DECODING:
BAHRAIN PRIVACY LAWS

An Exclusive Cheat-Sheet
Curated By:
tsaaro. consulting

DEFINITIONS

Data or Personal Data:
Any information, in any form, that can identify an individual directly or indirectly, especially through their ID number or personal characteristics such as physical, intellectual, cultural, or economic traits.

Sensitive Personal Data:
Any personal information revealing –directly or indirectly–about an individual's race, ethnical origin, political or philosophical opinions, religious beliefs, affiliation to union, personal criminal record, or any information in relation to his health or sexual status.

Data Controller:
A person who, either alone or jointly with other persons, determines the purposes and means of processing any particular personal data, unless specified by law.

Data Processor:
A person, other than an employee of the data controller or data processor, who processes personal data for the Data Controller's benefit and on the Data Controller's behalf.

Data Subject:
The person or individual subject of data.

Processing:
Any operation or set of operations which is performed upon personal data, whether or not by automatic means, including collecting, recording, organizing, classifying into groups, storing, adapting, altering, retrieving, using, disclosing by transmission, dissemination, transference or otherwise making available for others, or combining, blocking, erasing or destructing such data

SCOPE AND APPLICATION (ARTICLE 2)

This Law applies to any data processing, whether by automatic or non-automatic means, if the data is part of or intended for a filing system. It applies to:

- Natural persons habitually resident or with a place of business in the Kingdom.
- Legal persons with a place of business in the Kingdom.
- Persons outside the Kingdom who process data using means located within the Kingdom, except for data in transit.

The Law does not apply to data processing for personal or family affairs or to public security operations by specific national security bodies. Additionally, it does not affect confidentiality duties related to Bahrain Defense Force matters.

PRINCIPLES (ARTICLE 3)

- Lawfulness and Fairness
- Purpose Limitation
- Accuracy
- Data Minimization
- Data Anonymization

OBLIGATION OF DATA CONTROLLER

Article 8 of PDPL
Implement and document technical and organizational measures to ensure data security, select compliant Data Processors, and ensure processing follows strict contractual obligations.

Article 15 of PDPL
Ensure prior written authorization from the Authority for processing sensitive personal data, biometric data, genetic data, linked data from multiple controllers, or surveillance data.

Article 3 & 4 of order 48
Inform Data Subjects of automated processing decisions, provide a clear objection process, and obtain consent before processing data directly obtained from them.

Article 2 of Order No. 43
Implement Privacy by Design, privacy frameworks, breach mitigation, periodic VAPT, incident response plans, and competency-based task assignments.

Article 3 of Order No. 43
Conduct DPIAs for high-risk activities, covering processing details, risk analysis, and mitigation, with input from the Data Protection Guardian and data subjects.

Article 4 of Order No. 43
Establish breach reporting, document incidents, notify within 72 hours, or use public communication with breach details and mitigation steps.

Article 5 of Order No. 43
Set written guidelines for internal breach investigations, covering report handling, evidence preservation, and submission of findings to relevant authorities.

Article 6 of Order No. 43
Adhere to the provisions regarding cross border data transfer outlined in Order No. 42 of 2022 when contracting external processors or third parties

Article 7 of Order No. 43
Create a written agreement defining roles in joint data processing, disclose it to data subjects, and establish a contact point for them.

Article 8 of Order No. 43
Provide ongoing training to employees on data protection laws, protocols, and procedures to ensure compliance.

ENFORCEMENT AND PENALTIES

- Violations of data protection law can lead to up to one year in prison and fines up to **BD 20,000** for unlawful processing, improper data transfer, and other breaches. (**ARTICLE 58 of PDPL**)
- The Board can order the violator to stop and remedy the issue. Failure to comply allows the Board to withdraw authorization, impose daily fines up to **BD 1,000** for first-time and **BD 2,000** for repeat violations, or impose an administrative penalty up to **BD 20,000.** (**Article 55 of PDPL**)
- A party who suffers damage from personal data processing by the data controller or violations by the data protection guardian can claim compensation from the party responsible. (**ARTICLE 57 of PDPL**)
- A legal person may face fines up to **BD 40,000** if crimes are committed in its name, on its behalf, or for its benefit, due to actions, omissions, approval, cover-up, or gross negligence by its Board members, officials, or representatives, without prejudice to the criminal liability of individuals. (**Article 59 of PDPL**)

DATA SUBJECT RIGHTS

- Right to be informed (**Article 17**)
- Right to be notified when processing of personal data (**Article 18**)
- Right to object to direct marketing (**Article 20**)
- Right to object to processing causing material or moral damage to the Data Subject or Others (**Article 21**)
- Right to object to decisions made based upon automated processing (**Article 22**)
- Right to request rectify, block and erasure of data (**Article 23**)
- Right to consent withdrawal (**Article 24**)
- Right to lodge complaints (**Article 25**)

CROSS-BORDER TRANSFER

Article 12 of PDPL & Article 2 of Order no. 42:
The Data Controller may transfer personal data outside the Kingdom only if the transfer is to a country listed by the Authority as providing adequate protection, or if the transfer is authorized by the Authority on a case-by-case basis, which may be conditional or for a specific period.

Article 4 of Order no. 42:
To transfer personal data outside the Kingdom to a non-listed country or within a regional or international group, the Controller must obtain prior authorization from the Authority and comply with corporate rules.

Article 13 of PDPL:
The Data Controller may transfer personal data to a country with inadequate protection if:
1.The data subject consents to the transfer.
2.The data is from a public register, accessible according to legal conditions.
3. The transfer is necessary for:

- Fulfilling or entering into a contract with the data subject.
- *Concluding or fulfilling a contract in the data subject's interest with a third party.*
- *Protecting the data subject's vital interests.*
- *Complying with legal obligations or court orders.*
- *Preparing or pursuing a legal claim or defense.*

Article 5 of Order no. 42:
To transfer personal data to data controller or third party outside listed countries, prior authorization and a contract are required. The contract must limit processing to specified purposes, ensure data accuracy, retain data only as needed, implement security measures, inform the Data Subject, and guarantee their rights to access, rectify, or erase data if non-compliant.

OBLIGATION OF DATA PROCESSOR

Article 8(3) of PDPL:

- Implement technical and organizational measures, verified by the Data Controller to protect the data during processing.
- Process data strictly according to the instructions provided by the Data Controller.
- Implement security and confidentiality standards equivalent to those imposed on the Data Controller.