GUIDANCE NOTE

Kuwait - Data Protection Overview

Asad Ahmad
GLA & CO.

Liana Rashid
GLA & CO

Jehan Saleh
GLA & CO

November 15, 2024

November 2024

1. Governing Texts

1.1. Key acts, regulations, directives, bills

Enacted key legislation in the field of data protection:

- Kuwait Administrative Decision No. 26 of 2024 Concerning the Issuance of the Data Privacy Protection Regulation (only available in Arabic here) (the Data Privacy Regulation);
- the Civil, Commercial, and Administrative Electronic Transactions No. 20 of 2014 concerning Electronic Transactions (the ET Law);
- Decision No. 48 of the Executive Regulations of Law No. 20 of 2014 concerning electronic transactions (only available in Arabic here) (the Executive Regulations);

- Cybercrime Law No. 63 of 2015 (only available in Arabic here) (the Cybercime Law);
- Cloud Computing Regulatory Framework (v2.4) (the Framework) issued by the Communication and Information Technology Regulatory Authority (CITRA);
- Law No. 37 of 2014 on the Establishment of CITRA (the Law Establishing CITRA) Kuwait Decision No. 45 of on the Issuance of Instructions for Regulating the Electronic Payment of Funds (the E-Payment Regulations);
- The Users Rights Protection and Regulation of the Communications and Information Technology Services issued by CITRA (the User Protection Regulations);
- National Center for Cybersecurity Resolution No. 35 of 2023 regarding the National Framework for Cybersecurity Governance (only available in Arabic here) (the Cybersecurity Governance Law);
- Kuwait Decision No. 7 of 2023 On the General National Framework Regulation for the Classification of Electronic Data (the Data Classification Regulation);
- Law No. 70 of 2020 concerning the Regulation of the Practice of the Medical Profession, the Auxiliary Occupations, the Rights of Patients and Health Facilities (only available in Arabic here) (the Law on the Medical Profession).

1.2. Guidelines

Not applicable.

1.3. Case law

There is currently no case law in Kuwait that addresses data protection.

2. Scope of Application

2.1. Personal scope

The Data Privacy Regulation applies exclusively to individuals and entities serving as providers within the telecommunications sector and holding licenses issued by CITRA (referred to as 'Licensees').

The **ET Law** applies to private companies, government authorities, public institutions, and non-governmental organizations, and their employees.

The **Cybercrime Law** applies to every identifiable natural person.

The **Framework** applies to all cloud service providers licensed by CITRA with data centers in Kuwait. Although the Framework governs the licensing and other obligations of these cloud service providers, it does place obligations on individuals, public, governmental, and private entities in the State of Kuwait who subscribe to cloud services hosting certain types of data.

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

The **E-Payment Regulations** apply to all service providers licensed by the Central Bank of Kuwait (CBK) providing e-payment, e-money business, and e-payment systems works services, as well as limited purpose e-money providers, and local banks licensed in the State of Kuwait. Article 1 of the E-Payment Regulations defines limited purpose e-money providers as companies licensed by the CBK and operating as single issuers to provide a digital substitute for physical currency stored on an electronic payment platform, enabling payment transactions within the State of Kuwait for acquiring goods or services from a restricted network of providers with direct commercial agreements with the issuing entity.

The **User Protection Regulations** apply to all licensees.

The **Cybersecurity Governance Law** applies to all civil, military, and security government entities, as well as the institutions of the public and private sectors in the State of Kuwait whose activities relate to cybersecurity activities, as well as other entities determined by the Kuwait National Centre for Cybersecurity (the National Centre for Cybersecurity).

The **Law on the Medical Profession** applies to the Kuwait Ministry of Health and its personnel, as well as 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.

2.2. Territorial scope

The **Data Privacy Regulation** applies only to licensees that work to collect, process, and store personal and their users' data content in whole or in part, whether the processing takes place within or outside Kuwait. The term 'user' in the Data Privacy

Regulation typically refers to individuals benefitting from telecommunications services, with their data collected and stored by the licensees. We will use 'data subjects' to refer to the licensees' users when discussing data protection issues. The **ET Law** applies to the respective individuals and entities operating in the State of Kuwait mentioned in the section on personal scope above.

The **Cybercrime Law** applies to all natural individuals inside and outside of Kuwait.

The **Framework** applies to all cloud service providers licensed by CITRA with data centers in Kuwait. Although the Framework governs the licensing and other obligations on these cloud service providers, it does place obligations on individuals, public, governmental, and private entities in the State of Kuwait who subscribe to cloud services hosting certain sensitive data.

The **Law Establishing CITRA** applies to all licensees operating in the State of Kuwait.

The E**-Payment Regulations** apply to the respective individuals and entities operating inside and outside the State of Kuwait mentioned in the section on personal scope above.

The **User Protection Regulations** apply to those mentioned in the section on personal scope above.

The **Cybersecurity Governance Law** applies to all civil, military, and security government entities operating in the State of Kuwait.

The **Data Classification Regulation** applies to those mentioned in the section on personal scope above.

The **Law on the Medical Profession** applies to the respective individuals and entities operating in the State of Kuwait mentioned in the section on personal scope above.

2.3. Material scope

The Data Privacy Regulation: Personal data under this Regulation includes information that can identify an individual or an entity such as users of a telecommunications service provider. This encompasses but is not limited to name, identity, financial details, health records, ethnicity, religion, and any information that can pinpoint a person's geographic location, fingerprint, DNA, or internet contact details. To reiterate, we will use 'data subjects' to refer to licensees' users.

The ET Law: Encompasses a wide range of electronic records, documents, and information related to civil, commercial, or administrative transactions conducted in whole or in part through electronic means. Additionally, it should be noted that this Law imposes obligations on the relevant entities to which this Law applies to regarding data protection and processing of professional, personal, health, social status, and financial data of individuals as well as encompassing provisions related to the rights of data subjects.

The Cybercrime Law: Encompasses all types of electronic data, documents, and records. Electronic data includes data with electronic characteristics in the form of texts, symbols, sounds, images, computer programs, or databases.

The Framework: Covers personal identification data, contact data, marketing and communications data, behavioral data, technical data, aggregated data, and special categories of personal data.

The Law Establishing CITRA: See the section on personal scope above.

The E-Payment Regulations: Cover banking data, financial data, statistical data, and personal data.

The User Protection Regulations: See the section on personal scope above.

The Cybersecurity Governance Law:

- Sensitive data**:** Refers to information with restricted access, processing, or sharing permissions. Unauthorized loss, misuse, or disclosure of this data can lead to severe damage or negative impacts on national security, general security, the economy, individuals, properties, privacy, health, intellectual property, or the operations of the entities to which this law applies. Before retaining or processing any sensitive data beyond the borders of the State of Kuwait, the entities covered by this Law must secure approval from the Kuwait National Centre for Cybersecurity;
- Restricted or limited data**:** This information has access limitations for certain individuals or entities and does not have a limited definition but may encompass insensitive personal data; and
- Open or general data**:** Information accessible to everyone without restrictions. Any person or entity can freely access, check, process, or share such data.

Data Classification Regulation: See the section on personal scope above.

The Law on the Medical Profession: Covers all types of health data and the obligations of the applicable individuals and entities to whom this law applies to protect health data during storage and processing.

3. Data Protection Authority | Regulatory Authority

3.1. Main regulator for data protection

Kuwait does not currently have a regulatory authority that assumes all authority over data protection. Initially, CITRA was seen as the primary regulator for data protection given that the Data Privacy Regulation, originally imposed data protection obligations on a wider scope of entities. However, recent amendments have narrowed down its scope to telecommunication companies. Despite this, CITRA retains a crucial role in Kuwait as an authority overseeing various data protection issues, issuing laws, and providing directives, despite its primary focus on the telecommunications sector.

Another important regulator in the State of Kuwait for personal data protection is the Central Agency for Information Technology (CAIT), responsible for the issuance of the ET Law and the Executive Regulations. Additionally, the National Centre for Cybersecurity is a newly established authority that is a key regulator in the field of cybersecurity.

3.2. Main powers, duties and responsibilities

CITRA is responsible for:

- organizing telecommunication network services in Kuwait, ensuring efficient delivery at reasonable prices, and coordinating with the Gulf Cooperation Council (GCC) communication and information technology authorities;
- establishing detailed regulations for technical terms in the telecommunication and information technology sectors, regularly reviewing and updating them;

- developing regulations to organize the telecommunication and information technology sectors in line with the national policy, ensuring services meet the country's comprehensive development needs, and conducting annual reviews;
- establishing regulations for licensing telecommunication or internet networks, radio frequency use, international telecommunication infrastructure, and international access infrastructure, ensuring transparency, fairness, and consistency with existing laws and public morals;
- determining fees for licensees using the frequency spectrum, numbers, internet ranges, and other resources in the telecommunication and information technology sectors; and
- determining and updating prices and fees for telecommunication and information technology services, monitoring fair competition, and enforcing compliance with laws and public order.

CAIT is responsible for:

- developing national-level plans and policies for information technology;
- overseeing the implementation of the Kuwait Government's (the Government) electronic plan and projects in coordination with ministries and governmental entities;
- coordinating all activities related to the development plans of information technology among government entities;
- developing and managing methodologies, standards, and patterns necessary for information technology systems, devices, and services;
- establishing and managing the official electronic portal for the State;
- training technical human resources working in the field and industry of technology in the country and enhancing their capabilities in this field; and
- raising public awareness about information technology and its uses across all segments of society.

The National Center for Cybersecurity is responsible for:

- safeguarding Government data to prevent loss and ensuring its accessibility in the face of disasters;
- upholding the continuity of critical systems in various government agencies;
- serving as an alternative protective site for approximately 53 government entities;

- fostering confidence among users of electronic services;
- advancing government infrastructure to align with cutting-edge technologies;
- providing swift and effective responses to diverse risks and threats; and
- ensuring prompt recovery from risks on occurrence.

4. Key Definitions

Data controller: Not applicable.

Data processor: The closest definition is 'data collection and processing' which is defined as activities involving any set of actions performed on personal data, regardless of whether it occurs within or outside the State of Kuwait. These actions include automated processes or other methods, such as gathering, recording, organizing, analyzing, storing, modifying, retrieving, using, or disclosing the data. This also encompasses activities like transmitting, publishing, making available, merging, restricting, deleting, or destroying the data (as per the Data Privacy Regulation).

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

Sensitive data: The closest definition is 'special categories of personal data' referring to data related to race, religion, sect, philosophical beliefs, political opinions, memberships, or data relate to health and genetic or vital data. (Framework).

Health data: The closest definition is 'health file' which is defined as a record that encompasses the personal information of the patient along with comprehensive details about their health condition and medical background. It includes a record of all medical procedures conducted and the healthcare services provided to the patient (as per Article 1 of the Law on the Medical Profession).

Biometric data: Not applicable.

Pseudonymization: Not applicable.

Data subject: Data subject is not defined *per se*, but is referred to under the Data Privacy Regulation in the definition of personal data.

Customer under the E-Payment Regulations refers to anyone who benefits from the services of the entities governed by the same, including persons they legally contracted with. Please note that customers under the E-Payment Regulations will be referred to as data subjects for this guidance note.

5. Legal Bases

5.1. Consent

The entities governed by the ET Law are expressly required to obtain individuals' consent when accessing, disclosing, sharing, or processing personal data or information, and any such activities must be undertaken by lawful means and limited to the stated purpose (Articles 32 and 35 of the ET Law). Licensees are obligated to obtain the data subject's consent and state the purpose for which such data collection and processing is required before gathering and processing the data subject's personal data and following the termination of the services (Articles 2 and 4 of the Data Privacy Regulation). In addition, under Article 13.5 of the Law on the Medical Profession, written consent must be obtained before disclosing patient secrets and health information.

The Data Privacy Regulation, the User Protection Regulation, and the ET Law emphasize the importance of obtaining the explicit and informed consent of individuals before processing their personal data, especially for sensitive information.

5.2. Contract with the data subject

A contract is required when dealing with licensees and their 'users' or data subjects (Article 3.1 of the User Protection Regulation).

5.3. Legal obligations

Data collection and processing are considered legitimate and legal when necessary to comply with a legal obligation binding on the licensee (Article 3 of the Data Privacy Regulation).

5.4. Interests of the data subject

The processing of data by licensees is only deemed legitimate if it is also necessary to protect data subjects' data and the purposes pursued by the licensee necessitate the identification of the data subject (Article 3(3) and 3(4) of the Data Privacy Regulation).

5.5. Public interest

Not applicable.

5.6. Legitimate interests of the data controller

Not applicable.

5.7. Legal bases in other instances

Not applicable.

6. Principles

The Data Privacy Regulation and the User Protection Regulation elaborate in their preambles on certain measures and principles that are adopted in each to bring Kuwait's data protection framework in line with international standards. The same is echoed in the explanatory memorandum of the ET Law.

These four pieces of legislation cover the following principles and themes:

- **transparency:** Ensuring that individuals are informed about how their data is collected, processed, and used;

- **purpose limitation:** Restricting the processing of personal data to specific, explicit, and legitimate purposes disclosed to the individuals;
- **data minimization:** Collecting and processing only the data that is necessary for the stated purposes, avoiding excessive or irrelevant information;
- **accuracy:** Ensuring that the personal data collected is accurate, up-to-date, and relevant for the intended purposes;
- **storage limitation:** Setting clear guidelines on the duration for which personal data can be retained and specifying criteria for its deletion;
- **confidentiality:** Implementing measures to safeguard the confidentiality of personal data, preventing unauthorized access or disclosure;
- **security:** Mandating the implementation of adequate technical and organizational measures to safeguard personal data against unauthorized access, disclosure, alteration, and destruction; and
- **accountability and governance:** Encouraging organizations to adopt internal policies, conduct risk assessments, and appoint data protection officers (DPOs) to ensure compliance with data protection laws.

7. Controller and Processor Obligations

Licensees must clarify the purpose of processing their data subjects, and this purpose must be necessary to provide their services (Article 2 of the Data Privacy Regulation). Licensees must ensure that the processing of data is conducted in a manner that safeguards personal data against unauthorized or unlawful processing, as well as protects against accidental loss, destruction, or damage. This involves employing suitable technical and regulatory measures (Article 4(4) of the Data Privacy Regulation).

E-Payment Regulations

Robust systems must be developed to protect the confidentiality of data subjects' data, financial data, and other information when processing (Article 29 of the E-Payment Regulations).

7.1. Data processing notification

Not applicable.

7.2. Data transfers

The Data Privacy Regulation, the User Protection Regulation, and the ET Law establish rules and safeguards for the transfer of personal data across international borders to ensure that adequate protections are maintained.

Framework

Private and public entities in Kuwait using cloud service providers should avoid storing or hosting level three or four personal data, as defined within the now repealed CITRA Data Classification Policy, on the data centers and cloud computing environments located outside Kuwait, whether temporarily or permanently (Articles 3.2.1.2.2 and 4.2.1.1 of the Framework). Hybrid cloud usage is permitted within Kuwait for level three data (Article 3.2.1.2.2 of the Framework). Private entities using cloud service providers for level three and four data, including government entities' level four data, must ensure that the cloud service provider is registered and licensed by CITRA with a physical presence in Kuwait. Transferring, storing, or processing data with unregistered providers is prohibited (Article 4.2.1.2 of the Framework).

For awareness, the now repealed CITRA Data Classification Policy defined Tier 3 and Tier 4 data as per the following:

- **Private sensitive data** (**Tier 3 data**)**:** Refers to data held by the public and private sectors and may include, in part, insensitive private data that identifies the individual and leads to damage of individual privacy if the data were subject to unauthorized disclosure. Such data includes:
    - minutes of meetings and business plans;
    - internal project reports;
    - litigation files and court orders and judgments;
    - legal notes and opinions;
    - medical records; and
    - DNA information and criminal fingerprints.

- **Highly sensitive data** (**Tier 4 data**)**:** Refers to data of a very sensitive nature, and unauthorized disclosure may inflict great harm to the privacy of a person. It includes data owned by the Government or private entities or at a national level and thus should only be published specifically for those who require access to it. Such data includes:
  - encryption keys;
  - political documents, international negotiations, or international relations data; and
  - sensitive military or state security information.

7.3. Data processing records

Licensees have an obligation to maintain records of processing activities. These records should include details such as the licensee's name, contact information, and their legal representative if they are inside or outside of Kuwait. Additionally, the licensees must outline the purposes for processing data, provide a description of the categories of data subjects and other personal data categories involved, and specify any transfer of personal data to foreign countries, including the identification of such countries. The records must also feature a general description of the technical and organizational security measures employed in the data processing activities (Article 5(4) of the Data Privacy Regulation).

7.4. Data protection impact assessment

The Data Privacy Regulation, the User Protection Regulation, and the ET Law require organizations to conduct assessments to evaluate and mitigate the risks associated with certain data processing activities.

7.5. Data protection officer appointment

There is no mention of the mechanisms and obligations in relation appointment of data protection officers *per se*. However, the Data Protection Regulation does create obligations on Licensees to maintain information with respect to the Licensees' information and contact details when maintaining processing records of personal data (Article 5 of the Data Protection Regulation). In addition, Licensees have an obligation as well to provide CITRA the contact details of their appointed data protection officer when reporting data breaches (Article 6 of the Data Privacy Regulation).

7.6. Data breach notification

The Data Privacy Regulation, the User Protection Regulation, and the ET Law require organizations to promptly notify individuals and relevant authorities in the event of a data breach that may compromise the security of personal data. Licensees must report any personal data breaches to both CITRA and the affected individuals within a period not exceeding 24 hours from the time of awareness of the breach of any personal data. However, notification to the data subject is not required if the licensee has implemented suitable technical and organizational protection measures and these measures have been effectively applied to the personal data impacted by the breach (Article 6 of the Data Privacy Regulation).

In addition, under the Framework, cloud computing service providers must inform their subscribers, whether they are public or private entities, and CITRA, within a period not exceeding 72 hours, of an information security breach or data leakage as soon as they become aware of the leak (Article 4.2.2.1 of the Framework).

7.7. Data retention

The entities and individuals to whom the ET Law applies have a responsibility to regularly verify and update the accuracy of personal data and are also mandated to implement adequate measures to safeguard collected or stored personal data (Article 35 of the ET Law). Electronic records, including personal information, must be stored in their original form (Article 2(2) of the Executive Regulations). Storage must align with the policies and agreements in electronic transactions, specifying the duration of such storage (Article 2(3) of the Executive Regulations). Entities must define employee access to electronic records based on business needs, ensuring compliance with personal data protection standards (Article 4 of the Executive Regulations).

Under Article 4(13) of the Data Privacy Regulation, the Licensee is obligated to erase the data subject's data under the following circumstances:

- if the data subject withdraws consent for the processing or use of personal data;
- when the personal data is no longer essential for delivering the requested services; and
- if the data subject is no longer subscribed to the service for which the personal data was initially collected.

All healthcare facilities must establish a register and database 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 obligated to deliver the patient files or copies upon request to the patient or their family (Article 60 of the Law on the Medical Profession). A healthcare facility is defined as any place specifically designated to offer medical or healthcare services to individuals for purposes such as disease diagnosis, treatment, prevention, health enhancement, rehabilitation, or convalescence.

7.8. Children's data

The Data Privacy Regulation, the User Protection Regulation, and the ET Law introduce specific safeguards and requirements for the processing of personal data belonging to children, often requiring parental consent. Under the Data Privacy Regulation, licensees must ensure that they have the written consent of a minor's guardian if the minor is under the age of 18 (Article 3(5) of the Data Privacy Regulation).

7.9. Special categories of personal data

Licensees, whether from the public or private sector, must not use sensitive personal data to deduce their subscribers" or the data subjects' identities without obtaining clear, written consent from the data subjects (Paragraph 4.1.4 of the Framework).

The Licensee must implement appropriate security measures to safeguard the data subject's sensitive data from loss, damage, unauthorized disclosure, breaches, or the inclusion of incorrect information. These measures should be tailored to the nature of the activities and the sensitivity of the sensitive data collected. This includes encrypting and processing the data, maintaining the confidentiality, integrity, availability, and resilience of processing systems, ensuring timely restoration of data access in case of force majeure, and regularly testing the effectiveness of security measures (Article 5 of the Data Privacy Regulation).

7.10. Controller and processor contracts

Not applicable.

8. Data Subject Rights

The Data Privacy Regulation, the User Protection Regulation, and the ET Law define and grant individuals certain rights over their personal data, such as the right to access, rectify, erase, or port their data.

8.1. Right to be informed

Licensees have notification obligations, including informing data subjects about personal data transfers outside Kuwait and reporting any personal data breaches to both CITRA and the affected individuals. In addition, licensees are required to establish and uphold a written privacy policy that elaborates extensively on its procedures concerning the collection and processing of personal data. This policy should be publically accessible on its website and provided to users and data subjects when entering into service contracts.

Also, refer to the sections above on consent and data transfers.

8.2. Right to access

Any person whose personal data is stored with any one of the entities that are governed by the ET Law may request access to and a record of the data or information held or stored by those entities (Article 33 of the ET Law.) Please note, however, that personal data or information about individuals that is stored in the records and electronic processing systems of government security agencies for national security reasons are exempt from this requirement.

Licensees must develop appropriate and accessible technologies for data subjects to be able to access their personal data (Article 4(6) of the Data Privacy Regulation).

Patients have a right to request a detailed summary or report of their health files (Article 28 of the Law on the Medical Profession).

Subscribers of cloud service providers have access to their data that is stored with the cloud service provider (Article 6.4.12 of the Framework).

8.3. Right to rectification

Licensees must develop appropriate technologies for data subjects to be able to rectify and amend their personal data (Article 4(6) of the Data Privacy Regulation).

Any person whose personal data is stored with any one of the entities that are governed by the ET Law may modify any personal data or information stored or held by any one of those entities, in addition to replacing personal data or information in case of any changes (Article 36 of the ET Law). Only the person whose personal data or information is stored or held by an entity, or the person's legal representative, may request access to, modify, or delete the personal data or information (Articles 25 and 26(1) of the Executive Regulations.)

8.4. Right to erasure

Licensees must determine the mechanisms for their data subjects to be able to delete their stored personal data (Article 4(8) of the Data Privacy Regulation). Deletion of personal data or information held by the entities governed by the ET Law must be in cases where the data or information requires correction only, and the previously stored or held information should be maintained without using or dealing in them (Article 26(2) of the Executive Regulations).

8.5. Right to object/opt-out

Licensees must determine the mechanisms for their data subjects to be able to cancel their service contracts with the Licensee (Article 3.4(d) of the User Protection Regulations).

8.6. Right to data portability

Not applicable.

8.7. Right not to be subject to automated decision-making

Not applicable.

8.8. Other rights

Licensees must determine the mechanisms for their data subjects to be able to restrict the processing of their stored personal data (Article 4(8) of the Data Privacy Regulation).

9. Penalties

Data Privacy Regulation

The Data Privacy Regulation's penalties are included in Article 71 of the Law Establishing CITRA and apply to any individual engaging in the interception, obstruction, deviation, or deletion of messages and content transmitted through telecommunication networks, or encouraging others to do so. The prescribed punishment includes imprisonment for a maximum of one year and a fine ranging from KWD 300 (approx. $975) to KWD 3000 (approx. $9,750), or one of these penalties.

ET Law

Article 37 of the ET Law penalties apply to:

- anyone who unlawfully accesses, discloses, or publishes any personal data or information registered in the records or electronic processing systems registered with any of the entities governed by the ET Law. They shall be punished by imprisonment for a term not exceeding three years and a fine of no less than KWD 5,000 (approx. $16,250) and not exceeding KWD 20,000 (approx. $65,000), or by either penalty; and
- anyone who gains unlawful access, by any means, to an electronic signature, system, document or record, or hacks, intercepts, or disrupts such system. They shall be punished by imprisonment for a term not exceeding three years and a fine of no less than KWD 5,000 (approx. $16,250) and not exceeding KWD 20,000 (approx. $65,000), or by either penalty.

Law on the Medical Profession

The Law on the Medical Profession applies to:

- anyone who deliberately conceals or destroys the medical file of a patient or part thereof. They shall be punished by imprisonment for a period not exceeding five years and a fine not more than KWD 10,000 (approx. $32,500), or by either of these penalties (Article 69); and

- anyone who discloses or publishes by any means or method a patient's confidential information whether they have learned, discovered, or knew such information in the course of the performance of their work or by reason thereof. They shall be punished by imprisonment for a period not exceeding five years and a fine not more than KWD 10,000 (approx. $32,500), or by either of these penalties (Article 70).

Cybercrime Law

The Cybercrime Law applies to:

- anyone who illegally gains access to a computer or system thereof or a data electronic processing system, an automated electronic system, or an information network. They shall be punished by imprisonment for a period not exceeding six months and a fine no less than KWD 500 (approx. $1,625) and not more than KWD 2000 (approx. $6,500), or either of these penalties. If such act has resulted in the abolition, deletion, damage, destruction, disclosure, alteration, or republication of data or information, the penalty shall be imprisonment for a period not exceeding three years and a fine no less than KWD 3000 (approx. $9,750) and not exceeding KWD 10,000 (approx. $32,500), or either of these penalties if the data or information disclosed are personal (Article 2);
- anyone who illegally accesses an information site or system, whether directly or through the internet or via means of information technology, to obtain confidential government data. They shall be punished by imprisonment for a term not exceeding three years and a fine of no less than KWD 3000 (approx. $9,750) and not exceeding KWD 10,000 (approx. $32,500), or either of these penalties. The penalty shall be imprisonment for a period not exceeding 10 years and a fine no less than KWD 5000 (approx. $16,250) and not exceeding KWD 20,000 (approx. $65,000), or either of these penalties if such access results in the deletion, damage, destruction, publication, or alteration of said data or information. This also applies to data and information relating to clients' bank accounts (Article 3); and
- anyone who deliberately modifies or destroys an electronic document related to medical tests, medical diagnosis, medical care, or medical treatment or facilitates or enables the same, by using the internet or any means of information technology. They shall be punished by imprisonment for a term not exceeding three years and a fine of no less than KWD 3000 (approx. $9,750)

and not exceeding KWD 10,000 (approx. $32,500), or either of these penalties (Article 3).

9.1. Enforcement decisions

Not applicable.

Topics: Privacy Overview

Jurisdictions: Kuwait