Cloud Computing & Data Classification in the State of Kuwait

Margaret McKenzie - Associate - Corporate / Mergers and Acquisitions
m.mckenzie@tamimi.com - Kuwait City

On 21 September 2021, the Kuwait Communication and Information Technology Authority ("CITRA") issued a comprehensive cloud regulatory framework. Cloud service provider models include infrastructure-as-a-service ("IaaS"), Platform-as-a-Service ("Paas"), or Software-as-a-service ("Saas"), and their commitments and responsibilities vary depending on the model. In this article, we discuss the cloud computing guidelines as well as the related new CITRA Resolution No. 95 of 2021, Data Classification Policy Amendment ("Data Classification Policy").

With regard to cloud computing, the new framework utilises the Data Classification Policy tier system and has specific guidelines regarding handling cloud data in relation to the classifications. Certain obligations arise depending on the type of data and how it is processed. Below we lay out a few notable points in the cloud computing guidelines and Data Classification Policy in the State of Kuwait.

Information Security in Kuwait

Initially, the Data Classification Policy only listed three levels of data classification. In the subsequent amended policy, four levels were listed and additional categories were considered. In summary, the classifications include the following:

Level One: Is any non-classified data that is available to the public or that is not protected from public disclosure or subject to withholding under any law, regulation, or contract, and may not entail any encryption, as it does not relate to the Data Owner or government or private sector. Some examples include, but are not limited to, the following:

1. Open data such as policies, regulations and laws published on websites, official gazettes, daily newspapers, magazines or other publications.
2. Self-service forms available to individuals and institutions.
3. Public data and information made available to the public on websites.

Level Two: Is private insensitive data, it is any data owned by public or private sectors or by persons indicating the identity of the Data Owner. Unauthorised disclosure of such data will not lead to infringing privacy of the Data Owner. Examples of such data include, but are not limited to, the following:

1. First name or last name;
2. Job title, job duties and employer;
3. E-mail;
4. ID No.;
5. Sex;
6. Age;
7. Academic Qualification;
8. Social status;
9. Contact details such as: work telephone number, mobile phone number, or home phone number.

Level Three: Is private sensitive data. It means any data owned by public or private sectors or by persons. Data that indicate the identity of the Data Owner and is related to the content of the Data Owner. It may include a part of the non-sensitive data. Unauthorised disclosure of such data will infringe the

privacy of the Data Owner. Examples of such data include, but are not limited to, the following:

1. Minutes of meetings and work plans;
2. Internal project reports;
3. Legal action and proceedings files, in addition to the relevant the primary and final judgements thereon, court decisions and orders, and all related files;
4. Legal briefs and opinions rendered by law firms;
5. Medical Records;
6. Criminal fingerprints and DNA

Level Four: Is highly sensitive data – it means any private data of a high sensitive nature. Unauthorised disclosure of such data may cause serious infringement on the privacy of the Data Owner or data owned by government, private sector, individuals or at the national level. Therefore, such data may be only circulated to a very specific category of individuals who require authorisation to such data. Such data contains high encryption requirements and needs the highest level of protection and security. Examples of such data include, but are not limited to, the following:

1- Encryption key;

2- Political documents, international negotiations or international relations;

3- Sensitive information of a military nature or related to State security;

Ultimately, level three and level four of the Data Classification Policy provide extra protections and considerations for individuals and service providers. CITRA grants licenses to cloud computing service providers who host the third and fourth data levels, and who have data centres within the State of Kuwait. If the data is classified above level three under the Data Classification Policy, the data owner must encrypt the data. The service provider may only disclose the subscriber's content or data only in the following cases:

1. Based upon an official request from security or intelligence authorities, in compliance with the laws enforced in the State of Kuwait.
2. Upon the subscriber's approval for the service provider to do so and when the data is not within the third and fourth levels of data classification. Also the subscriber has the right to cancel this approval in the future.

Entities that utilize Paas and SaaS cloud models from cloud service providers and that host data from first and second level of data classification will direct the cloud service providers to register and obtain permission from CITRA. Service providers are prohibited from signing any contracts to provide cloud services in the public sector in Kuwait until they have registered and obtained permission or a license from CITRA.

Service providers must notify their subscribers "without delay" if their information security has been compromised or reviewed without authorisation. If such data falls under the third or fourth levels, the service provider must alert the relevant authorities as well.

Generally, cloud service providers should review their operations and ensure they are following the guidelines as appropriate. For instance, cloud computing service providers are obligated to inform their subscribers in advance and obtain their prior consent before transferring or processing their content permanently or temporarily outside the state of Kuwait. Further, cloud service providers are responsible for the security of their cloud environment and their available security controls, the level of security required by subscribers, not responsible for monitoring the subscriber's content and data or determining their level of confidentiality, and not responsible for the damage caused by the negligence of subscribers resulting from not using the information security controls provided by the service provider. The security measures to protect subscribers' data becomes stricter as the tier of classification of such data increases. Data that

falls under the fourth tier of classification requires special handling. CITRA has the right to adjust the tiers of classification and their security requirements.

CITRA and relevant authorities are constantly updating their policies and resolutions. These new regulations appear to provide more data protection regulatory clarity on cloud computing in the State of Kuwait. According to the Data Classification Policy, the regulatorisation of government entities shall be subject to the Data Classification Policy within a period that shall not exceed two years. Entities should consult with their legal counsel on the nuances of these new regulations to develop appropriate policies and practices in line with the State of Kuwait's evolving data protection regulatory landscape.

For further information, please contact Phil Kotsis or Margaret McKenzie.