict with human rights, including the right to privacy and freedom of expression. The right to privacy is recognised as a fundamental human right under international law and, as such, is protected by numerous human rights treaties and conventions. The UN Human Rights Committee, for example, has stated that "the collection and retention of personal data must be regulated by law" and that "the law must be adequate to provide effective safeguards against arbitrary interference with an individual's privacy".

In addition to privacy concerns, the collection and use of personal data by the government can also have an alarming effect on freedom of expression. If individuals believe that their online activity or communications are being monitored by the government, they may be less likely to express themselves freely or engage in political or social activism.

4. International Considerations

4.1 Restrictions on International Data Issues

There are restrictions on international data transfers of personal information, especially those classified as Tier 3 and Tier 4 under the Policy.

The DPPR states that a Licensee must collect and process data during and after providing a service, according to certain conditions. If the Licensee intends to transfer a subject's personal data outside Kuwait, it must notify the data subject.

Furthermore, the Policy imposes restrictions on the transfer of personal information classified as Tier 3 and Tier 4. Such data must be encrypted during transmission from one government entity to another or when transmitted between different physical geographical locations of government entities – and this applies to the private sector as well. Therefore, encrypted data may not be transferred internationally.

Subscribers from the private sector and the public sector are explicitly prohibited from storing or hosting Tier 3 and 4 data as classified under the Policy, whether on a temporary or permanent basis, on data centres and cloud computing infrastructure provided by CSPs located outside Kuwait. However, the use of hybrid clouds is allowed for third-level data within Kuwait.

In addition, subscribers engaging CSPs for Tiers 3 and 4 data are prohibited from transferring, storing or processing data unless the CSP is

appropriately registered and licensed by CITRA. Compliance with this requirement mandates that the CSP itself is physically located within Kuwait.

As for less sensitive data, the CSP must obtain written consent from the subscriber before transferring or copying its stored Tiers 1 and 2 data outside the State of Kuwait. CSPs must also ensure that they explain the reasons for the transfer and disclose the party to which the data will be transferred.

In addition, there may be restrictions imposed by the government on the transfer of data for national security and/or public interest concerns.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

Kuwait does not have any specific mechanisms or derogations for international data transfers in place that resemble those provided by APEC or other multilateral frameworks. However, under the DPPR, Licensees are required to obtain the data subject's consent before disclosing their personal data to any affiliate company or third party for any marketing purposes not directly related to the provision of telecommunications and IT services requested by the person concerned. In addition, appropriate security measures must be implemented to protect the personal data of any person against loss, damage, disclosure or hacking by an unauthorised third party.

In practice, many companies in Kuwait use standard contractual clauses or binding corporate rules to ensure compliance with data protection requirements when transferring personal data outside of the country. Companies may also rely on the individual's consent to the transfer, provided that the consent is informed, specific and given freely. However, it is important to note that data protection laws under the DPPR and the E-Transactions Law may impose certain limitations on the use of consent as a basis for data transfers and, of course, such consent must be given freely and obtained in a manner that is specific and informed.

4.3 Government Notifications and Approvals

At the time of writing, there are no express government notifications or approvals required to transfer data internationally. However, please see **4.1 Restrictions on International Data Issues** for further detail.

4.4 Data Localisation Requirements

As mentioned in **4.1 Restrictions on International Data Issues**, there are data localisation requirements for certain types of data. The following types of data must not be hosted or stored outside Kuwait:

- data classified under the Tier 3 and Tier 4 levels of data classification; and
- government entity data falling within the Tier 4 level of data classification.

In order to comply with these requirements, Section 4.2 of the Framework outlines several obligations for subscribers and providers of CSPs in Kuwait. Subscribers must ensure that certain types of data are not hosted or stored outside Kuwait, and providers must disclose the location and technical information of their data centres in Kuwait (and in other countries where they process or transmit the data of subscribers in Kuwait).

Licensees must obtain written consent from their subscribers before transferring or copying data outside of Kuwait. However, this requirement only applies to data that does not fall within the

Tier 3 and Tier 4 levels of data classification. Therefore, only data classified as Tier 1 or Tier 2 can be transferred or stored outside of Kuwait with the notification of the data owner.

4.5 Sharing Technical Details

Currently, there are no legal requirements to share any software code, algorithms or similar technical details with the government.

4.6 Limitations and Considerations

There are express limitations or considerations with regard to foreign government data requests or foreign litigation proceedings or internal investigations; please see **4.1 Restrictions on International Data Issues** and **4.2 Mechanisms or Derogations that Apply to International Data Transfers** regarding the limitations or considerations concerning the international transfer of personal data.

4.7 "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 case of an error in classifying the content as prohibited.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Artificial Intelligence

In Kuwait, domestic entities in regulated industries are beginning to use AI, while multinational targeted advertising companies have been using it for some time. However, there are two primary legal risks and compliance issues for entities in Kuwait looking to incorporate AI into their businesses. The first issue is that using AI for business purposes requires the use of large amounts of data, which often needs to be outsourced to foreign entities, leading to potential data breaches and cybersecurity risks. The second issue is that Kuwait does not have a comprehensive data protection law and is therefore exposed to cybersecurity risks.

Another issue is the limitation on data transfers, as described in **4.1 Restrictions on International Data Issues**, **4.3 Government Notifications and Approvals** and **4.4 Data Localisation Require-**

ments, whereby certain tiers of data cannot be transferred internationally.

Unmanned Aircraft Systems

The Directorate General of Civil Aviation (DGCA) is the regulatory body in the State of Kuwait governing the registration of unmanned aircraft systems (UAS)/drones in Kuwait. The DGCA registers the following three types of uses of UAS/drones:

- recreational (toy, sport, advanced sport activity);
- professional (commercial and non-commercial); and
- special.

Prior permission must be obtained from the DGCA to operate drones for commercial purposes. The following activities are strictly prohibited:

- using drones to carry dangerous goods;
- dropping any object from the drone; and
- using the drone to capture images or videos of private property without obtaining prior consent.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Although there are no specific laws or regulations in Kuwait that require organisations to establish protocols for digital governance or fair data practice review boards or committees, some companies in Kuwait have voluntarily established such protocols as part of their corporate governance practices.

With the increasing importance of data privacy and security, companies in Kuwait have begun to recognise the importance of having a framework in place for managing digital technologies and data practices. Some companies have established internal committees or review boards in order to oversee data privacy and security, and to ensure compliance with local laws and regulations. These committees are often responsible for reviewing the company's policies and procedures related to data collection, storage, processing and sharing, and for assessing the risks associated with emerging or disruptive digital technologies.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

There are no publicly available details concerning any regulatory enforcement. Furthermore, as the Data Protection Regime is so new, it has yet to be tested in the courts. Please see **2.5 Enforcement and Litigation** and **3.1 Laws and Standards for Access to Data for Serious Crimes**.

It is worth noting that there is a growing focus on privacy and data protection in several countries in the Middle East. It is possible that Kuwait may follow suit in the future and introduce more robust legislation in this area.

5.4 Due Diligence

In Kuwait, conducting due diligence is an essential part of corporate transactions, as it helps to identify and assess risks and potential liabilities associated with a company.

The process involves a comprehensive review of the target company's financial, legal and operational records, as well as its contracts, IP and relationships with customers, suppliers and other stakeholders. The parties in a transaction typically execute a Letter of Intent that would include a confidentiality provision and other restrictive covenants. Thereafter, a virtual

data room is established where the target would upload the documents requested by the buyers.

The following issues are typically relevant when conducting due diligence in corporate transactions in Kuwait:

- legal and regulatory compliance;
- corporate governance;
- financial statements;
- material contracts;
- IP;
- management and employment; and
- litigation.

5.5 Public Disclosure

There is no requirement to make a public disclosure regarding an organisation's cybersecurity risk profile or experience.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

There have been no developments or trends regarding the convergence of privacy, competition and consumer protection in connection with the regulation of tech companies, digital technology or data practices in Kuwait. Although there is a growing awareness of the importance of these issues in Kuwait and throughout the Middle East, Kuwait has yet to implement any laws or policies specifically addressing these issues and is not considering (or subject to) any new laws or policies along the lines of the EU's Digital Markets Act, Digital Services Act or Data Act.

5.7 Other Significant Issues

Significant issues faced by Kuwait in relation to data protection include the following:

- lack of comprehensive data protection laws – the existing laws and regulations that touch on the collection, processing and sharing of personal data (by both public and private entities) are scattered across different pieces of legislation, making it challenging to enforce data protection standards in Kuwait;
- inadequate data security measures – many organisations in Kuwait do not have adequate data security measures in place to protect personal data from unauthorised access, theft or other forms of data breaches, thereby leaving personal data vulnerable to misuse and abuse; and
- lack of oversight and enforcement – there is a lack of effective oversight and enforcement mechanisms for data protection in Kuwait, which can make it difficult to hold organisations accountable for data breaches and other violations of data protection standards.

Trends and Developments

Contributed by:
Alex Saleh, Feras Gadamsi, Asad Ahmad and Jehan Saleh
GLA & Company

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It 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 doing business in the Middle East. GLA is 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 Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area 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' experience in both the GCC and the USA, he has accumulated extensive 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.

Feras Gadamsi is a partner in GLA's Dubai office and leads the global technology, data and privacy practice. He was previously Uber's lawyer in the MEA region, and served as Regional General Counsel at IBM, as Oracle Cerner's Regional General Counsel from 2010–2014, and as CLO and Head of Policy for a Dubai-based start-up. He has advised several technology and payments companies throughout the EMEA region. Feras started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. He also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations and audits.

Asad Ahmad is a senior associate at GLA & Company and has been involved in a number of transactional and advisory works in various industries, including logistics, construction, finance, healthcare and education. His practice has involved comprehensive representation with regard to M&A, conducting extensive due diligence exercises in relation to complex transactions, as well as distribution and agency arrangements. Asad has an extensive background in advising on the marketing of securities, corporate governance issues, policies and regulatory compliance, and he has expanded his expertise to include advising on data protection and regulation.

Jehan Saleh is an Associate at GLA & Company, specialising in corporate transactions and commercial advisory. With a law degree from Wayne State Law School, she clerked at the Wayne County Circuit Court in Michigan and previously practised civil litigation at a mid-sized US law firm. Jehan also gained Gulf experience in a legal role at a major rideshare company in Dubai. She is admitted to the Michigan State Bar and is currently pursuing admissions to the New York and Ohio State Bars, expanding her legal expertise. Jehan's diverse background in civil litigation and corporate law, combined with her Gulf experience, enables her to provide valuable counsel in corporate transactions and commercial advisory work.

GLA & Company

Arraya Tower II
36th and 37th Floors
Al Shuhada Street
Sharq
Kuwait
Tel: +965 2291 5800
Web: www.glaco.com

Data Protection and Privacy in Kuwait: An Introduction

This article will explore some of the biggest trends and developments in Kuwait, from a partnership with one of the world's largest publicly traded companies designed to jump start digital transformation across the country to the expanded adoption and deployment of artificial intelligence. It will also examine some of the laws and regulations that have recently been introduced to help support the country's wider goals under Kuwait Vision 2035.

Partnership between Google Cloud and the Kuwaiti government

Kuwait is undergoing a digital transformation. At the forefront of this transformation is the strategic alliance between Google Cloud and the Kuwaiti government. The Google collaboration aligns well with Kuwait Vision 2035 ("Vision 2035"), a national development plan that envisions a dynamic, diversified and technologically advanced Kuwait that is nimble enough to adapt as technology is deployed in the country and even newer technologies are introduced over time. At its core, Vision 2035 seeks to reduce dependency on oil revenues by fostering economic diversification through the promotion of non-oil sectors.

The partnership between Google Cloud and the Kuwaiti government is designed to support the digitisation of government services, the migration of national data securely to the cloud, and the setting up of a national digital skills programme. The decision to enter a public-private partnership with Google stems from the Kuwaiti government's commitment to enhancing government efficiency through rapid digital transformation to stimulate economic growth across all sectors.

Initiated in January 2023, the collaboration marks a pivotal moment in Kuwait's journey towards a digital era, not only shaping its regulatory and governmental landscapes, but also changing the economic landscape. It also lays the foundation for tackling and managing the data trends anticipated to affect Kuwait's economy in the coming years.

Vision 2035 is also grounded in the values of fostering economic diversity, encouraging innovation and embracing digital progress. These values all align with the nation's evolving trends and advancements in data protection and privacy regulations. As Kuwait embraces this digitised era, the alliance with Google Cloud becomes instrumental in steering the nation towards a future that makes Vision 2035 a reality.

Growing the non-oil sectors is essential to Vision 2035, so it should come as no surprise that technology is being used as a catalyst to power growth across all sectors. To do that, the proper infrastructure must be in place to support the deployment of cutting-edge technology. Being able to handle "big data" as datasets continue to grow, while simultaneously maintaining the high levels of data security and privacy demanded by governments and individuals alike, is essential to empowering the type of economic growth Kuwait wants to see as part of Vision 2035.

Consequently, the establishment of data infrastructure capable of powering the type of growth projected in Kuwait becomes essential to fulfilling Vision 2035, and Kuwait's embrace of the potential of data-driven economies becomes a key part of realising Vision 2035. Kuwait's enactment of data privacy laws is also in line with Vision 2035, reflecting a commitment to fostering a technologically advanced society.

These laws, modelled after their European and US counterparts, are intended to safeguard individuals' privacy, and to create standards for the utilisation of data. These regulations support the vision's broader goal of economic diversification and a digital ecosystem that supports projected growth under Vision 2035.

The strategic alliance between the Kuwaiti government and Google Cloud marks a significant milestone in Kuwait's journey toward digital transformation. The Kuwait government has allocated approximately KWD306 million for a seven-year implementation. This collaboration aims to leverage technologies in data analysis, cybersecurity and AI, positioning Kuwait to keep up with the pace of technology globally and the expected economic growth under Vision 2035.

This partnership extends beyond technological advancements to encompass broader societal benefits. The collaboration focuses on healthcare, education, disaster management and smart cities – all areas that are in line with Vision 2035. This agreement seeks to create new job opportunities for Kuwaiti youth by establishing a training programme targeting more than 5,000 citizens, students and workers. The partnership is a joint effort involving the Direct Investment Promotion Authority, the Central Agency for Information Technology and the Communications and Information Technology Authority.

The DPPR and effect of Google Cloud partnership

In 2021, Kuwait introduced Decision 42 of 2021 (the "Data Privacy and Protection Regulation" or DPPR), modelled after international data protection regulations like the EU's General Data Protection Regulation (GDPR).

The DPPR serves as a more comprehensive framework than the preceding regulations. It is not a replacement but rather an addition to the Kuwait E-Transactions Law and the Data Classification policy. When it was first enacted, the DPPR originally addressed activities related, inter alia, to the storage, collection and processing of personal data, including sensitive personal data, performed in or out of Kuwait.

The DPPR has since evolved, and currently applies only to service providers engaged in the telecommunication sector and licensed by the Communication and Information Technology Regulatory Authority (CITRA).

The shift in the DPPR's scope can be attributed to the collaboration between Google Cloud and the Kuwaiti government. The government changed the scope of the law because the law as originally drafted applied to all data collectors in Kuwait. However, with the introduction of the Google Cloud partnership, sensitive data that is required by law to be stored on the ground in Kuwait would, in fact, be stored on the Google Cloud in the interim period, thus violating the law.

To address this challenge, the Kuwaiti government strategically carved out the DPPR to exclusively govern telecom providers initially. This temporary measure allows the government to ensure compliance within the telecom sector while creating a path to revert the regulations to their original form to encompass all data collectors.

Effects of the Kuwait government and Google partnership

The partnership encompasses an array of initiatives designed to digitise citizen services and elevate the efficiency of the government. Digitis-

ing citizen services ensures wider accessibility to the residents and citizens of Kuwait. Moreover, this digital transition is poised to streamline bureaucratic processes within the Kuwaiti government. By eliminating these hurdles, citizens and residents can expect a more efficient and cohesive service experience.

Impact on businesses

The digitisation of services extends beyond the enhancement of resident experiences: it will also lead to a transformative shift for both local and foreign companies engaging in business activities in Kuwait. This new digital landscape will eventually streamline processes such as filing applications with the Competition Protection Authority or managing the closure of companies with multiple regulatory bodies.

Currently, not all of Kuwait's ministries have fully functioning online portals through which to submit applications or ask questions; many applications and processes can only be completed or submitted using paper applications or even in-person visits to the different ministries in Kuwait. These changes would significantly impact the operations of foreign and local companies, and are expected to connect the systems of different regulatory bodies, which could lead to a full digitisation of processes, including acts that require interaction with different regulators.

Cybersecurity regulations

Another notable trend in Kuwait is the government's heightened emphasis on data security and privacy regulations. Recognising the importance of safeguarding information, Kuwait is taking strides, with the help of its alliance with Google Cloud, to maintain all sensitive data in local data centres and to draft relevant regulations to protect sensitive data.

This initiative aligns with a broader global movement of refining data protection standards and maintaining standard cybersecurity practices. This renewed focus on data security is evidenced by Kuwait's new cybersecurity regulations, which include Decision No 7 of 2023 ("General National Framework Regulation for the Classification of Electronic Data") and Decision No 35 of 2023 ("National Framework for Cybersecurity Governance"), which reiterate Kuwait's intention to establish a robust and comprehensive cybersecurity legal framework.

The establishment of data centres and the efficient management of data also reinforce Kuwait's cybersecurity framework. This data-centric approach is in line with Vision 2035's overarching goal of ensuring national security and stability by safeguarding critical data assets.

Artificial intelligence in Kuwait

Kuwait's digital revolution is also marked by significant strides in the deployment and adoption of artificial intelligence (AI) and other "big data" technologies. The intersection of these innovations is reshaping many of the nation's sectors, including healthcare, education, finance and government services.

Abundant data availability and a tech-savvy youth population drive AI and "big data" technology expansion in Kuwait. The government's focus on education and research plays a pivotal role in cultivating a skilled workforce for AI and data science. Initiatives from leading universities and research institutions are addressing the skills gap and fostering expertise in these domains.

While Kuwait envisions a promising future, challenges in its AI and big data journey include the need for a robust data infrastructure, concerns

about data privacy and security, a shortage of skilled professionals, and regulatory and ethical considerations. Collaborative efforts among the government, industry and academia are crucial to overcoming these challenges. As Kuwait actively embraces AI applications in various sectors, from healthcare to finance, the demand for skilled professionals is only expected to rise.

Kuwait's alliance with Google Cloud acknowledges the importance of secure, robust and adaptable data centres in relation to the processing of even more data as technology is deployed to power economic growth, and it becomes even more important when the wider use and adoption of AI are factored in.

In alignment with Vision 2035, the expanded use, deployment and adoption of AI, together with the establishment of data centres in Kuwait, are transforming Kuwait's data landscape. Economically, the integration of advanced technologies is a major step in realising the government's goal of economic growth and a digitally driven society. An important aspect of Vision 2035 is the emphasis on economic diversification. The integration of AI technologies and the digitisation across all key sectors, especially non-oil and gas sectors, is aimed at driving innovation and efficiency, which will help Kuwait transition from its reliance on oil revenues to a more diversified economy.

In the realm of education, the digitisation of learning materials and the application of AI-driven education tools represent emerging data trends. This evolution also supports Vision 2035's goal of human capital development by leveraging data to enhance the quality of education and nurture a workforce equipped with digital skills.

Within Kuwait's healthcare sphere, a significant trend is the growing utilisation of data analytics coupled with AI. Kuwait's healthcare industry has already begun deploying AI on a limited basis, and it is expected that wider adoption of more AI-driven tools will help shape the present and future of medicine in Kuwait. The digitisation of health records and the application of AI in diagnostics contribute to more data-driven healthcare practices. The deployment of AI-driven technology in the healthcare sector will help build a healthier society through advanced and responsive healthcare services, which also aligns with the wider objectives of Vision 2035.

Conclusion

The collaborative efforts between Google Cloud and the Kuwaiti government have laid the groundwork for transformative data trends and developments in Kuwait. This partnership signifies a pivotal moment in Kuwait's journey towards a digital era, reshaping regulatory landscapes, governmental processes and the overall economy.

Kuwait's heightened emphasis on data security and privacy, reinforced by new cybersecurity regulations introduced in 2023, reflects a commitment to establishing a comprehensive legal framework. The establishment of data centres and the efficient management of data underscore Kuwait's dedication to ensuring national security and stability by safeguarding critical data assets.

The impact of digitisation extends beyond regulatory and governmental spheres. Digitising citizen services enhances accessibility and streamlines bureaucratic processes, contributing to a more efficient and cohesive service experience for residents. For businesses, the shift towards the digitisation of processes is poised to stream-

line operations, connecting the systems of different regulatory bodies and impacting the way applications are filed.

In alignment with Vision 2035, the integration of AI and data centres stands as an important step towards realising the vision's goal of a digitally driven society. This extends into education, where the digitisation of learning materials and the application of AI-driven tools align with the vision's emphasis on human capital development. The healthcare sector is experiencing a significant trend with the growing utilisation of data analytics and AI, presenting a paradigm shift towards more data-driven healthcare practices.

As Kuwait continues forward into this new digitisation era, the alliance with Google Cloud contributes to the nation's digital transformation, supporting Vision 2035's aspirations for a diversified and advanced future.