Privacy and Data Protection Program

By: Leen Qassisiya
VP – Head of Privacy and Data Protection, Arab Bank

البنك العربي
ARAB BANK

Agenda

1 INTRODUCTION

2 INTENSIFIED MENA REGULATORY FOCUS

3 HOW IT ALL STARTED

3 BEST-PRACTICE ALIGNED PRIVACY AND DATA PROTECTION PROGRAM

4 Q&A

Introduction

Key Terms:

Personal Data - any information relating to an identified / identifiable individual, whether it relates to his or her private, professional, or public life. An individual can be identified either:

- Directly, if you are able to identify a specific individual solely through the data you're processing. Example: name, national ID number.
- Indirectly, if different sets of data from different sources, when combined, could identify a specific person. Example: gender, birth date, and license plate number.

Sensitive personal data - is generally data that directly or indirectly reveals a person's racial or ethnic origin, political opinions, religious or philosophical views, trade union membership, sexual orientation, health, genetic, or biometric data.
Some MENA countries expand definition – examples:
Definition under Jordan Personal Data Protection Law also includes "data that is indicative of financial status"
Definition under Qatar Personal Data Protection Law also includes "marital status data"

Data Subjects - is the individual (natural person) whose data can be processed. This includes customers, employees, ex-employees and customers, job applicants, business partners, shareholders, and Board members.

Processing - any operation performed on personal data whether or not by automated means, such as collection, recording, organization, structuring, storage, retrieval, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, and erasure.

Data Controller: determines the purpose of the processing. This means that they make decisions about what data is captured and why.

Data Processor: is a third party that processes personal data based on the Data Controller's instructions.

1 Introduction

- **Privacy & Data Protection:** Data privacy is about what personal data has been collected lawfully and what can be done with it and what controls are available over the retention and use of data. Data protection ensures that the data is safeguarded from unlawful access by unauthorized parties.
- **GDPR**, The General Data Protection Regulation, is a regulation in EU law on data protection and privacy in the European Union, and is considered the golden standard for privacy regulations.

The Key Principles

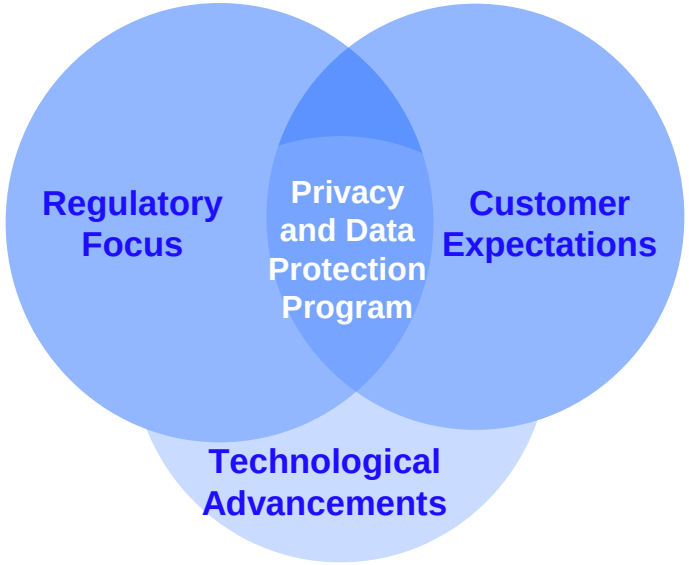
Legality	Demonstrate lawful reasoning for processing personal data • With Consent • Without consent based on: contractual obligation, legal obligation, vital interest, public interest, or overriding legitimate interest
Minimization	**Personal data must be relevant, adequate, and limited to what is necessary for the specified purpose**
Storage Limitation	**Personal data should not be kept for longer than what is necessary for the specified purpose**
Minimization	**Personal data must be relevant, adequate, and limited to what is necessary for the specified purpose**
Integrity and Confidentiality	**Personal data should be processed in a manner ensuring appropriate security measures are there to protect its integrity**
Accuracy	**Personal data should be up to date, and actions must be taken to ensure inaccurate data is erased**

Accountability for Principles

Introduction

The Key Drivers of Change – How it all Started

The EU's General Data Protection Regulation (GDPR) has become the gold standard with regulators worldwide issuing and revising their data protection legislation to embrace key principles thereunder



In the digital age, individuals and customer advocacy groups are more aware of and involved in data privacy issues. On the other hand, advanced technology tools, such as those related to advertisement personalization, present business opportunities yet pose significant privacy risks

Organizations are increasingly reliant on data in pursuing business objectives ranging from driving internal automation and digital transformation to providing innovative products and services . This brings to the fore, the need to ensure data processing is grounded on ethical principles!

EU **- General Data Protection Regulation (issued May 2016, effective May 2018)***

*Replaced the EU Data Protection Directive of 1995

2 Intensified MENA Regulatory Focus - 2025 Select Key regulatory developments

Key Development / Regulations 2025 YTD

Jordan

Central Bank of Jordan

1. Regulations on Personal Data Protection
2. Circular on the Accreditation and Registration of Data Protection Supervisors for Bank – DPOs
3. Circulars on the Registration Process of Data Protection Supervisors for Financial Leasing Companies and Insurance Companies

Personal Data Protection Authority *under Ministry of Digital Economy and Entrepreneurship*

1. Guidance on Completing Privacy Impact Assessments
2. Regulations on Personal Data Breach Management
3. Draft Regulations on Consent Managment and Data Subject Rights
4. Guidance on Privacy and Security by Design
5. Regulations on Technical and Organizational Security Measures
6. Regulations on Records of Processing Activities
7. Accreditation and Registration of Data Protection Officers (DPOs)
8. Personal Data Protection Law went into effect (issued September 2023 - went live March 2025).
9. Guidelines on Privacy Notice

Bahrain

New CBB Circular in Bahrain: 2025, requires banks to appoint and register a Personal Data Protection Guardian. The Guardian must hold a Bachelor's Degree in information technology, or a professional certificate in information security or have at least two years of practical experience and be a resident in Bahrain.

Algeria

Revised Law in Algeria- Issued July 2025, amends earlier Law of 2018 requires privacy impact assessment prior to launching new products and services impacting personal data processing; covered entities need to consult the Algeria Personal Data Protection Authority where the assessment results indicate potential high risk to individuals. Law also requires appointment of a Personal Data Protection Liaison responsible for overseeing compliance with the Law. Covered entities must notify the Authority of the appointed Liaison.

Palestine

Draft Personal Data Protection Law for Consultation - Issued January 2025, requires data owner consent or an authorization from the Authority prior to personal data sharing, as well as requires entities to submit annual reports to the Data Protection Authority concerning data protection risks, compliance levels, and personal data breaches. Law also imposes Data Controllers' Registration Requirements under a National Registry of Data Controllers and requires Controllers processing sensitive data (e.g. health data) to appoint a Data Protection Supervisor.

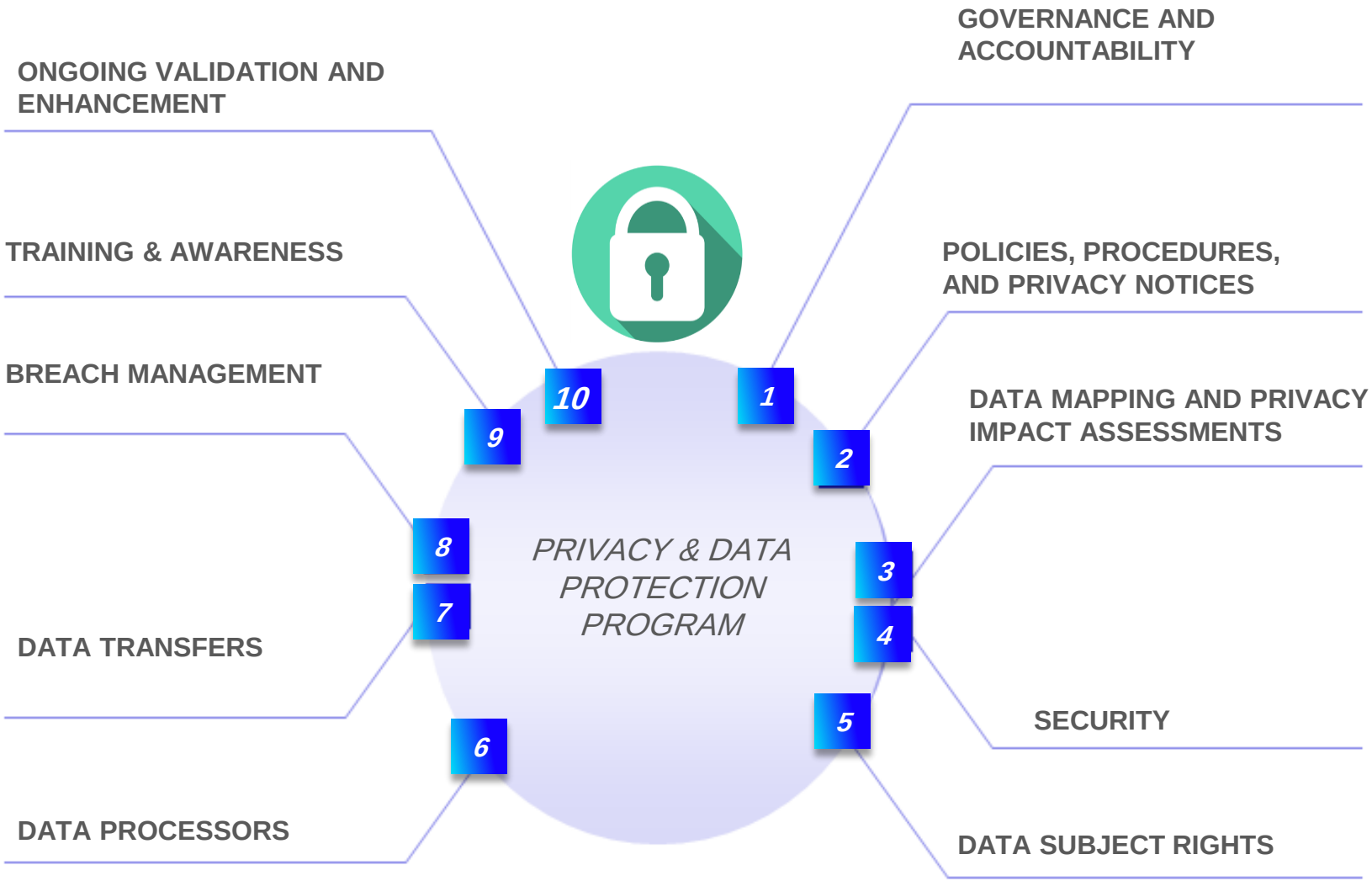
Tunisia

Draft Personal Data Protection Law - Issued July 2025, draft Law requires submitting authorizations to the Personal Data Protection Authority for any processing involving sensitive personal data (e.g. health and biometric data). Law also requires appointment of a Data Protection Officer who should be a Tunisian and resident in Tunisia. For any implementation of AI-decision making, data owners need to be informed of the AI processing, the logic applied behind the AI, the intended benefits, as well as their right to opt out.

Qatar

New Data Protection and Management Regulation issued by QCB Feb 2025 and effective Feb 2026. Requires QCB approval on cross border transfers and automated decision making as well as nomination of DPO

3 Best-Practice Aligned - Privacy and Data Protection Program



3 Best-Practice Aligned - Privacy and Data Protection Program

1.Governance and Accountability

Key Roles and Accountabilities:

- **Committee of the Board** oversees the effective implementation of the Program on quarterly basis
- **All employees** are accountable for protecting personal data with disciplinary actions undertaken for violations
- **Data Protection Officer (DPO).** Mandatory in some countries. Responsible for privacy and data protection activities and reports directly to the highest management level. The roles and responsibilities of the DPO should be clear while ensuring there is no conflict of interest.
- **Privacy and Data Protection Champions -** responsible for privacy and data protection within their respective function and undertakes the role of completing the Records of Personal Data Processing Activities across their function and it regular update

2.Policies, Procedures, and Privacy Notices

- **Policies & Procedures** –a data protection policy inclusive of applicable data subject rights and a breach management policy. Clear and detailed procedures should be developed and promulgated to related parties across the organization to ensure compliance.
- **Assessments & Assurance –** Self Assessments to assess privacy and data protection controls across various business lines.
- **Privacy Monitoring Program –** identify gaps and ensure ongoing effectiveness. This is vital to identify any weaknesses that may arise after the initial assessment as well as to drive enhancements in light of evolving risks such as revised regulatory requirement and breach scenarios.
- **Data Protection Clauses –** ensure the risk of an engagement or process is adequately covered through appropriate clauses covering any engagement with processors or sharing data with third parties for the purpose of conducting essential business.
- **Retention Schedules –** ensure all personal data are retained for only as long as necessary taking into consideration applicable regulatory requirements.
- **Privacy Notice –** should accurately reflect how an organization collects and uses data.

3 Best-Practice Aligned - Privacy and Data Protection Program

PRIVACY NOTICE – KEY CONSIDERATIONS

CONTENT - at the minimum should address:

- The contact details of the Data Protection Officer
- The purposes of processing
- The recipients or categories of recipients of personal data
- The details of transfers of the personal data to any third countries or international organizations
- The retention periods for personal data
- The rights available to individuals in respect of the processing and expected timeframes for reply
- The right to lodge a complaint with the supervisory authority (where applicable)
- The sources of the personal data (if the personal data is not obtained from the individual it relates to)
- The details of the existence of automated decision-making, including profiling and data mining
- Record retention practices
- Data storage locations (e.g. as part of DR)

Remember:
Privacy Notice needs to be regularly reviewed and updated. For example, to reflect new data mining activities or implementation of AI, new DR locations, new categories of personal data processors, etc

Dedicated Privacy Notices are needed per Data Subject, e.g. customer, employee, Vendor, Board member etc.

Bad and Good Practices?

"We may use your personal data to develop new services"	
"To improve our services and enhance your experience, this application uses analytics tools to collect information about the use of the application. This includes details such as device type, device ID, IP address, the country/city from you're accessing the app. The data collected is used in aggregated and anonymized form to help us understand how the application is used, identify areas for improvement, and ensure the security and reliability of our services. "We may use your personal data for research purposes"	
"We may use your personal data to offer personalized services"	
"We may use information provided or obtained via this site to respond to your queries and feedback (for example, if you've asked a question or submitted feedback via the site), provide you with information, products or services you have requested, carry out our obligations from any contracts entered into between you and us, allow you to participate in any interactive features of the site, notify you about changes to the site, or provide you with updates where you've consented to receive these by registering on the site"	

3 Best-Practice Aligned - Privacy and Data Protection Program

3. Data Mapping and Privacy Impact Assessments

Data Mapping (Records of Personal Data Processing Activities (ROPA)) identifies the full-life cycle of personal data – including:

- Categories of personal data (customer identification data, online identifiers)
- Data subjects involved (e.g. representatives of corporate customer, joint account holders, minor/guardian, employee, employee family members, representatives of vendors
- Source of the personal data
- Systems where the personal data is maintained
- Locations where the personal data is maintained including as part of DR and any cloud hosting
- Where the data is transferred to and the list of recipients
- Data retention periods
- Enforced technical and security measures
- Any automated decision making
- ***The legitimate basis of processing***

**ROPA must be updated on regular basis (at least annually)*

Lawful basis for processing

- Legal obligation - example: processing personal data to comply with AML, sanctions-screening, FATCA, or other regulations
- Contract - example: An individual is looking for a Car Loan, a bank needs to process certain data to provide a quote; such as credit score, make, and age of the car.
- Legitimate Interest – example: the Processing of family members' data in the context of Human Resources records (e.g., emergency contact, benefits, and insurance). Another example is processing customers' personal data in order to deliver targeted products and services that better suit their needs.
- Indivisual Consent: direct marketing, data mining and profiling, automated decision making

Note: basis differ country to another

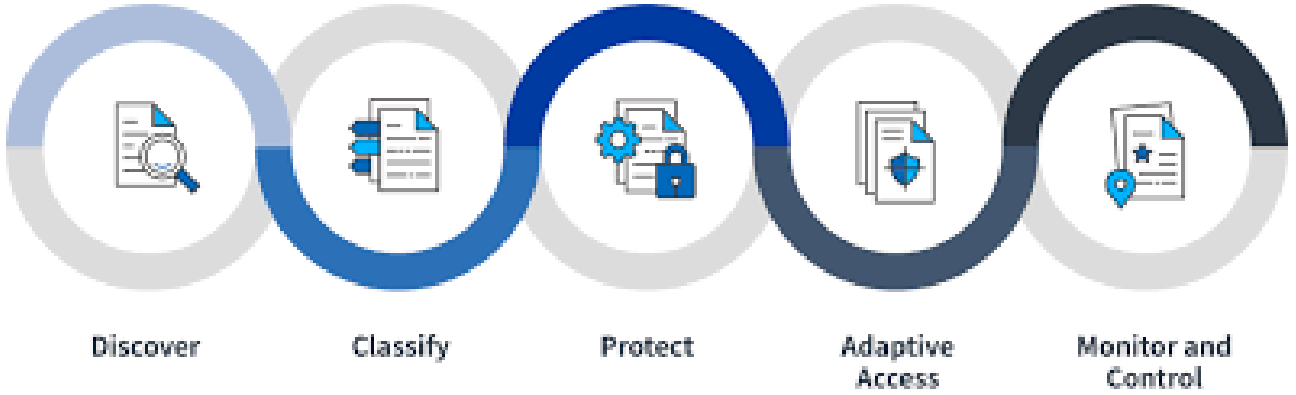
Privacy by Design - Privacy Impact Assessments

Carried out on all activities and initiatives that may have privacy implications including:

- Using a new way for storing data (i.e., cloud)
- Engaging a data processor to manage and maintain an IT system
- Transferring personal data
- New use of existing data to improve a product or service
- Directing customers to an external party
- Processing personal data in a way that involves tracking individuals' online or offline location or behaviour
- Implementing a new initiative that involves automated decision making or Artificial Intelligence (AI)

3 Best-Practice Aligned - Privacy and Data Protection Program

4. Security



Application of appropriate technical and organizational measures.

Organizational measures: approach taken by the organization in assessing, developing, and implementing controls that secure and protect personal data. These include information security policies, business continuity, regular assessment of processing activities and mitigating measures, robust policies and procedures, as well as ongoing training to ensure a culture of security and data protection.

Technical Measures: measures and controls implemented on systems from a technological aspect. These include appropriate measures in relation to cyber security, access management rights, password management, encryption of personal data, robust data disposal measure, passwords and two-factor authentication, bring your own device (BYOD) and remote access. Security controls and processes are updated regularly to meet industry standards.

3 Best-Practice Aligned - Privacy and Data Protection Program

5. Data Subject Rights (DSR)

Right to Access Personal Data
Data subjects have the right to access and request copies of their Personal Data.

Right to Limit Personal Data Processing
Data subjects have the right to request the restriction of the Processing of their personal data.

Right to Correct Personal Data
Data subjects can have their personal data rectified if inaccurate or completed if it is incomplete. This includes for example, data subjects' right to rectify their credit report with the national credit bureau.

Right to Erasure
Individuals can request the deletion of their personal data without undue delay.

Rights Related to Automated Decision Making
Individuals can object to decisions made about them based solely on automated processing.

Right to Objection
Individuals can object to the processing of their personal data by an organization.

Right to Data Portability
Individuals have the ability to receive their personal data in an organized, commonly used machine-readable form.

DSR operating Procedures

- How the organization intends to receive all requests, i.e. the channels for submitting requests?
- What information is required from the data subject?
- Where allowed under the local legislation, how the organization computes the fee in a way that accurately reflects the time and effort required to respond to the request?
- How the organization ensures requests are processed within the regulatory timeframe and what feedback would be provided to the individual in the event the organization is unable to fulfil the request within that timeframe?
- What procedures are established by the organization to verify the identity of the individual making the request?
- What is the organization's documentation process for recording requests received and processed. Documentation may also include requests received but not processed due to an applicable exception?
- What is the organization's retention policy for keeping records of requests received?

Not all of these rights are 'absolute'; some only apply in specific circumstances. For example, while data protection laws grant customers the right to personal data erasure, this does not apply where an organization has a lawful basis for maintaining this personal data such as compliance with data retention regulations.

3 Best-Practice Aligned - Privacy and Data Protection Program

Data Subject Rights - Right to object to decisions made solely on automated basis

SOLELY

Is totally automated and excludes any human influence on the outcome. A process might still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system. A process won't be considered solely automated if someone interprets the result of an automated decision before applying it to the individual.

- Example:

  An employee is issued a warning about late attendance at work. The warning was issued because the organization's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data. In this example, the decision was not taken solely by automated means.

SIGNIFICANT

Decision affects a person's legal status or their legal rights. In extreme cases, it might exclude or discriminate against individuals. Decisions that might have little impact generally could have a significant effect for more vulnerable individuals, such as children

- Examples:
  - o Automatic refusal of an online credit application.
  - o E-recruiting practices without human intervention.
  - o An individual applies for a loan online. The website uses algorithms and automated credit searching to provide an immediate yes/no decision on the application.

3 Best-Practice Aligned - Privacy and Data Protection Program

6. Data Processors

Minimum Requirements:

- Only act on the written instructions of the controller (unless required by law to act without such instructions)
- ensure that any individuals processing the data are subject to a duty of confidentiality
- take appropriate measures to ensure the security of processing
- only engage a sub-processor with the prior consent of the data controller and a written contract
- assist the data controller in allowing data subjects to exercise their rights
- assist the data controller in meeting its regulatory obligations in relation to the security of processing and notification of personal data breaches
- delete or return all personal data to the controller as requested at the end of the contract
- submit to audits and inspections by the data controller.

Data Controllers need to ensure they maintain detailed records on Third Party access, storage location, storage medium, processing location, and retention periods.

7. Data Transfers

Whitelist

Many data protection laws (e.g. Jordan*, Bahrain, Morocco) contain a 'whitelist' of countries to whom personal data may be transferred with standard security measures because they provide adequate levels of personal data protection.

For non-whitelisted countries or 'third countries' as they are also known, data protection laws require additional safeguards to be in place such as contractual clauses for the protection of data transferred. E.g. Contractual Clauses (SCC) in the EU.

Regulatory Approval

All cross border transfers versus transfers to non-whitelisted jurisdictions:

- **All cross border transfers**: examples

Qatar: cross border transfers made by banks as required by Qatar Central Bank.

Algeria: all cross border transfers made by Data Controllers require Algeria Data Protection Authority

- **Transfers to non-whitelisted countries**: examples

Bahrain and Morocco

* In progress

3 Best-Practice Aligned - Privacy and Data Protection Program

8. Breach Management

- Ascertain severity of the breach and whether it is still occurring.
- If still occurring, establish immediate steps to contain breach (e.g. restricting access to systems)
- Recover data loss where possible and limit damage caused (e.g. use of backups to restore data, changing passwords etc.)
- Inform Board Committee if severity and likely impact of the breach warrants such.
- Seek legal advice if it is believed that illegal activity has occurred or likely to occur.
- Ensure regulatory reporting within prescribed timeframes.
- Ensure actions/decisions fully documented in Data Security Breach Log.

- Types and volume of data are involved
- Is there sensitive data impacted with the breach
- Were preventions in place to prevent access/misuse? (e.g. encryption)
- Number of individuals affected
- Potential harm on individuals, e.g. physical safety, reputation, finances, identity theft, other private aspects to their life

- Full review of both; breach causes and effectiveness of the response.
- Report review results to related Board Committee for information and discussion
- If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans must be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements.
- Committee to monitor progress against the actions appropriately.

When to report to the Regulator and Data Subject

Under the majority of personal data protection regulations:

- Reporting warranted when significant damage expected to data subject which is subject to the organization analysis on a case by case basis. Yet organizations needs to ensure decision of “not to report” is properly documented and justified.
- Reporting timeframe:
  - Reporting must be made “as soon as possible” after event discovery (e.g. in Algeria)
  - Reporting must be made within 24/72 hours to the data subject and authority respectively (i.e. in Jordan)

3 Best-Practice Aligned - Privacy and Data Protection Program

9. Training and Awareness

	TIMING	DETAILS
BOARD OF DIRECTORS	• At the start of the organization's personal data protection journey • Periodically to ensure the Board is kept abreast of regulatory developments, best practice, and evolving risks	Board awareness and support of personal data protection risks and inclusion of personal data protection risks into corporate risk management framework
SENIOR MANAGEMENT	• At the start of the organization's personal data protection journey • Periodically (e.g. during formulation of annual internal audit plans)	Rationalize business benefits of personal data protection, highlight key roles of senior management, and establish risk reporting structure to identify and manage risk
ALL STAFF	• Upon hiring (e.g. within 3 months of employment) • On a periodic basis (e.g. annually) • Ad-hoc when there is a revision to data protection laws or the organization's data protection policies and processes	Educate staff on regulatory requirements and the organization's data protection policies and processes. Remember, it is important to make available data protection training materials in an accessible platform (e.g. intranet)
STAFF HANDLING PERSONAL DATA	• Upon assignment to a specific job role or change in role/job scope • When there are new data protection policies or processes	In-depth data protection training specific to internal policies and processes
PROFESSIONAL CERTIFICATION	• As part of career development	The DPO and staff who are part of the DPO team

3 Best-Practice Aligned - Privacy and Data Protection Program

10. Ongoing Validation and Enhancement

Independent Audits: Specific independent audits reinforce the privacy culture by continuously enhancing processes and internal controls and ensuring accountability. The organization's audit process should also include a fire drill of a data breach or an investigation. The organization may also consider engaging a third party to conduct audits/assessments.

KPIs/KRIs: Key Performance Indicators and Key Risk Indicators related to the data protection framework and activities help ensure a privacy culture is enforceable and measureable. These include but are not limited to number of data breaches, PIAs completed, privacy issues escalated by the Champions, Privacy and Data Protection training completion rates, and results of mock breach exercises.

Benchmarking against Best Practice: The organization should also maintain a process for keeping abreast of best practice developments in order to identify areas for enhancement and drive needed changes to continue to add value and ensure effectiveness of the Program. This should be officially formalized in the DPO job description.

Record Retention: The organization should maintain documentation of monitoring results and reviews as necessary to demonstrate compliance to regulators.

Thank You

Leen Qassisiya
VP – Head of Privacy and Data Protection, Arab Bank