New Data Protection Regime in Bahrain

Lara Haidar, Senior Associate, 
And Mark Hill, Partner
Bahrain is a jurisdiction that is putting particular effort into updating various of its laws of relevance to the business community and including in relation to its ongoing efforts to promote the digital economy for businesses operating and based in Bahrain. The next step on this journey comes into effect on 1 August 2019 with Bahrain's new personal data protection law, Law 30 of 2018 (the “Law”).

In essence, the new Law adopts a position, as is often the case with Bahrain's new wave of related legislation, which sits alongside broad international practices. It continues Bahrain's attempts to create a business environment which is attractive to the business community within Bahrain and also to investors coming into the region. The Law sets out to provide a clear framework for the processing of personal data. For sure, the new Law will require quite a number of changes in the way that businesses process personal data in Bahrain and all businesses should be giving attention to this new development.
1 What are the main requirements set out in the Data Protection Law?

The broad range of obligations placed on organizations and data controllers will be pretty familiar to any organization that operates under data protection laws in other parts of the world. The Law imposes new requirements on how businesses manage their data, including requirements to process data fairly and lawfully, collect personal data for legitimate, specific and clear purposes and to ensure that data is adequate, relevant and not excessive in relation to the purpose for which it was collected.

Obligations broadly fall into categories relating to: processing provisions (general rules and definitions relating to processing, data processing and transfer controls together with an overview of the rights of data holders); provisions relating to the establishment of the regulator, the Data Protection Authority, and an overview of its rights and responsibilities; and the implications of falling foul of the new requirements including accountability to the regulator, investigation procedures, civil and criminal liability and of course penalties for any violations.

2 Who does the new Data Protection Law affect?

The Law is stated to apply to individual residents or workers in Bahrain, to locally established businesses and also to any businesses outside of Bahrain that process personal data “by means available within the Kingdom” other than for purely transitory purposes. The net therefore is very broad. It does for example mean that even non-Bahraini businesses operating data centres or using third party data processors in Bahrain will be subject to the provisions of the new Law. Even those non-resident businesses (or individuals) must have an appointed authorized representative in the Kingdom to comply with the obligations under the new Law.

Pretty much the only thing that the new Law does not apply to is the processing of personal data within the context of personal or family affairs or the processing of personal data that relates to national security undertaken by the security authorities in the Kingdom.

3 What data is covered by the new Data Protection Law?

Personal data is defined under the new Law as any information in any form relating to an identified or identifiable individual, whether directly or indirectly, and this includes through personal identification number or one or more physical, physiological, intellectual, cultural or economic characteristics or social identity. Again a broad list. In essence, data subjects will have rights of access to personal data and to information concerning the processing of their personal data, as well as the right to object to processing for direct marketing or automated decision making purposes. This is broadly consistent with other international standards including in Europe although the express reference to identification of an individual by their personal ID card brings an added element alongside the other factors I have listed.
4 Collection and processing of data

Again, there are no great surprises when looking at the way the Law deals with collection and processing issues. Processing is defined as any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organizing, classifying in groups, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making them available to others, integrating, blocking, deleting or destroying them.

Consent is a key element. In particular, processing personal data can only occur with the consent of the data subject unless it falls within a number of exemptions set out in the Law, namely:

- To implement a contract to which the data subject is a party;
- To take steps at the request of the data subject to conclude a contract;
- To implement an obligation required by law, contrary to a contractual obligation or an order from a competent court;
- To protect the vital interests of the data subject; or
- To exercise the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject.

5 Transfer of data

Key provisions of the new Law relate to controlling (and prohibiting) the transfer of personal data out of Bahrain unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries will be listed by the regulator from time to time.

One key aspect for most organisations are the circumstances in which data can be transferred to countries that are not determined to have sufficient protection in place for personal data. These exemptions are where:

- The data subject has consented to the transfer;
- The data is from a public register;
- The transfer is necessary for the execution of a contract between the data subject and the data controller in order to follow through with the data subject’s request in order to conclude such a contract;
- It is required to execute or conclude a contract between the data controller and a third party for the benefit of the data subject;
- The transfer is in order to protect the data subject’s vital interests;
- It is required to fulfill a non-contractual obligation imposed by law, an order of the court, or an investigating judge, public prosecution or military prosecution; or
- It is in relation to preparing, executing or defending a legal claim.
6 Added security requirements

The new Law also requires data controllers to apply technical and organizational measures capable of protecting the data against an intentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access or any other form of processing. It is also key that data controllers use data processors who are able to provide sufficient guarantees about applying those same technical and organizational measures. It is the data controller’s obligation to take steps to verify that data processors are able to and do in fact comply with required measures.

7 Penalties and enforcement

As is to be expected, there are several criminal and administrative fines which may be imposed under the new Law. Criminal offences (including relating to the processing of sensitive personal data or the transfer of personal data outside the Kingdom in violation of the Law or failure to comply with any notification requirements in the Law) can attract fines of up to BD 20,000 (USD 53,200) or imprisonment for up to 1 year.

Administrative fines for other offences may be imposed on a scale up to BD 20,000 (USD 53,200) for one-off fines or daily penalties of up to BD 1,000 (USD 2,650). These may also be increased for repeat offences.

There are various other sanctions available to the regulator including the publication of negative publicity statements concerning established violations and the opportunity for individuals to claim compensation for damage suffered due to any processing of their personal data by a data controller in breach of the Law.

8 What should you do now?

The new Law fundamentally changes the way that businesses are able to operate in Bahrain in relation to the way that they process personal data. It is also key to understand that this is a business process issue not just a matter of applying a privacy policy in terms and conditions or on a website. The documentation, IT systems, business processes and data flow, personnel awareness and training are all key parts of compliance. In order to meet regulatory obligations, organisations cannot treat the new Law as a one-off compliance activity.
9 A checklist for data protection in Bahrain

- Does your organization have a clear view about what personal data and sensitive personal data is being processed by the organization and including in relation to the data of your customers and your staff?

- Has data protection responsibility been clearly set out for your organization? Do you know who is responsible for what within the organization?

- Has an internal data protection policy been created for your organization and is it accessible for people within the organization?

- Has an assessment been undertaken of the organisation’s data flows, categories and types of data processed? Has an audit and, if required, a gap analysis been undertaken relating to current organizational compliance and awareness? This is fundamental.

- Are procedures in place relating to retention periods for personal data?

- How does your organization address privacy issues in a contractual and operational context when outsourcing IT services to any third party?

- What assessment has been undertaken to ensure that adequate measures are in place to protect personal data in your organization?

- Are you able to deal with customer or employee requests relating to their own data and including relating to access, correction, alteration or deletion of personal data?

- Have appropriate consent procedures been put in place including in relation to any third party (including customers) whose data you are collecting, processing and storing but also in relation to your employees?

- Are staff trained on data protection and do they understand the practical implications of implementing the organisation’s data protection policy on a day to day basis?
Contacts

Lara Haidar
Senior Associate
Lara.Haidar@crsblaw.com
+971 4 246 1920

Mark Hill
Partner
Mark.Hill@crsblaw.com
+971 4 246 1921