KPMG

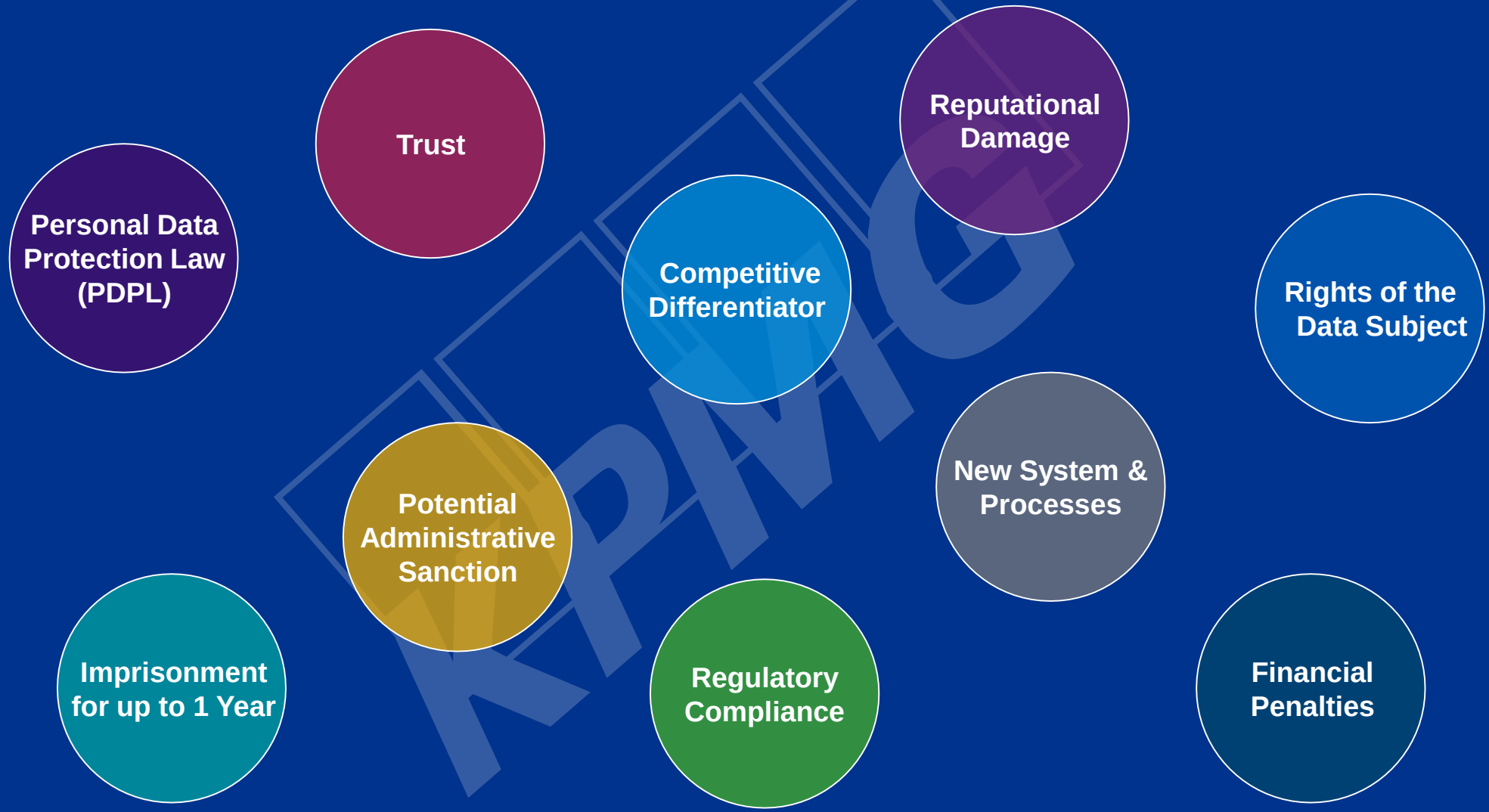
The National Audit Office

Personal Data Protection Classroom Training

6 February 2020

Contents

Why is privacy important



Bahrain Personal Data Protection Law (PDPL)

01 August 2019

Bahrain Personal Data Protection Law came into force – defining stringent requirements on collection, processing, storing and disposing of personal data.

His Majesty King Hamad Bin Isa Al Khalifa issued Decree No.78 for the year 2019 on 30 September 2019 confirming the Ministry of Justice, Islamic Affairs and Waqf as the official Independent Authority with the full powers and functions promulgated by Law No.30 including monitoring and enacting compliance within the marketplace.

Key definitions and roles

Person

Any natural or legal person including any public entity.
(PDPL definition of person has been extended to legal person also)

Legal Person

Legal person may be a private or public organization

Personal Data

Information in any form (1) related to an identifiable individual, or (2) can identify an individual directly or indirectly

Sensitive Personal Data

Information that is of a special category and for which law mandates specific protection

Data Controller

Person who decides, solely or in association with others, the purposes and means of processing

Data Processor

Person who processes data for and on behalf of the Data Controller

Data Subject

Individual whose personal data is being processed

Data Recipient

Any Person to whom personal data is disclosed

Processing *means any operation or set of operations 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.*

Data processing Principles

Lawfulness, fairness and transparency

Processing is based on legitimate grounds and expectations.

Purpose Limitation

Data must only be collected for specified, explicit and legitimate purposes.

Data Minimization

Collected data must be adequate, relevant and limited to what is necessary for the purpose.

Accuracy

Collected data must be accurate, and kept up to date.

Storage Limitation

Data must be retained only as long as necessary.

Integrity and Confidentiality

Data must be processed securely.

Accountability

All employees and processors must demonstrate compliance to these principles.

Data controller/ protection officer – Key obligations

Data Controller shall implement appropriate technical and organizational measures

Data Controller shall choose Data Processor who provides sufficient safeguards and ensure appropriate compliance

Data Controller shall give prior notice to Authority of any wholly or partially automated processing operation

Data Controller shall inform Data Subjects about rights of Data Subject

Data Controller shall ensure that the processing is only carried out pursuant to a written contract between the Data Processor and Data Controller

In case of breach, Data Controller to eliminate the cause of violation or undertake the necessary rectification

Data Controller must not process any Personal Data in breach of this Law

The Data Controller must not disclose any personal data and sensitive personal data without the data subject's consent or in execution of a judicial order issued by a competent court, Public Prosecution, investigation judge or Military Prosecution.

Joint controllers

Obligations of joint controllers

Regardless of any arrangements, EACH controller remains accountable for complying with all the obligations of the Data Controllers.

Transparent arrangement

Joint controllers are not required to have a contract, however MUST have a transparent arrangement that sets out agreed roles and responsibilities which should be made available to all individuals.

Individuals' rights

Must decide (and be transparent about) how the controllers will comply with transparency obligations and individuals' rights. Data subjects must be able to exercise their rights against each controller.

Example:

A luxury car company teams up with a designer fashion brand to host a co-branded promotional event. The companies decide to run a prize draw at the event. They invite attendees to participate in the prize draw by **providing their name and address** into their prize draw system at the event. After the event, the companies give out the prizes to the winners. They **do not use** the personal data for any other purposes.

In this case, the companies will be joint controllers of the personal data processed in connection with the prize draw, because they both decided the purposes and means of the processing.

Key Risks and Impact

Key risks and impact

The law impacts the way you:

Collect | Store | Use | Manage | Monitor | Protect

Impact the way you retain historical data

Dispose off any personal data

While meeting regulatory obligations is a must, this is not a one-off 'tick the box' compliance activity, but should be considered as a strategic business imperative that impacts the way your organization transitions towards a more privacy conscious culture – where:

Transparency | **Citizens' Rights** | **Accountability**

Must become second nature to the way a business is run.

Applies to:

- Employees/ Prospective Employees
- Customers/ Prospective Customers
- Vendors
- Contractors/ Suppliers
- Professional Service Providers
- Shareholders
- Third Party Service Providers
- Directors/ Approved Persons

Transfer of data outside of Bahrain

The data can be transferred out of Kingdom in the following cases

Transfer to countries/ jurisdiction not having adequate level of protection

- Data subject has provided the consent for the transfer
- When the transfer is for the purpose of providing information to the public
- The performance of a contract between the data subject and the Data Controller
- Protecting the vital interests of the data subject
- Preparing or pursuing a legal claim or defense

Transfer to countries/ jurisdiction having adequate level of protection

- The transfer is to a country on a list compiled and updated by the Authority
- Provides adequate laws and regulations according adequate level of protection to personal data.
- Case-by-case basis and depending upon following considerations:
  a) Nature of data to be transferred
  b) Originating country, final destination & measures to protect the personal data
  c) Relevant international agreements

Key requirements of the law

Protect personal information with appropriate safeguards.

Privacy breaches must be reported to the Authority and to the individuals affected without undue delay.

Ensure that personal information is used fairly and lawfully in accordance with the rights of individuals.

Organizations must designate a named Data Controller/ Data Privacy Officer (DC/ DPO) who will have the primary responsibility for communicating with the Authority.

Data collection must be for the specified purpose and proportional to its use.

Third Parties are also covered, meaning that the DC/ DPO must conduct due diligence on any third parties that are processing data on the organizations behalf.

Data inventory – What needs to be recorded

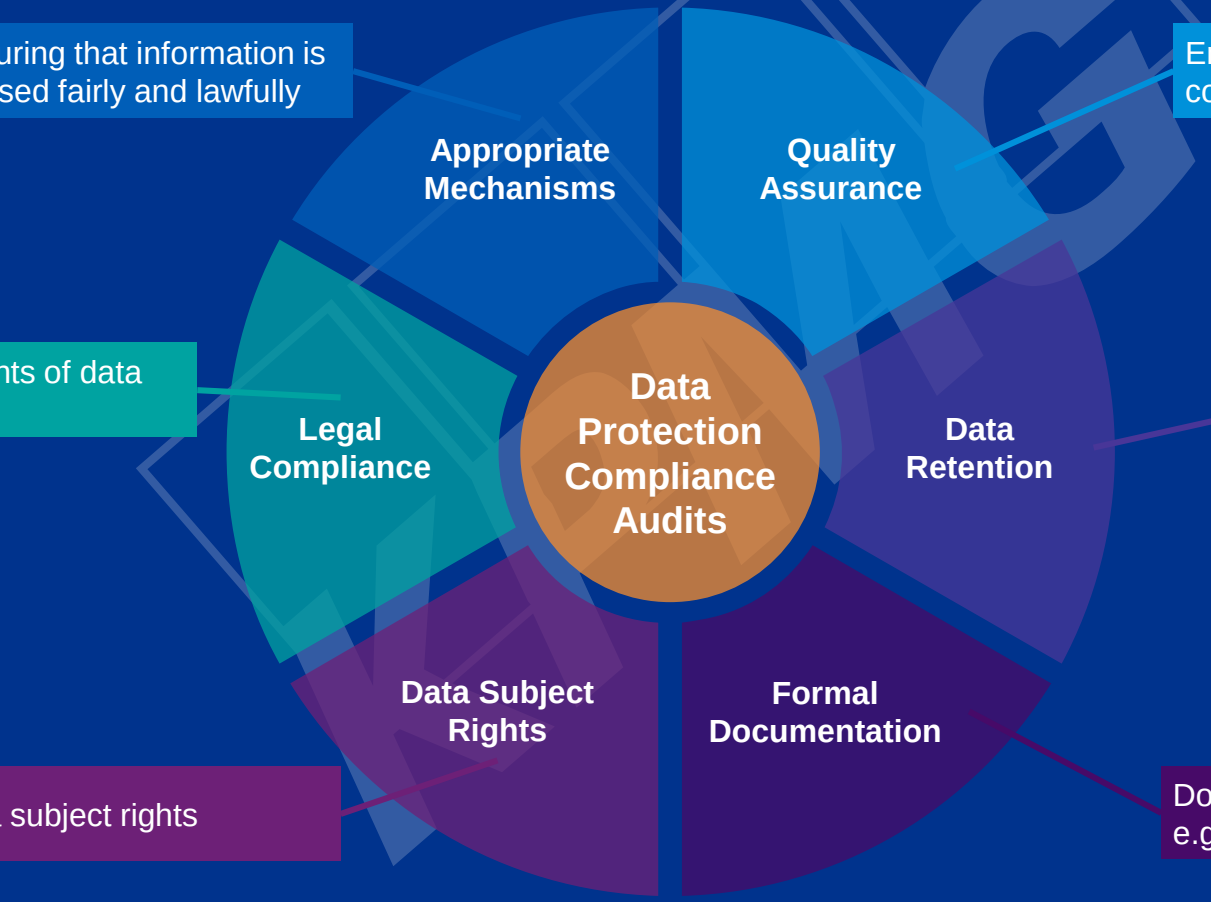
The Data inventory must include, but not be limited to:

- Name and contact details of the controller(s) / representative / processor / DC/ DPO
- Purpose and nature of the processing including the categories of data subject
- Brief description of technical and organizational security measures including systems used to store data
- Documentation including suitable safeguards of personal data transfers to third parties / overseas
- Appropriate retention and disposal measures taken by the organization

Role of an Auditor

Data protection compliance audits

Most organizations are familiar with existing audit methodologies, however the Data Protection Compliance Audits go beyond the basic requirements of Data Security and address wider aspects of data protection including:



Mechanisms for ensuring that information is obtained and processed fairly and lawfully

Ensuring that information is accurate, complete and up-to-date, adequate, relevant

Compliance with the requirements of data protection law

Retention – appropriate monitoring and disposal of information where applicable

Compliance with data subject rights

Documentation on authorized use of systems, e.g. codes of practice, guidelines etc.

Role of an auditor when conducting data protection audit

The key roles identified for an auditor when conducting a personal data protection audit includes, but not limited to:

- **Checking the current compliance status**
- **Assessing staff awareness of their data protection obligations**
- **Assessing whether the rights of Data Subjects are adequately protected**
- **Identifying non-compliances**
- **Agreeing suitable corrective action to remove non-compliances.**

Illustration – HR audit checklist

01

Is employee data/ hiring data anonymized?

02

Is there a secure tool to store employee contracts?

03

Does the employment contract include a section on training and data protection?

04

Can an employee's data be easily erased after they leave the organization?

05

Do the employees know how the organization use their personal data?

06

Are all systems used to store employee data compliant with the applicable laws (i.e. payroll, HRMS, scheduling systems, etc.)?

07

Does the organization have a legitimate reason for collecting the personal information?

08

Can the employees easily edit their data or exercise their rights as a data subject?

09

Does the job application process comply with the law (i.e. asks only for necessary data, specifies how long you will keep the data, etc.)?

Breach management – Best practice take-away

Record

Record the breaches in the **Internal Breach Register** including:

- What happened, causes, effects and consequences
- Data involved, individuals affected
- Decisions regarding the breach, notification, timelines
- Post event **report,** including Root Cause Analysis

Assess

Assess the **Risk** including:

- Assess level of risk posed to data subjects (adverse impact test)
- Sensitivity of personal data, type of data subjects (e.g. children)
- Volume of data and number of data subjects affected
- Any safeguards (e.g. encryption, anonymization) in place

Notify

Based on the **Assessment** a decision to **Notify** should be taken:

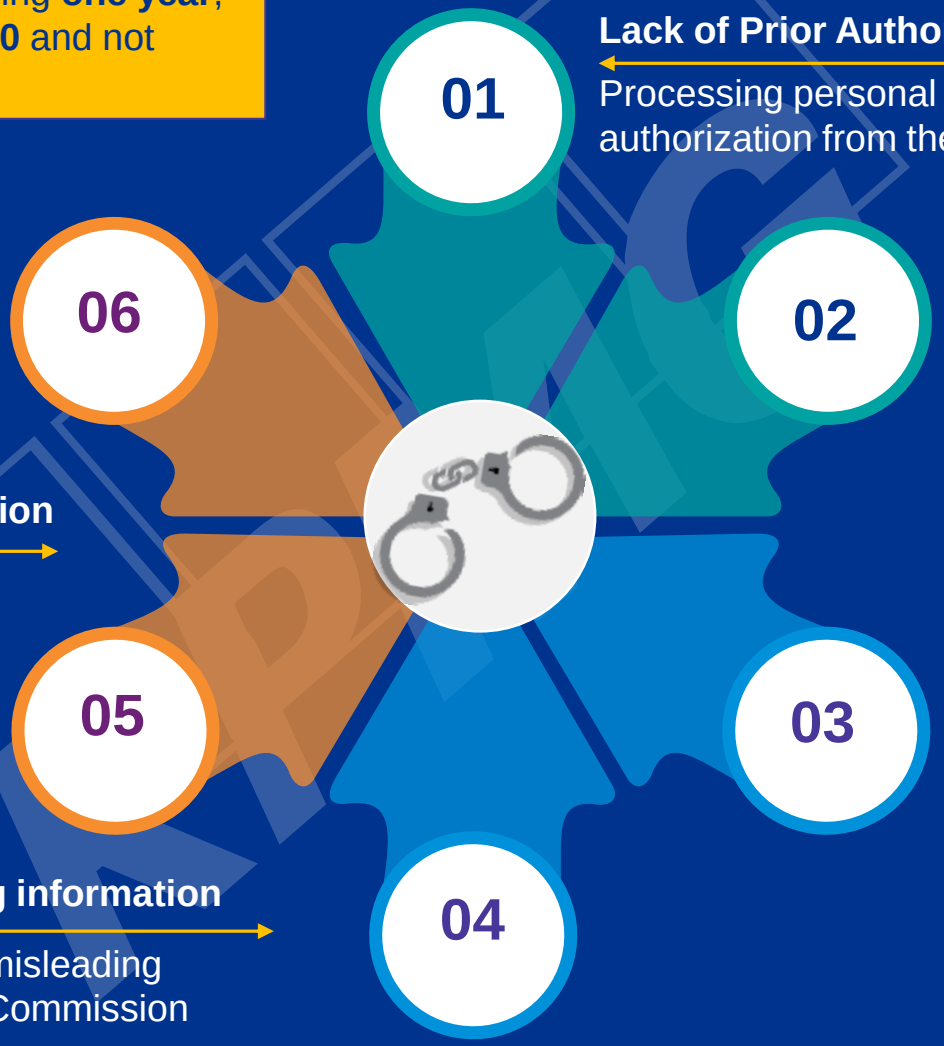
- **Unlikely** to result in a risk to the rights and freedoms of data subjects – **do not notify**
- **Likely** to result in a risk (High/Low) to the rights and freedoms of data subjects – **notify**

Example checklist (PDPL compliance)

- Personal data protection policies and procedures
- Data classification and access management
- Third party agreements
- Risk Management and periodic review/ monitoring on privacy controls
- Roles and responsibilities
- Incident and Breach Management
- Staff awareness and training
- Data Transfers
- Legal review of changes in regulatory and/or business requirements
- Data Minimization and accuracy of data
- Consent framework
- Data subject rights and requests
- Data retention, disposal, destruction and anonymisation
- Privacy architecture (Privacy by Design and Privacy by Default)
- Data Protection Impact Assessments (DPIAs)

What can attract penalties?

Imprisonment for a term not exceeding **one year**, and / or a fine not less than **BD 1000** and not exceeding **BD 20,000**



Lack of Prior Authorization

Processing personal data without prior authorization from the Commission

Transferring Data outside Bahrain

Transferring personal data outside Bahrain contrary to the provisions of the Law

Disclosing information

Disclosing any data or information accessed due to work, or using the same for own or others benefit unreasonably and in violation of the Law

False / misleading information

Providing false or misleading information to the Commission

Processing Data without notification

Processing personal data without notifying the Commission

Processing Sensitive Personal Data

Processing sensitive personal data contrary to the provisions of the Law

Thank You