Catching the wave: New Data Protection Law in Bahrain

by Nick O'Connell - n.oconnell@tamimi.com - Riyadh
Zahir Qayum - z.qayum@tamimi.com - Manama

June – July 2018

Bahrain's Law on the Protection of Personal Data was published on 19 July 2018, and will come into effect on 1 August 2019. The Law will require a variety of changes to the way businesses process personal data in Bahrain or about residents of Bahrain. Data protection has not been a high priority topic for most businesses in Bahrain, with the limited exception of international entities subject to data protection requirements in other jurisdictions in which they operate. While the publication of the new Law provides a considerable lead-in period within which entities subject to the Law will need to comply, the fact that the Law creates criminal offences means that compliance is all the more important and should be treated as a high priority.

Until now, and with one exception (namely, Qatar), none of the Gulf Cooperation Council member states had a modern, nationally applicable data protection law. Legal issues relating to privacy and data protection are typically analysed in terms of general, and ill-fitting, criminal provisions relating to the unauthorized disclosure of secrets, or – in appropriate circumstances – industry-specific obligations relating to healthcare or credit data, or telecommunications sector subscriber data.

The Law is generally composed of 60 articles divided into three broad sections or 'titles'. These are:

- Title 1: Processing Provisions – Including definitions and general rules for the legality of processing, controls of data processing and transfer, statements as well as the rights of the data holder.
- Title 2: Data Protection Authority – Including provisions relating to the establishment of the regulator, and its rights and responsibilities.
- Title 3: Accountability of the data manager (data controller) and data processor – Including provisions relating to accountability to the regulator, investigation procedures, civil and criminal liability, and penalties for violation.

In this article, we consider some key areas addressed in the Data Protection Law.

Application

Bahrain's Data Protection Law describes the legal protection of personal privacy as among the main constitutional rights of the person, and notes that it should be protected, particularly in the context of the increasing use of electronic/digital means for processing information.

The Law applies to:

- Every individual residing normally in Bahrain or having a workplace in Bahrain, and every legal person (corporate) having a place of business in the Kingdom of Bahrain; and
- Every individual not residing normally in Bahrain or having a workplace in Bahrain, and every legal person (corporate) not having a place of business in the Kingdom of Bahrain, where such persons are processing data using means available in Bahrain, except where such processing means are solely for the purpose of passing data through Bahrain.

In this latter scenario, the legal person (corporate) is required to appoint an authorized representative in Bahrain, and notify the Authority of such appointment. This provision would appear to affect, for example, corporate customers of cloud service providers, where the customer is based outside Bahrain, and the services being provided to the customer are being provided from data centres located in Bahrain.

Criminal provisions

The Law criminalizes a variety of acts that would, at most, be the subject of administrative penalties in data protection laws elsewhere. Penalties generally comprise up to one year in prison and/or a fine of between BHD1,000 and BHD20,000 (between about USD 2,600 to about USD 53,000) (or a fine only in the case of corporate entities). The following are examples of activities that attract criminal penalties under the Law:

- processing sensitive personal data in violation of the provision specifying requirements for processing sensitive personal data;
- transferring personal data outside Bahrain contrary to the provisions specifying requirements for transfers to jurisdictions that provide an adequate level of data protection, and associated exceptions;
- processing personal data without notifying the Authority in accordance with the provision that sets out the obligation to notify the Authority before commencing any data processing activities (except where certain exceptions apply), or failing to update such notification to the Authority;
- Processing personal data contrary to the provision that requires prior authorization from the Authority before processing personal data in certain circumstances;
- Providing false or misleading information to the Authority or to a data subject, or withholding relevant information from the Authority, or otherwise hindering the Authority's work; and
- Disclosing any data or information accessed due to work, or using the same for own benefit or for the benefit of others unreasonably and in violation of the provisions of this law.

Security considerations

Generally, the security of processing provisions, and the confidentiality provisions, appear to be fairly standard.

Data controllers are required to apply technical and organizational measures capable of protecting personal data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing. The measures adopted need to be appropriate, bearing in mind the nature of the data in question and the risks associated with processing it. The Law also indicates that 'state-of-the-art' technological protection measures should be adopted, but this is tempered by reference to the costs arising from use of such technology.

Additionally, the Law contemplates the issuance of a regulation specifying requirements that technical and organisational measures must satisfy. It also provides scope for specific requirements to be prescribed in such regulations.

Data controllers are required to maintain documentation that reflects the technical and organizational measures adopted. This documentation must be available for viewing by the parties concerned (presumably, including data subjects), as well as the Authority, any data processors, and the data controller itself.

With regard to processing by data processors, the Law requires data controllers to engage only data processors who provide sufficient guarantees regarding the application of technical and organisational measures. Importantly, there is an obligation on data controllers to take steps to verify compliance with such measures, and to enter into a written contract with the data processor

requiring that the data processor shall only process data in accordance with the instructions of the data controller, and in accordance with the data controller's requirements with regard to security and confidentiality.

There does not appear to be any specific obligation to notify the Authority in the event of a data breach incident. It is possible that this level of detail might be addressed in the regulations, or that the Authority is expected to address breaches only in the event that they become aware of them, and the circumstances indicate a breach of the obligation to use suitable technical and organizational security measures.

Data protection supervisor

The Law contemplates a role of 'Data Protection Supervisor' (which is not a data protection officer) intended to act as an independent and impartial intermediary between the data controller and the Authority.

The data protection supervisor will help the data controller fulfil its rights and obligations, and coordinate between the data controller and the Authority. It will also be required to verify the data controller's processing in compliance with the law, alert the data controller to any apparent non-compliance to enable the issue to be addressed, and alert the Authority where such non-compliance has not been addressed within a specified timeframe. The data protection supervisor will also be required to maintain a register of the data controller's processing operations that the data controller must notify the Authority, and update the Authority of the same on a monthly basis. (If no data protection supervisor is appointed, then the data controller is required to do this itself.)

The qualifications and requirements for registration as a data protection supervisor will be officially issued, and data protection supervisors will need to be registered on a register maintained by the Authority. The requirement to appoint a data protection supervisor is optional, although it may be made compulsory for specific categories of data controllers.

The concept of a data protection supervisor has the potential to result in a whole new industry in the Bahrain market. The regulations setting out the requirements for the registration of data protection supervisors may shed greater light on what is anticipated, in terms of who might be able to fulfil such roles. The most natural development may be for the role to be filled by consulting/audit firms with expertise in data protection related issues.

Conclusion

Bahrain's new Data Protection Law will require a great deal of attention from businesses operating in Bahrain. Data protection has not been a high priority topic for most businesses in Bahrain, with the limited exception of international entities subject to data protection requirements in other jurisdictions in which they operate. While the publication of the new Law will result in some degree of a lead-in period within which entities subject to the Law will need to comply, the fact that the Law creates criminal offences means that compliance is all the more important and should be treated as a high priority.