CITRA

الهيئة العامة للاتصالات و تقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Data Privacy Protection Regulation

Version: V1.8

Preface

Demand for information technology services is growing, by both the public and private sectors, as service providers in the State of Kuwait offer such services using traditional and advanced technologies such as Cloud Computing solutions, Block Chain and Internet of Things "IoT", in addition to other technologies. This is due to the advantages associated with such services, which depend on the resources of operational infrastructure, software and other elements of information technology that are provided and operated by Communications and Information Technology Service Providers, that include storage, transfer, or process the user's data. Therefore, CITRA realizes the need for Communications and Information Technology Service Providers to commit to the protection of such data and basic rights and freedoms in respect of transferring the privacy of aggregated personal data. This in turn requires CITRA to issue a set of regulatory tools, conditions, and guidance related to the practice of service providers and all associated provisions and benefits, and obligations to support this vision.

The Communications and Information Technology Regulatory Authority ("CITRA") aspires to develop a robust industry that relies on the best communication and IT services, making it available to government bodies, businesses and individuals within the State of Kuwait. This would enhance government, commercial and industrial activities and contribute to attracting investors interested in this field, and strengthen competitiveness foundations to realize the State of Kuwait's vision in transforming it into a financial and commercial center (New Kuwait 2035).

Definitions

The following words and phrases wherever used in this guide shall have the meanings assigned to them below and the definitions contained in the Communications and Information Technology Regulatory Authority Law and its executive regulations shall be adopted:

CITRA: The Communications and Information Technology Regulatory Authority established under Law 37 of 2014, its amendments and executive regulations.

Communications and Information Technology Service Provider (Service Provider): A natural or legal person who provides communications and information technology services in Kuwait and who provides, manages, establishes, creates a public communications network, operates a website, smart application or cloud computing services, collects or processes personal data or directs another party that collects and processes personal data on its behalf through information centers that they own or use directly or indirectly.

Legal Person: Is an independent autonomous entity that seeks to achieve a specific objective and enjoys legal personality within the limits of this objective. Such definition applies to private or public companies or institutional entities owned by the State or organizations that maintain a domicile in the State of Kuwait.

Personal Data: Such data relevant to a natural or legal person whose identity is identified or can be identified through such data directly using name, identity, financial, health, racial or religious information or any information that allows the identification of a person's geographical location or personal tracking systems, personal fingerprint or genetic fingerprint, or through a combination of available data and any other data, or any audio file including the person's voice, and any other identifier that allows physical or online contact with the person who shall be referred to as the data owner.

Data Collection and Processing: Any process or set of processes applied to personal data, whether inside or outside Kuwait, using automated means or other means such as collecting, recording, organizing, analyzing, storing, modifying, retrieving, using or disclosing through transmission and posting, making available, merging, restricting, deleting or destroying the same.

Encryption: The process of converting data from readable text to unread text by anyone except by someone with special knowledge or special key to re-encode the encrypted text to readable text.

Encryption process applies either while the data is being stored or when transmitted across communication networks.

Data Center: A center that contains an operating structure for information technology and communication services and hosts communication and IT services inside or outside the State of Kuwait.

Third Party Content: Such content provided to the user by a third party that is not authorized to process its personal data and is related to the user preferences such as marketing and advertising materials.

Privacy Notice: A notification or message sent by the telecommunications and Information Technology Services provider about the user's personal information and the practices on which it will be conducted.

Scope of the Regulation

Article (1)

Such regulation apply to all public and private sectors service providers who collect, process and store personal data and user related content in whole or in part, either permanently or temporarily using automated means or any other means that are part of a data storage system, whether processed inside or outside the State of Kuwait when it relates to processing activities linked to transmission of advertising or marketing material or monitoring the behavior and tendencies of data owners.

Article (2)

1) The provisions of such regulation do not apply to a natural person who collects and processes personal and family data.
2) Such regulation shall not apply to security authorities for the purposes of crime prevention, investigation, discovery, prosecuting the perpetrators, the enforcement of criminal penalties or preventing threats related to public security.

Data Classification

Article (3)

Any person, whether natural or legal, who wishes to contract with any service provider, shall classify his data for information security purposes by following the data classification policy adopted by CITRA or global best practices.

Personal Data Collection and Processing Conditions

Article (4)

Prior to providing the service to the user, service providers shall:

1) Provide all information and service conditions as well as request to change or delete data in easy terms in both English and Arabic.
2) Obtain the consent of the service applicant to collect or process personal data, his knowledge and consent to all conditions, obligations, and provisions applicable to data collection and processing.
3) Clarify the purpose of collection of user data being necessary to provide the service and how such data may be used.

Article (5)

Data processing shall be lawful and legitimate only if one or more of the following conditions is available:

1) Consent of the data owner;
2) Be necessary to comply with a legal obligation to which a communication and IT service provider is subject;
3) Be necessary to protect the natural or legal person data;
4) If the objectives performed by a service provider do not require identification of the data owner identity.
5) Obtain an explicit consent of the guardian of a child whose age is less than 18 years. Acceptable efforts will be exerted, and available technologies considered to verify the age of the user. CITRA shall establish the mechanism to obtain the guardian's consent.

In any case, the service provider shall be able to demonstrate that the data owner has agreed to process the data.

The data owner shall be entitled to withdraw his consent at any given time. Such withdrawal of the consent shall not affect the legality of processing before it is withdrawn. The service provider shall facilitate withdrawal of consent as at the start of the process. The data owner shall be entitled, upon requesting withdrawal of consent, to request the service provider to destroy his data processed before withdrawing it and the service provider shall destroy such data from his hardware devices and logs and refrain from keeping any duplicates thereof.

Article (6)

During or after the service is provided, the service provider shall collect and process the data in accordance with the following conditions:

1) Provide clear and easily accessible information about their personal data practices and policies to ensure that collection and processing are conducted transparently.
2) Specify the purpose of data collection and legal basis for data processing and retention period, if any.
3) Identify such authorities to which personal data is disclosed.
4) Specify the identity and location of the service provider, including information on how to contact them about their practices and processing personal data.
5) Maintain personal data in a form that allows identifying data owners identities for the purposes personal data are processed.
6) Process data in a way that ensures personal data are protected against unauthorized or illegal processing and accidental loss and impairment or damage using appropriate technical and organizational measures ("Safety and Confidentiality").
7) Use of appropriate technology means that enable individuals exercise their right to have direct access to, review and edit personal data. The service provider shall grant its support IT staff all necessary and regulatory licenses to use any software, or other intellectual property works protected by the system.
8) Provide information on personal data storing period and storage location, or if storing feature is not available.

9) Determine a mechanism for obtaining, correcting, deleting, restricting access or processing, objecting to processing or filing a request for the transfer of personal data.
10) Notify the data owner in case the service provider intends to transfer his personal data out of Kuwait in accordance with the data classification policy issued by CITRA.
11) Inform the personal data owner in the event that the service provider intends to perform further processing of personal data for purposes other than those for which the personal data was collected.
12) Destroy personal data in its possession once the contractual relationship with the data owner has expired, or during the contract term if the data owner so requests.
13) Refrain from collecting, using, processing or disclosing any personal data to any person without first obtaining the consent of the respective person or representative thereof.
14) The data owner shall not be required to provide and disclose unsolicited personal information in connection with the provision of the product or service that he or she requests, and, as a condition of the provision of a product or service, may not require the user to consent to the collection, use or disclosure of personal information required to provide this product or service.
15) Prior to collecting personal information, shall indicate the purpose by which the personal information collected by the service provider will be used.
16) Use personal information only for purposes collected as specified by the service provider.
17) Obtain the consent of the data owner before disclosing his personal data to any subsidiary or third party for any marketing purposes that are not directly related to the provision of communications and information technology services requested by the person concerned.
18) Implement appropriate security measures to protect users personal data against loss, damage, disclosure, breach by any unauthorized third party, replace or add data or information with incorrect ones. Such measures shall be appropriate to the nature and scope of providers activities and the sensitivity of any personal information collected and stored.
19) A person who has already agreed to collect, use, process or disclose his personal information may withdraw such consent at any time, and every licensee who provides public communications and information technology services may provide an easy-to-use,

practical and easily accessible way through which the person can withdraw his consent or disable the way personal information is collected, used, processed or disclosed.

20) The service provider shall, at the request of the data owner, provide access to any personal information collected in relation to the end user of such information. The licensee shall modify any personal information when such personal information is incorrect, outdated or invalid.

21) The service provider shall delete the user's personal information if:

(a) The user has withdrawn his consent for the processing or using of personal information.

(b) Personal data is no longer required to provide the services requested by the user.

(c) The end user is no longer involved in the service for which personal data has been collected.

22) Each Communications and Information Technology Service Provider shall create and maintain a written privacy policy that:

(a) Establish in detail the service provider's processes and procedures regarding the collection, use and disclosure of personal information, including the manner in which they will comply.

(b) Is posted on the service provider's website and provided to users when they subscribe to the services.

23) Each Communications and Information Technology Service Provider shall:

(a) Provide a privacy notice which:

1. Informs customers clearly and accurately of the personal information they collect, use and store, and the circumstances in which they share such information with other entities.

2. Informs users of their right to consent, withdraw approval, or cancel any use of end-user personal information in accordance with this article.

3. Provides an option that allows the user not to receive an email, text message or phone call related to marketing materials if they don't wish to.

(b) Announce the privacy notice referred in Article (6) on its website in a manner viewed by any sensible person, and merge it as part of the online application and transaction forms as well as make it available at the points of sale.

(c) Provide users with a prior notice of any fundamental change in their privacy policies.

24) Each Communications and Information Technology Service Provider shall ensure that any person engaged in the collection, handling or use of personal information is fully informed and trained on the licensee's practices of protecting security and privacy, whether such person works for him or any third party contracted by the service provider for the purpose of collecting or processing the personal data of users. When it is necessary to provide user's personal information to affiliates or other third parties to provide a service, the licensee shall ensure, through contractual means, that such subsidiaries and other parties take all necessary steps and measures to protect confidentiality, security and use personal information solely for the purpose of providing the required service.

25) Upon prior notice, CITRA may visit the premises of the licensee or any third party who processes personal information on its behalf to review the security measures in place to maintain the protection of personal information. If CITRA is not reasonably satisfied with such measures, it may instruct the licensee or its affiliates to strengthen security measures and processes as it deems appropriate.

26) If personal information stored by the licensee is incorrectly disclosed or accessed by a third party, and this disclosure or access causes harm to a large number of users, the licensee shall notify CITRA, end users and law enforcement agencies as soon as possible and in no more than 24 hours after the licensee reasonably determines that there has been a violation of this disclosure or access.

27) When preparing any process, system, or procedure to provide communications facilities or services, the licensee shall adopt privacy through the design approach in which the principles set out in this article will be incorporated into such process, system, or procedure.

28) The licensee may not disclose the personal user data of any associate or owner company of the service provider directly or indirectly without the written consent of CITRA.

Security and Protection of Personal Data

Article (7)

The service provider shall establish the following:

1) Measures to ensure the appropriate level of protection for risk response, considering the latest technology, taking into account the potential risks and impact in respect of the rights and freedoms of natural and legal persons, including:

   (a) Processing and encrypting personal data. CITRA shall determine the mechanism and standards of encryption according to the level of data specified in the Data Classification Policy issued by CITRA.

   (b) Continuous confidentiality, integrity, availability and flexibility of processing systems and services.

   (c) Restoring availability and timely access to personal data in the event of force majeure.

   (d) Testing and evaluating the effectiveness of technical and regulatory measures to ensure processing security.

2) Secure data against accidental or illegal destruction, loss, change, unauthorized disclosure, access to personal data sent, stored or processed in any other way.

3) Comply with any rules or directives authorized by CITRA regarding business continuity, disaster recovery, and risk management to ensure that any regular person with access to personal data processes such data as per the instructions of the service provider.

4) Keep records of processing activities provided that such records include all the following information:

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

(b) Data processing purposes.

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

(d) Transfer of personal data, if necessary, out of Kuwait with the identification of such country.

(e) A general description of the technical and regulatory security measures used.

5) Make records available for viewing by CITRA upon request.

6) Take into account the controls for the design, change or development of products, systems and services that can affect the processing of personal data.

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

8) Identify, train and educate processing staff responsible for protecting personal data.

9) Develop internal systems for receiving and examining complaints, requests for access to data, and requests for correction or deletion around the clock.

10) Develop internal systems for effective personal data management and report any breaches of procedures aimed at protecting the same.

11) Conduct comprehensive audits and reviews as to the extent of the adherence to protect personal data.

12) Provide 24-hour communication with the data protection officer in relation to all issues related to the processing of their personal data and the exercise of their rights under these regulations.

13) On-demand advice on assessing the impact of data protection and monitoring its performance in cooperation with CITRA.

Notification to Communications and Information Technology Regulatory Authority (CITRA) in the Event of Breaches to Personal Data

Article (8)

1) The service provider shall, within a period not exceeding 72 hours following its knowledge of the incident, provide a notification of any breach incident of personal data to CITRA.

2) The notification shall include:

(a) The nature of the breach, the extent to which data leaked, the persons affected, and the security levels that have been breached.

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

(c) Possible consequences of breach, and measures taken or proposed by the service provider to address the penetration.

(d) Notify the personal data owner in the event of breach to his personal data.

Article (9)

1) Upon the occurrence of a breach of personal data, the service provider shall notify the personal data owner within a period not exceeding 72 hours following its knowledge and such notification shall include the nature of the breach and technical protection measures.

2) It shall not be necessary to notify the data owner if the service provider has taken the following steps:

(a) Appropriate technical and regulatory protection measures were taken, and such measures were applied to personal data affected by the breach.

(b) Subsequent measures were taken to ensure that risks associated with the rights and freedoms of data owners are not escalated.

Violating Content

Article (10)

1) The service provider shall not be held responsible for any civil, administrative or criminal liability if the violating content of the system or user content that violates intellectual property rights of any third party uploaded, processed or stored in the service provider systems, unless the service provider becomes aware of it and fails to take appropriate action.

2) Service providers may on their own initiative, or at the request of any third party, remove or restrict access in the State of Kuwait and/or in any other country to any violating content of the system or user content that violates third-party intellectual property rights.

3) Service providers shall notify CITRA and/or any competent entity, without delay, if they discover the existence of any user content or any information in a system that may constitute a violation under the Electronic Crimes Law as well as the laws and regulations applicable in the State of Kuwait.

4) Service providers shall refer any third party that has a complaint against violating content in their systems to the competent authorities in the State of Kuwait.

General Provisions

Article (11)

1. All service providers or such parties licensed to own public communication networks shall reconcile their status with the provisions of these regulations and other related regulations issued by CITRA within a period not exceeding one year from the date of publication.

2. CITRA may issue instructions or guidance regarding the privacy of the data whenever necessary.

3. In the event of a proven violation to the provisions of these regulations or the laws of the State of Kuwait, CITRA may apply the penalties and fines stipulated under Law No. 37 of 2014 establishing the Communications and Information Technology Regulatory Authority as amended by Law No. (98) of 2015.