CITRA

الهيئة العامة للاتصالات و تقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Data Privacy Protection Regulation

Version: 2.0

Preamble

The demand for communications and information technology services, which are provided by service providers in the State of Kuwait through using advanced technologies such as Cloud Computing, Internet of Things, and others, has witnessed a surge by both the public and private sectors. However, due to the advantages of such services, which rely upon the resources of the operational structure and software as well as other information technology components that are provided and operated by communications and information technology services providers, including the processes of storage, transmission, or processing of the user's data and content, the Communication and Information Technology Regulatory Authority is cognizant of the need that the providers of communications and information technology services must be obligated to protect such data and the basic rights and freedoms of transmission respecting the privacy of collected personal data. As this entails that the Authority shall issue a set of regulatory tools, conditions, terms, and directives pertinent to the practice of providers of this activity, in addition to all that is relative to it of provisions, advantages, and obligations to promote such orientation.

Furthermore, the Communication and Information Technology Regulatory Authority aspires to develop a firm industry that relies upon the provision of the best communications and information technology services. As well as providing them to the government authorities, business sector and individuals across the State of Kuwait, which in turn enhances the work of the government, commercial and industrial activities, and contributes to attracting investors interested in this field. In addition to promoting competitive foundations that fulfil the vision of the State of Kuwait that aims at transforming it into a financial and commercial center (New Kuwait 2035).

Definitions

The following words and phrases, wherever they are used in this Guide, shall have the meanings designated for them below, as well as the definitions set out in the Law of the Communication and Information Technology Regulatory Authority and its executive regulation:

Authority: It means The Communication and Information Technology Regulatory Authority under Law No. (37) of 2014, its amendments and executive regulation.

Service Provider/Licensee: It means the natural or legal person who is licensed to provide one or more of the communications services to the public, or who is licensed to manage, setup, or operate a communications network or internet service to provide communications services to the users. This also includes information or content providers who provide such services through communications network.

Legal Person: It means an independent entity that aims to achieve a specific purpose and has a legal character within the scope of this purpose. It also applies to public or private companies or corporate entities owned by the state or organizations, which have a domicile in the State of Kuwait.

Personal Data: it means the data pertinent to a natural person or a legal person with a specified identity, or that can be identified through such data directly, such as identifying name and identity, or financial, health, ethnic or religious information. As well as any data that allows identifying the geographic location of the person, or the personal fingerprint or the DNA; or through bringing between the available data and any other data. As well as any audio file, including the person's voice, or any other identification data that allows connecting with that person via the Internet.

Beneficiary/User: It means the person who benefits from the public communications service, or which is intended for purposes pertinent to using communication processes.

Data Collection and Processing: It means any process or set of processes that are applied to personal data, whether inside or outside the State of Kuwait, using automatic methods, or other methods such as collecting, recording, organizing, analyzing, storing, modifying, retrieving, using or disclosing it through dispatch and publishing, or make it available, or integrating, restricting, deleting or destroying it.

Encryption: It means the process of transforming data from a readable text to an unreadable text by any person except for whoever owns special knowledge or a special key to retransform the encrypted text to a readable text. As the encryption process is applied either during data storage or when transferring it via communication networks.

Third Party: It means any natural or legal person that collects or processes personal data on behalf of the service provider and with its direction, which is made through data centers they possess or use directly or indirectly.

The Scope of Regulation

Article (1)

This regulation shall apply to all service providers from the public and private sectors who work on collecting, processing and storing personal data. As well as the user's data, in whole or in part, either permanently or temporarily, using automatic systems or through any other means that constitute part of the data storage system, whether such processing is made within the State of Kuwait or outside it.

Personal Data Collection and Processing Conditions

Article (2)

The service provider, and prior to providing the service to the user, shall do the following:

1) Provides all the information and terms of service, as well as the request for change or deletion of the data, which should be given in clear and easy statements and shall be available in both English and Arabic languages.

2) Obtains the approval of the service applicant respecting collection or processing of personal data, as well as his/her knowledge and acceptance of all terms, conditions, and provisions of data collection and processing.

3) Explains the purpose of collecting the user's personal data, which is necessary for service provision and the method of handling such data.

Article (3)

The process of collecting and processing data shall be only legitimate and legal in the following cases:

1) Obtaining the approval of the data owner.

2) It shall be necessary for compliance with a legal obligation to which the service provider is subject.

3) It shall be necessary for protecting the natural or legal person's data.

4) In case the purposes, which the service provider conducts, require the identification of the data owner's identity.

5) Obtaining the written approval of the child's guardian in case his/her age is under 18 years.

However, in all cases, the service provider shall have the ability to prove the data owner's approval to process the data thereof.

Article (4)

The service provider, during the service provision or following its termination, shall collect and process data in accordance with the following conditions:

1) Provides clear information that is easily accessible about their practices and policies respecting the personal data to ensure conducting the collection and processing processes, and with transparency.

2) Identifies the purpose of data collection and the legal basis for data processing, as well as the data retention period, if any.

3) Identifies the identity and location of the service provider, including the information regarding how to contact them regarding their practices and personal data processing.

4) Conducts data processing in a manner that ensures the protection of personal data from unauthorized or illegal processing, as well as against incidental loss, damage, or distortion of it, through using the appropriate technical and regulatory measures ("Safety and Confidentiality").

5) The service provider shall notify the Authority in case of disclosing the users' personal data to any associate or parent company of the service provider or a third party, either directly or indirectly. While the service provider shall be responsible for protecting the privacy of the shared data.

6) Applies the relevant technological means that enable the users to exercise their right to access the personal data and review and modify them directly. The service provider also shall grant the third party (if any) all the required and regulatory powers to use any software or any other intellectual property works protected by the law.

7) Provides information about the location of personal data storage in case it is inside or outside the State of Kuwait.

8) Identifies the mechanism of accessing, modifying, or deleting the personal data, or restricting access to it, processing it, objecting to its processing, or requesting the transfer of personal data.

9) Notifies the data owner in case the service provider intends to transfer the user's personal data outside the State of Kuwait.

10) Destroys the personal data in its possession upon the termination of the contractual relationship with the data owner.

11) Obtains the approval of the data owner prior to disclosing his/her personal data to any third party for marketing purposes that are not directly related to the provision of communications and information technology services requested by the user.

12) The service provider shall provide an easy-to-use, practical and accessible means that enables the user to withdraw its approval, or deactivate the method of collecting, using, processing, or disclosing his/her personal data.

13). The service provider shall delete the user's personal data if:

(a) The user has withdrawn its approval regarding the processing or use of personal data.

(b) The personal data is no longer required for the provision of services requested by the user.

(c) The user is no longer subscribed to the service for which the data was collected.

14) Every service provider shall create and maintain a written privacy policy that:

(a) Indicates in detail the service provider's processes and procedures respecting the collection, use, and disclosure of personal data, including the method it adopts for compliance.

(b) It shall be published on the service provider's website, and to be given to the users upon contracting for services.

15) In case the personal data stored by the service provider is inappropriately disclosed, and such disclosure or access has resulted in inflicting damage on a large number of users, the service provider shall notify the Authority and users, as well as law enforcement agencies at the earliest time possible and within no more than 24 hours in all cases.

16) Upon the preparation of any process, system, or procedures to provide facilitations or services of communications, the service provider shall adopt privacy through the design of services.

Security and Protection of Personal Data

Article (5)

The service provider shall take the following actions:

1) Takes the necessary measures to protect the user's personal data against loss, damage, disclosure, or breach by an unauthorized party; or otherwise, replace the data or information with other incorrect ones, or add incorrect information. While such measures must be consistent with the nature and scope of its activities, as well as the sensitivity of any personal data to be collected and stored, including the following:

(a) Processes and encryption of personal data, according to the level of data stated in the data classification policy of the service provider.

(b) Ensures the continuous confidentiality, integrity, availability and resilience of processing systems and services.

(c) Restores the availability and access to personal data in a timely manner in case of force majeure occurrence.

(d) Tests and evaluates the effectiveness of technological and regulatory measures to ensure the security of processing.

2) Secures and protects the data from incidental, or illegal damage, loss, alteration, unauthorized disclosure, or access to the personal data sent or stored, or that is processed by other methods.

3) Adheres to international policies and practices relative to business continuity, and disaster recovery, as well as risk management and information security.

4) Maintains the processing activities records; and the records shall include all the following information:

(a) The name and contact details of the service provider, and its representative, if it is outside the State of Kuwait, as well as the data protection officer.

(b) The purposes of data processing.

(c) Description of data owners' categories and other personal data categories.

(d) Transfer of personal data, if necessary, outside of the State of Kuwait, with the identification of such state's identity.

(e) General description of the adopted security, technical and regulatory measures.

5) Makes the records available to be reviewed by the Authority upon request.

6) Takes into consideration the controls relative to the design, change, or development of products, systems and services, which can affect personal data processing.

7) Develops and adheres to internal policies for data protection and privacy.

8) Identifies, trains, and educates personal data protection officers.

9) Develops internal systems for receiving and investigating complaints around the clock, as well as data access requests, in addition to requests of modifying and deleting it.

10) Develops internal systems for effective management of personal data, and informs any violation of procedures that aim to protect it.

11) Conducts comprehensive audit and review processes on the extent of compliance with personal data protection.

Notifying the Communication and Information Technology Regulatory Authority in case of Personal Data Breaches

Article (6)

1) The service provider, upon the occurrence of personal data violation and within a period not exceeding 72 hours from its knowledge of it, shall notify the Communication and Information Technology Regulatory Authority of such breach of personal data.

2) The notice includes:

(a) The nature of breach, the extent of personal data leakage, the users whose data has been leaked, as well as the affected security levels.

(b) The name and mechanism of communication with the data protection officer.

(c) The potential results of the breach, and the measures taken or that the service provider proposes to remedy the violation.

(d) Notifying the personal data owner in case of personal data breach occurrence.

1) It is unnecessary to notify the data owner if the service provider has taken the relevant technical and regulatory protection measures, and such measures have been applied to the personal data affected by such breach.

2) Takes the subsequent measures that guarantee the mitigation of risks against the rights and freedoms of data owners.

General Provisions

Article (7)

1. All service providers or those authorized to own public communications networks shall rectify their status in accordance with the provisions of this regulation and other regulations pertinent to this regulation, which have been issued by the Authority within a period not exceeding a year from the date of its publication.

2. Where necessary, the Authority may issue instructions or directives relative to data privacy.

3. The Authority, in case of substantial violation of the provisions of this regulation or the laws of the State of Kuwait, may apply the penalties and sanctions provided for in Law No. (37) of 2014 concerning the establishment of the Communication and Information Technology Regulatory Authority (CITRA), amended by Law No. (98) of 2015.