Diplomatic immunity for data: Bahrain’s Data Embassy Law

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

Krishna Jhala - Senior Counsel - Digital & Data
k.jhala@tamimi.com - Abu Dhabi

Hussain Osman
h.osman@tamimi.com - Manama, Bahrain

The practice of cloud computing by using a network of remote servers hosted on the Internet to store, manage and process data, rather than a local server or PC, is increasingly common place. However, storing of data on the cloud also has its potential downsides and countries have tried to implement new laws in order to protect important information.

As the Kingdom of Bahrain moves towards becoming a cloud computing hub, it extended its innovative scope in 2018 by implementing new legislation that allows foreign parties to store their data in data centres located in Bahrain under what is known as a ‘data embassy’ which blurs the legal lines of national borders and sovereignty.

It is revolutionary as when fully implemented it will allow consumers to store their information in data centres in the Kingdom of Bahrain while having the comfort of their data being governed by the domestic data protection law of their residence.

What is a Data Embassy?

A Data Embassy is a relatively new legal concept. It was first introduced through a bilateral agreement between the governments of Estonia and Luxembourg in 2017.

In 2007, Estonia reportedly fell victim to 'distributed denial-of-service attacks' by Russian attackers which consequently took a number of government and bank websites offline and threatened to make Estonia's entire public sector data communications network inoperable.

The Estonian Government's response was to strengthen their protection against such attacks, penalisation for cybercrime, and to develop the concept of an out of country 'data embassy' under which Estonian data and related systems are stored in Luxembourg's government owned data centre. As with physical embassies, the Estonian state owned servers resource outside its borders are considered sovereign embassies in the Luxembourg data centres.

The Cloud Computing Services Law in Bahrain

In 2018, the Kingdom of Bahrain implemented the Legislative Decree No. 56 of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties ('Cloud Law'). The Cloud Law's purposes is to 'provide a legal framework that encourages Foreign Parties use of an investment in Cloud Computing Services within Data Centres.'

Under Article 3 of the Cloud Law the data stored in data centres by overseas consumers of cloud services in the Kingdom of Bahrain will be subject to the domestic law in the 'Foreign State' where the relevant consumer resides (or is incorporated in cases of legal persons) and so will be subject to the jurisdiction of that Foreign State's courts, and other competent authorities.

Therefore, the courts and other competent authorities of the consumer's Foreign State are empowered to issue binding judgments with respect to any dispute which may arise between the overseas consumer and the domestic service provider, for example, orders for providing access, disclosure, preserving or maintaining the integrity of the consumer's data.

This means that competent courts and competent public authorities have to issue binding orders in the event of a dispute arising between an overseas consumer and the domestic service provider in Bahrain, 'including orders for providing access, disclosure, preserving or maintaining the integrity of the Customer Content.'

A service provider is obliged to inform the Attorney General in writing 'as soon as practicable' when they have received an order from a competent court or competent public authority of a Foreign State and must provide a copy of the order.

The competent judge and Attorney General in Bahrain can order the enforcement of any executable order, 'which is final and not subject to further appeal' concerning matters relating 'to providing access, disclosure, preserving or maintaining the integrity of Customer Content, or any matter in connection with Customer Content (…).'

What does it mean for cloud service customers?

Consumers worry about the safety of their data being held outside of their reach while awareness of the possible vulnerabilities of data is increasing.

The Cloud Law addresses what is a significant concern that there is always a risk that country data does not have the same level of protection as your own. Further, it clarifies who can have access to it.

However, the law is not yet fully effective. The Cloud Law only applies to:

- **Data Centre** defined as any data centre designated under Article 4 of the Cloud Law that is physically located in the Kingdom and which provides Cloud Computing Services to Customers; and
- **Foreign State** defined as any foreign state, including where applicable any of its territorial units which has its own laws, designated under Article 4 of the Cloud Law

The Kingdom of Bahrain's Council of Ministers shall issue a resolution to designate local Data Centres subject to the Cloud Law and Foreign States which have jurisdiction to issue judgments in connection with foreign consumers' data. To date no such resolutions have been issued.

Accordingly, the data embassy concept is still very new and not yet fully developed

At the same time there appears to be an increasing number of data localisation laws being introduced.

Data Localisation Law

In contrast to the concept of data embassies, a data localisation or data residency law mandates that data about a country's citizen or residents be collected, processed, and /or stored inside that country that businesses operating on the Internet, store and process data within the country.

By way of example, under the UAE's Federal Law No. 2 of 2019 Concerning the use of Information and Communications Technology in HealthCare it is not permitted to store, develop or transfer health data outside of the UAE that is related to health services provided within the UAE, except where the relevant health authority and the Ministry of Health and Prevention have passed a resolution to allow specific data to be handled outside of the UAE.

The common justification for data localisation laws is that where data is stored onshore ensures security and privacy.

However, data localisation laws clearly create barriers and pose a threat to the free flow of information across borders on the internet as well as the maintenance of global supply chains, in a world increasingly relying on e-commerce.

Fit for purpose

The Cloud Law's purpose is to 'provide a legal framework that encourages Foreign Parties use of an investment in Cloud Computing Services within Data Centres.' (see Article 2).

In July 2019, Amazon Web Services ('AWS') opened three data centres in Bahrain: the company's first in the region, bringing its global network to 69 centres in 22 locations.

This is indicative of the growing success of Bahrain's innovative strategies to encourage cloud computing services.

For further information, please contact Andrew Fawcett (a.fawcett@tamimi.com).