Bahrain issues new privacy guidelines supplementing the Personal Data Protection Law

The Middle East has seen a rapid rise in data protection legislation with the UAE, Saudi Arabia and Oman recently issuing standalone data protection laws. In the latest regional development, the Kingdom of Bahrain has issued new guidelines addressing aspects of its Personal Data Protection Law. This article summarises the key requirements of the guidelines and identifies additional obligations that companies operating in Bahrain will need to consider.

The Kingdom of Bahrain was the second country in the GCC to issue national privacy legislation with the Personal Data Protection Law No. 30 of 2018 (the PDPL), which came into force on 1 August 2019.

On 17 March 2022, the Kingdom's Minister of Justice, Islamic Affairs and Waqf issued six ministerial resolutions (the Resolutions) supplementing the PDPL and bringing the PDPL more into line with international standards such as the European General Data Protection Law (GDPR). The Resolutions focus on the following areas:

- transfers of personal data outside Bahrain;
- technical and organisational measures to protect personal data;
- notification procedures;
- sensitive personal data processing;
- data protection guardians (i.e. DPOs);
- fees for DPO registration;
- data subject rights; and
- complaints by individuals;
- data relating to criminal claims; and
- conditions for publicly available registers.

The PDPL applies to individual residents or workers in Bahrain, locally established businesses and any businesses outside Bahrain that process personal data "by means available in the Kingdom" other than for purely transitory purposes. This means that non-Bahraini businesses operating data centres or using third party data processors in Bahrain will be caught under the PDPL.

For a summary of the PDPL please see “Five questions you should ask about Bahrain’s new data protection law” and our related infographic.

Transfers of personal data outside Bahrain
Resolution No. 42 of 2022 on the transfer of personal data outside the Kingdom establishes a list of countries that have been deemed by the Personal Data Protection Authority (PDPA) to provide an adequate level of data protection (the Adequacy List). The Adequacy List is much more extensive than the equivalent list issued by the European Commission: it includes 83 countries, including the UAE, Saudi Arabia, Oman, Jordan, Kuwait, Egypt, India, all EU countries, UK, and USA. Controllers may transfer personal data to any country on the Adequacy List without needing to obtain any authorisation from the PDPA.

Transfers to countries not on the Adequacy List require authorisation from the PDPA, which is determined on a case-by-case basis, unless an exclusion applies.

Where transfers are made to third parties in a country not on the Adequacy List and pursuant to a contract, Resolution No. 42 requires controllers to obtain authorisation from the PDPA and to provide a copy of the agreement.

Where data is transferred within a "Regional or International Group" (i.e. intra-group transfers) to a country not on the Adequacy List, controllers must obtain authorisation from the PDPA and comply with "Corporate Rules"; these are a set of binding policies and procedures regulating intra-group transfers which are submitted to the PDPA for approval – similar to Binding Corporate Rules under the GDPR.

Technical and organisational measures

Resolution No. 43 of 2022 sets out the technical and organisational measures that controllers should implement to protect personal data. It introduces certain new concepts and obligations that mirror the GDPR, including privacy by design and the obligation to conduct data protection impact assessments in certain cases.

There is also a new breach notification requirement with controllers obliged to notify the PDPA not later than 72 hours after having become aware of a data breach, unless the breach is unlikely to result in a risk to the rights of data subjects. Controllers must also communicate data breaches to data subjects in certain circumstances.

Employees should be updated and trained on the measures taken by the controller in line with Resolution No. 43.

Notification procedures

Resolution No. 44 of 2022 sets out the rules and procedures for submitting notifications to the PDPA in accordance with Article 14 of the PDPL (unless an exemption applies) and requesting prior authorisation in accordance with Article 15 for certain types of processing.

It also sets out obligations for data processors, including notifying the data subject of the method of data processing and enabling data subjects to have access to their processed data.

Employees should be updated and trained on the measures taken by the controller in line with Resolution No. 43.

Sensitive personal data processing

Resolution No. 45 of 2022 sets out the rules and procedures for processing sensitive personal data. The definition of "sensitive personal data" in the PDPL is similar to the GDPR’s special categories of personal data, excluding genetic and biometric data.

Resolution No. 45 reiterates that sensitive personal data should not be processed without the consent of the data subject, unless one of the cases in Article 5 of the PDPL applies. These cases mirror the additional legal bases required for the processing of special category data under the GDPR including where: (i) the processing is
required to comply with obligations and rights in the field of employment; (ii) the data is required to exercise or defend legal claims; and (iii) the processing is required to protect a person, where that person is legally unable to provide consent.

Controllers will also have to implement additional organisational rules when processing sensitive personal data including appropriate high-level technical measures to ensure a high degree of protection against secrecy, breach or unlawful processing of such data.

Data Protection Guardians (or DPOs)

Resolution No. 46 of 2022 on Data Protection Guardians (known internationally as DPOs) states that controllers may appoint a qualified external or internal DPO. However, it does not specify the circumstances where appointing a DPO is mandatory: this will be determined by way of a separate resolution.

If a controller appoints a DPO it must notify the PDPA within three working days of such appointment. DPOs shall be listed on a register available on the PDPA's website (the Register), consisting of a list of external DPOs and a list of internal DPOs.

DPOs will need to make a declaration stating whether anything could cause a conflict of interest to their duties or could affect their independence or impartiality.

Fees for DPO registration

Resolution No. 47 of 2022 sets out a table of fees for registering DPOs, including renewal fees. Fees for registration can go up to BD 500 (US$1,326) for legal entities as external DPOs and BD 100 (US$265) for internal DPOs.

Data subject rights

Resolution No. 48 of 2022 on the rights of personal data subjects clarifies what controllers must do if they carry out automated processing, such as establishing clear rules that set out procedures to enable the data subject to submit an objection to such processing, explaining the purpose of the processing as well as how decisions are made and informing the data subject of the outcome of the decision.

Resolution No. 48 also clarifies that where consent is relied upon to process personal data obtained directly from the data subject, such consent must be express and obtained in writing or by electronic means. Data subjects have the right to withdraw consent at any time and such withdrawal should be made through easy procedures after verifying the identity of the data subject.

In relation to websites, consent granted by a data subject shall be considered void if the cookie banners oblige the data subject to provide consent before browsing the website.

Individual complaints

Resolution No. 49 of 2022 specifies the rules and procedures for filing complaints against entities that breach the PDPL. Any person who has interest or capacity has the right to file a complaint with the PDPA if they believe that there has been a breach of the PDPL or that someone is processing personal data in violation of the PDPL.

Once the PDPA has examined and accepted the complaint, it will provide a notification to the relevant controller, who will have a short period of time to respond with its defence: seven working days from the date of the notification. The PDPA may not provide a notification if there is serious evidence of violation of the PDPL and a notification would hinder the investigation.
Data relating to criminal claims

Personal data relating to the initiation and pursuing of criminal claims and judgments cannot be processed unless by the persons specified in Article 7 of the PDPL, including specialised public bodies required to perform legal duties and to the extent required to pursue any litigation procedures filed against an entity.

Resolution No. 50 of 2022 sets out the controls for processing personal data relating to criminal claims by authorised persons. It requires such authorised persons, for example, to prohibit the disclosure, transfer and publishing of criminal claims data to persons who are not authorised to access such data and to use technical systems and modern electronic applications that ensure an adequate level of protection and privacy during the processing of such data.

Conditions for creating publicly accessible registers

The PDPL and Resolution No. 51 of 2022 set out conditions for creating a publicly available register of personal data. Data controllers that create such registers must meet certain requirements such as:

- notifying the data subject of the inclusion of his or her data in the register and obtaining the data subject's approval (unless the data was obtained from public sources, in which case only notification is required);
- enabling the data subject to amend or write off his or her personal data contained in the register under clear and simple procedures; and
- including specific information in the register, such as type and purpose of data.

What are the penalties for non-compliance?

A range of criminal and administrative fines may be imposed under the PDPL.

Processing sensitive personal data or transferring personal data outside the Kingdom in violation of the PDPL or failure to notify as required by the PDPL could lead to fines of up to BD 20,000 (US$ 53,200) or imprisonment for up to one year.

Other violations may lead to administrative fines ranging from BD 20,000 (US$ 53,200) for one-off fines or daily penalties of up to BD 1,000 (US$2,650), which may be increased for repeat offences.

Other sanctions available to the PDPA include publishing statements concerning established violations and referring potential crimes to the Public Prosecutor. Additionally, individuals may claim compensation for damage suffered due to any processing of their personal data by a controller in breach of the PDPL.

What should companies do next?

The PDPL has been in force since 1 August 2019 and companies operating in Bahrain are expected to be compliant with the PDPL.

The Resolutions all came into force from the day following the date of their publication in the Official Gazette, i.e. 18 March 2022. Companies therefore need to review the Resolutions and ensure their data processing practices and procedures are swiftly brought in line with the requirements set out in the Resolutions. This includes new requirements not previously stated in the PDPL, such as the obligation to notify data breaches to the PDPA – controllers will need to ensure that they implement appropriate data breach response procedures to comply.
Controllers will also be required to hold training for employees on the technical and organisational measures and, where applicable, specific training for DPOs.

Following the publication of the Resolutions, we expect that the PDPA will start to play a more active role in enforcing the PDPL in Bahrain. All organisations operating in the Kingdom will need to ensure that a culture of data protection is suitably embedded into the organisation and that appropriate procedures and policies are implemented in line with the PDPL and the Resolutions.

We have previously issued tips for enterprises on how to create an effective privacy framework and worked with many companies to help them implement the required processes and policies for compliance.