CITRA

الهيئة العامة للاتصالات و تقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Data Privacy Protection Bylaw

V2.5

Contents

Introduction

The demand for communications and information technology services is increasing by the public and private sectors provided by the providers of these services in the State of Kuwait using advanced technologies, such as Cloud Computing solutions, Internet of Things …etc. As well as the advantages these services provide that depend on the resources of the operational structure, software, and other elements of information technology provided and operated by telecommunications and information technology service providers, including collection and processing of user's data and content.

The Communication and Information Technology Regulatory Authority ("CITRA") is aware of the need for communication and information technology service providers to adhere to data protection and basic rights and freedoms of transfer related to the privacy of collected personal data, which in turn motivates the Authority to issue a set of regulatory tools that include conditions, and principles. As well as directives related to regulating data management and processing practices by providers of communications and information technology services and all related provisions and obligations to support this regulatory approach.

Furthermore, the Communication and Information Technology Regulatory Authority aspires to develop a solid industry that relies on providing the best communications and information technology services for the purpose of providing them to government agencies. As well as the business sector and individuals within the State of Kuwait, which supports the work of governmental, commercial, and industrial activities, and contributes towards attracting investors interested in this field and strengthening competitive foundations to achieve the vision of the State of Kuwait towards advancement to a financial and commercial hub (New Kuwait 2035).

Definitions and Technical Terms

The following words and expressions, wherever mentioned in this Guide, shall have the meanings assigned to them below, and the definitions contained in the Communication and Information Technology Regulatory Authority's Law and its Executive Regulations shall also be adopted:

CITRA: The Communication and Information Technology Regulatory Authority under Law No. (37) of 2014 as amended by Law No. (98) of 2015, and its executive regulations.

Service Provider/Licensee: A person who is licensed to provide one or more communications services to the public, or who is licensed to manage, set up, or operate a telecommunications network, or an Internet service to provide telecommunications services to the public, including providers of information or content provided via a telecommunications network.

Legal Person: An independent and autonomous entity that achieves a specific purpose and enjoys legal personality within the limits of this purpose. This applies to companies or institutional

entities, private or public, owned by the state or organizations that have a domicile in the State of Kuwait.

Personal Data: Data related to a natural or legal person identified or can be identified through this data in a direct way, such as identifying the name and identity, or financial, health, ethnic, or religious information, or any data that allows identifying the person's geographical location or personal fingerprint, DNA, or by a combination of available data with any other data, or any audio file including a person's voice, and any other identifier that allows online communication with a person.

Beneficiary/User: A person who benefits from a public telecommunications service or intends to use it for special purposes using communication operations.

Data Collection and Processing: Any operation or set of operations undertaken on personal data, whether inside or outside the State of Kuwait, using automated means or other means such as collecting, recording, organizing, analyzing, storing, modifying, retrieving, using or disclosing through transmission, publishing, making available, merging, restricting, deleting or destroying them.

Removal and Deletion of Data: A process or set of operations taken by the licensee/service provider with the aim of stopping the use of customer data for commercial purposes and not making it available to the public, with the possibility of continuing to keep this data and use it for security purposes. As well as to implement judicial decisions and judgments and financial claims resulting from the subscription contract concluded between the beneficiary/user and service provider/licensee only.

Third Party: Any natural or legal person who collects or processes personal data on behalf of and at the direction of the Service Provider, whether directly or indirectly.

Article (1): Bylaw Scope

This bylaw applies to all service providers licensed by CITRA, who collect, process, and store personal data and user data content in whole or in part, whether permanently or temporarily by automated means or by any other means that form part of the data storage system, whether the processing takes place inside or outside the State of Kuwait.

The provisions of this bylaw do not apply to practices related to security investigations and monitoring violations or practices contrary to laws, decisions, judicial rulings, and financial claims arising from the subscription contract.

Article (2): Conditions for Collections and Processing of Personal Data

The service provider must, before providing the service to the user, do the following:

1) Provide all information and conditions of service and request changing or canceling the data, explained in easy terms, and be available in both English and Arabic.

2) Obtain approval of the service applicant to collect or process personal data along with his knowledge and acceptance of all terms, obligations and provisions of data collection and processing.

3) Clarify the purpose of collecting the user's personal data necessary to provide the service and how this data is used.

Article (3): Legality of Data Collection and Processing

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

1) Obtain the consent of the user who owns the data.

2) It is necessary to comply with a legal obligation to which the service provider is subject.

3) It is necessary to protect the user's data.

4) If the purposes, carried out by the service provider, require identification of the data holder.

5) Obtain written consent from the guardian of the minor if he/she is less than (18) years old.

In all cases, the service provider must be able to prove the consent of the data owner to process the data.

Article (4): Conditions for Data Collection and Processing

The service provider must, during the provision of the service or after its termination, collect and process data according to the following conditions:

1) Provide clear and easily accessible information about their practices and policies in relation to personal data to ensure that the collection and processing operations are conducted in a transparent manner.

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

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

4) Process data in such a way as to ensure the protection of personal data against unauthorized or unlawful processing and against accidental loss, damage or detriment to it using appropriate technical and organizational measures ("Integrity and Confidentiality").

5) The service provider must notify CITRA if the personal data of users is disclosed to any affiliate or owner of the service provider or a third party, directly or indirectly, provided that the service provider is responsible for protecting the privacy of the data involved.

6) Using appropriate technological means that enable users to directly exercise their right to access, review and correct personal data, and the service provider must grant the third party (if any) all necessary and regulatory powers to use any software, or any other intellectual property work protected by the system.

7) Provide information on the place where personal data is stored, whether it is inside or outside the State of Kuwait.

8) Determine the mechanism for obtaining, correcting or removing personal data, restricting access to or processing it, objecting to its processing, or requesting the transfer of personal data.

9) Notify the data owner if the service provider intends to transfer his/her personal data outside the State of Kuwait.

10) Remove the personal data in his possession upon termination of the contractual relationship with the data owner.

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

12) The service provider must provide an easy-to-use, practical and easily accessible means that enables the user to modify his/her data, withdraw their consent, disable the service, or the method of collecting, using, processing, or disclosing their personal data.

13) The service provider must remove the user's personal data if:

    a) The user withdraws consent to the processing or use of the personal data.

    b) The personal data is no longer necessary to provide the services requested by the user.

c) The user is no longer subscribed to the service in respect of which personal data was collected.

14) The Service Provider shall establish and maintain a written privacy policy that:

a) Describes in detail the Service Provider's operations and procedures with respect to the collection, use, and disclosure of personal data, including the method it will adopt for compliance.

b) It is published on the website of the service provider and is provided to users when contracting for services.

15) If the personal data stored by the Service Provider is improperly disclosed and such disclosure or access causes harm to a large number of Users, the Service Provider shall notify CITRA, the Users and law enforcement agencies as soon as possible and in no case within no more than (72) hours.

16) When setting up any process, system or procedures to provide telecommunication facilities or services, the service provider must adopt privacy through the design of the services.

Article (5): Security and Protection of Personal Data

The service provider shall:

1) Provide appropriate security measures to protect the user's personal data against loss, damage, disclosure or hacking by an unauthorized third party or replacing data or information with incorrect ones or adding incorrect information. Such measures must be appropriate to the nature and scope of its activities and the sensitivity of any personal data collected and stored, including the following matters:

a) Process and encrypt personal data, and in accordance with the level of data specified in the data classification policy of the service provider.

b) Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.

c) Timely restoration of availability and access to personal data in the event of force majeure.

d) Test and evaluate the effectiveness of technical and organizational measures to ensure processing security.

2) Secure and protect data from accidental or unlawful destruction, loss, and/or alteration or unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

3) Adhere to global policies and practices related to business continuity, disaster recovery, risk management, and information security policies.

4) Maintain records of processing activities, and that the records include all of the following information:

    a) The name and contact information of the service provider, and its representative if outside the State of Kuwait and data protection officer.

    b) Purposes of data processing.

    c) Description of the categories of data owners and other categories of personal data.

    d) The transfer of personal data, if necessary, outside the State of Kuwait with the identification of this country.

    e) General description of the technical and organizational security measures adopted.

5) Make the records available for review by CITRA upon request.

6) Take into account the controls for designing, changing or developing products, systems and services that may affect the processing of personal data.

7) Develop and adhere to internal data protection and privacy policies.

8) Identify, train and educate those responsible for the protection of personal data.

9) Establish internal systems for receiving and studying complaints around the clock, requests for data access, and requests for correction or deletion.

10) Establish internal systems for the effective management of personal data, and reporting any violation of the procedures aimed at protecting it.

11) Conduct comprehensive audits and reviews of the extent of compliance with the protection of personal data.

12) Notify CITRA of any breaches of personal data.

Article (6): Notification of Personal Data Breaches

1) The service provider, upon the occurrence of a breach of personal data, and within a period not exceeding (72) hours after its knowledge of the occurrence of a breach of the personal data, shall notify CITRA.

2) The notification shall include:

    a) The nature of the breach, the extent of the personal data leakage, the persons whose information was leaked, and the security levels affected.

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

    c) The possible consequences of the hack, and the measures taken or proposed to be taken by the Service Provider to remedy the breach.

    d) Notify the owner of personal data in the event of breaches of personal data.

3) It is not necessary to inform the data owner if the service provider has taken appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach.

4) Take subsequent measures to ensure that the risks do not increase to the rights and freedoms of data owners.

Article (7): General Provisions

1) All service providers or those authorized to own public telecommunications networks must reconcile their status with the provisions of this Regulation and other regulations related to this Regulation issued by CITRA within a period not exceeding one year from the date of its publication.

2) CITRA may issue instructions or guidelines related to data privacy whenever necessary.

3) In the event of a violation of the provisions of these regulations or the laws of the State of Kuwait, CITRA may apply the penalties and fines stipulated in Law No. (37) of 2014 on the establishment of CITRA, as amended by Law No. (98) of 2015.