Implementing a Privacy & Data Protection Program aligned with Leading Practices

Date: August 16. 2022

Delivered by: Ahmad Al Qawasmeh, VP – Head of Regulatory Standards and Privacy

البنك العربي
ARAB BANK

Agenda

I. Intensified Focus on Privacy and Data Protection

II. Overview of GDPR

III. Evolving laws and regulations

IV. Key Elements of Privacy and Data Protection Program

Effective Privacy & Data Security is a Competitive Advantage

To some, **Privacy is a Right**, to others, Privacy is an Expectation even if laws haven't yet caught up with the practices of the times

Personal information that is misused, mishandled, or inadequately protected can result in identity theft, financial fraud, and other problems that can cause significant damage to a company's reputations as well as significant cost to individuals to repair

البنك العربي
ARAB BANK

Intensified Focus on Privacy and Data Protection

Fines and Penalties

Danske Bank fined €1.3 million over non-compliant data deletion processes – Apr 2022

The Spanish Data Protection Agency fines CaixaBank 6 million euros for violating GDPR – Jan 2021

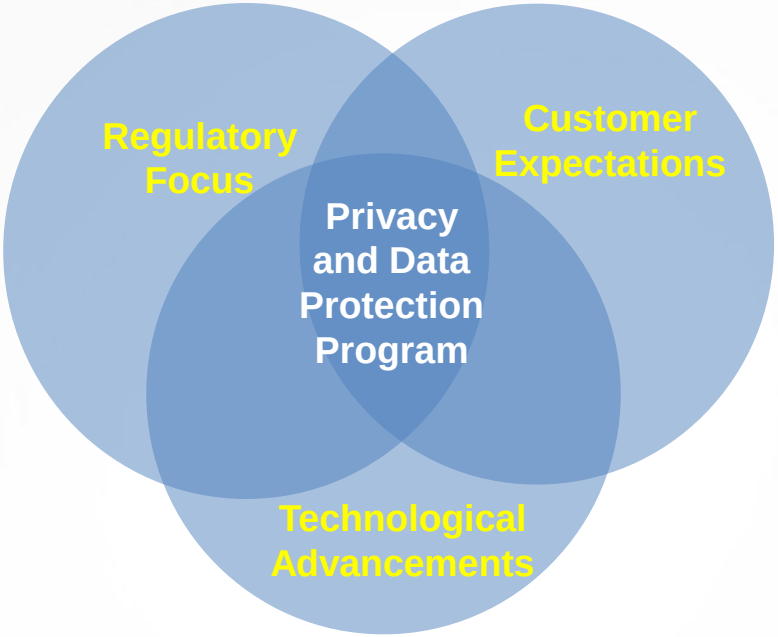
Google fined €150 million for Cookies breaches – Jan 2022

WhatsApp fined a record €225 million by Ireland over privacy issues – Sep 2021

E.U. regulator hits Amazon with record $887 million fine for data protection violations – Jul 2021

I. Intensified Focus on Privacy and Data Protection

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!

Embracing Innovation - Ensuring Regulatory Compliance - Enhancing Customer Trust

البنك العربي
ARAB BANK

II. Overview of GDPR

GDPR Principles	
Legality Principle	Demonstrate lawful reasoning for processing personal data
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
Purpose Limitation	Personal data should be collected for a specific purpose, and not processed outside of this 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 stated above**

البنك العربي
ARAB BANK

Overview of GDPR (Cont.)

Extraterritorial Scope:

Organizations established in the EU and to data controllers and processers outside the EU whose processing activities relate to the offering of goods or services OR monitoring the behavior (within the EU) of EU data subjects

Key Requirements:

I. Accountability

- Demonstrate accountability for personal data in possession and compliance with “Data Processing Principles”
- Data Protection Officers must be appointed if an organization conducts large-scale systematic monitoring or processes large amounts of sensitive personal data

II. Data Subject Rights

Introducing additional data subject rights: the right to be forgotten, the right to data portability, and the right to object to automated profiling

البنك العربي
ARAB BANK

Overview of GDPR (Cont.)

III. Privacy By Design / Privacy Impact Assessments

Embed privacy into the culture of the organization and therefore any activity that an organization undertakes shall be assessed for its privacy impact

IV. Security

Availability of technical and organizational measures protecting personal data

V. Data Transfer Mechanisms

Availability of technical and organizational measures to safeguard the transfer of personal data

VI. Breach Notification

Notify the supervisory authority of data breaches ‘without undue delay’ or within 72 hours, unless the breach is unlikely to be a risk to data subjects. In case of high risk, inform data subjects

Overview of GDPR (Cont.)

Data Subject Rights:

Subject Rights	
Right to be Informed	Right of the data subject to be informed of if his/her Personal Data is being processed, why its being processed and in what way
Right of Access	Right of the subject to access his personal information
Right to Rectify	Right to rectify Personal Data or request corrections
Right to Erasure	Right to erase Personal Data
Right to Restrict Processing	Right to stop processing in certain cases
Right to Data Portability	Right to receive Personal Data and/or transmit it to another controller
Right to Object	Right to object to processing on grounds relating to his/her particular situation
Right to Object against Automated decision making	Right not to be subject to a decision based solely on automated processing

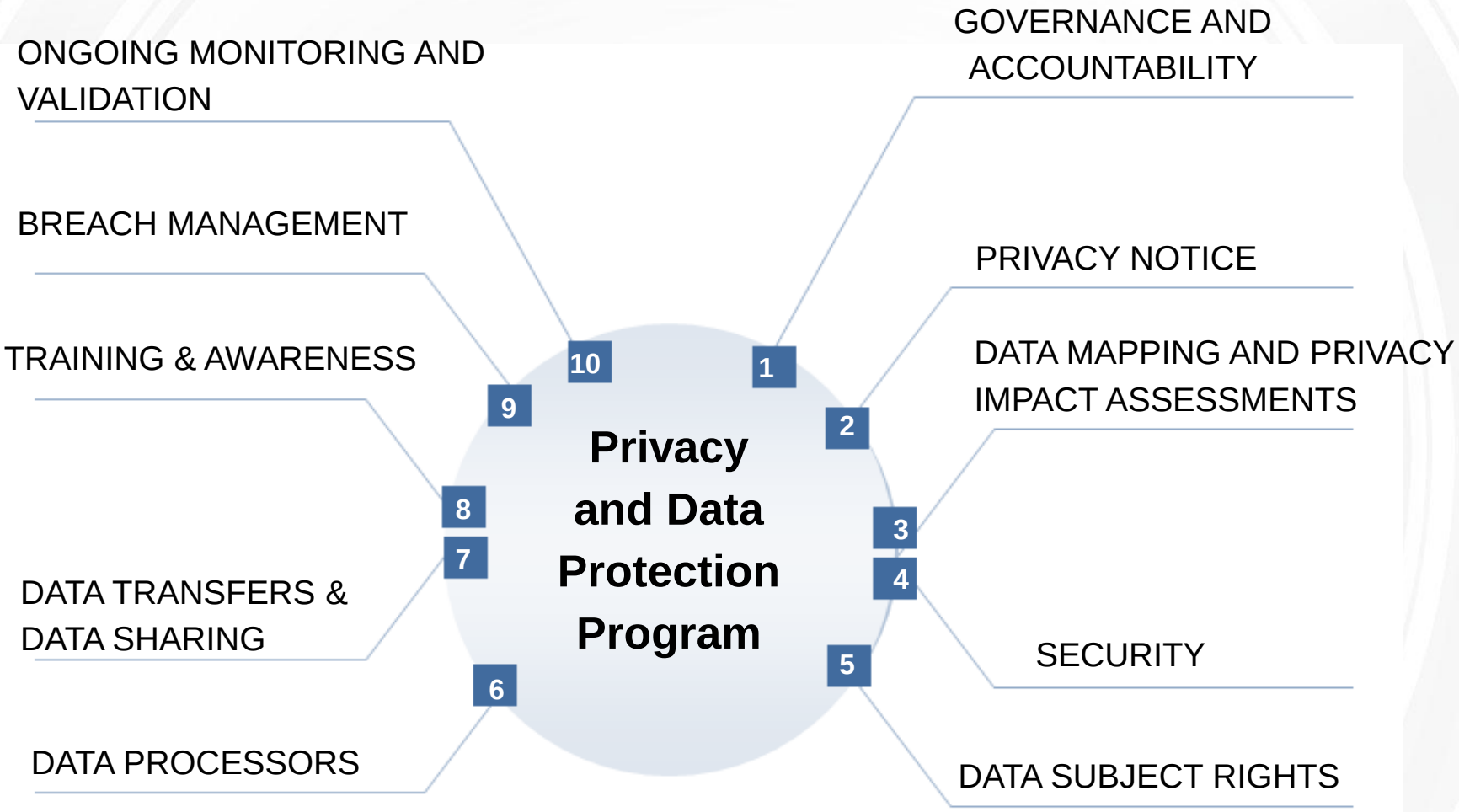
البنك العربي
ARAB BANK

III. Evolving laws and regulations

Algeria	• Law No. 18-07 Relating to the Protection of Individuals in the Processing of Personal Data *
Bahrain	• The Law of Personal Information Protection No. 30, 2018 (effective August 2019)
Egypt	• Data Protection Law No.151 of 2020**
Jordan	• Data Privacy Protection Act (Draft)
Lebanon	• E- Transactions and Personal Data Law, 2018 (effective January 2019)
Morocco	• Moroccan Data Protection Act 09-08, 2009
Oman	• Protection of Personal Data Law 06/2022
Qatar	• Personal Data Privacy Protection Law No.13, 2016 (PDPPL)
Saudi Arabia	• Personal Data Protection Law (effective March 2022)
Tunisia	• Organic Act 2004-63 on the Protection of Personal Data
UAE	• Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and Article 6 - Protection of Consumer Data and Assets Under the CBUAE Consumer Protection Regulations and Standard and

* Law will go into effect following establishment of Data Protection Authority within the office of the President
** According to final version issued, the Law does not apply to banks.

IV. Key Elements of a Privacy and Data Protection Program



البنك العربي
ARAB BANK

1. GOVERNANCE AND ACCOUNTABILITY

- Data protection and privacy must be a regular topic discussed at Board Level; Board must endorse privacy and data protection policies and procedures and oversee effective implementation of the program.
- Organizations are encouraged to appoint senior personnel “Data Protection Officer/ Data Protection Office” according to the size of the organization to assume responsibility for the privacy and data protection program
- Organizations are also encouraged to appoint “privacy and data protection champions” at each function responsible for ensuring compliance with data protection principles and liaising closely with the Data Protection Officer / Office
- All employees must be held accountable for protecting personal data with disciplinary actions undertaken for violations

2. PRIVACY NOTICE

KEY CONSIDERATIONS - CONTENT

To ensure alignment with leading practices, consider including the following in your Privacy Notice:

- Contact details of your Data Protection Officer (if applicable)
- Purposes of processing
- Recipients or categories of recipients of personal data
- Details of transfers of the personal data to any third countries
- Retention periods for personal data
- Rights available to individuals in respect of the processing
- Source of the personal data (if the personal data is not obtained from the individual it relates to)
- Details of the existence of automated decision-making, including profiling (if applicable)

Data Mapping

Some data protection regulations (e.g., under GDPR and data protection laws in Bahrain and Qatar) require identifying all processing activities in the organization involving personal data and documenting how and why the data is used in what is called a Personal Data Register or Data Mapping.

Among other things, Data Mapping requires organizations to identify and document the following for every processing activity:

- The different categories of personal data involved
- The systems and locations where the personal data is maintained
- The individuals to whom the personal data relates (e.g. customers, vendors, employees, etc.)
- Where the data is transferred and the list of recipients
- The data retention period
- Enforced technical and security measures
- **The lawful basis and purpose of processing the data**

Lawful basis for processing

- **Contractual Obligation:** processing is needed in order to enter into or perform a contract.
- **Legal Obligation:** processing is necessary for an organization to comply with regulatory requirements or an issuance of an order from a competent Court or the Public Prosecution.
- **Legitimate Interest:** processing of personal data is necessary in order to carry out tasks related to the organization's business activities and its legitimate interests or the legitimate interests of a third party.
- **Vital interest**: processing is necessary to protect the vital interests of the customer or of another individual. Generally, this lawful basis primarily applies to the health sector.
- **Public interest:** this is typically specific to organizations exercising official authority or carrying out tasks in the public interest. Generally, this lawful basis primarily applies to governmental entities and does not apply to the banking sector.
- **Consent:** an organization must seek to obtain the individual's consent to the processing of their personal data if none of the above five lawful bases apply.

Privacy Impact Assessments (PIAs)

PIAs must be carried out on all activities and initiatives that may have privacy implications, including policy proposals, new or amended programs, activities, systems or databases. It aims to ensure proper identification of privacy and data protection risks and application of commensurate risk mitigation measures. It is essential for a “Privacy by Design” approach

Questions to consider:

- Does the initiative change the method of data hosting? if yes, what is the method of hosting? E.g. in-house, cloud?
- Does the initiative involve processing of sensitive personal data?
- Are customers /data owners aware of the nature, purpose, and extent of the processing of their personal data under this initiative?
- Will the initiative/activity result in profiling or automated decision-making to make significant decisions about data owners?
- Will the initiative require marketing /additional contact with data owners?
- Is there some form of earlier consent on such processing under this initiative/activity?
- Will personal data be transferred cross-border? If yes, will this third party store/host personal data?
- Will this third party in turn share this personal data with any other third party/parties or rely on any third parties to provide the service?

4. SECURITY

Organizational Measures

Are defined as the approach taken 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

Are defined as the 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.

5. DATA SUBJECT RIGHTS

When establishing an internal policy on handling data subject requests, organizations should consider the following:

- The channels for submitting requests.
- What information is required from the data owner.
- 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.
- What is the organization's retention policy for keeping records of requests received.

6. DATA PROCESSORS

Data Controller determines the means and purpose of the processing. This means that they make decisions about what data is captured and why. Data Processor is the party that processes personal data based on the Data Controller's instructions.

Consider including the following in your contracts with Data Processors:

- Processor must only act on the written instructions of the Data Controller,
- Processor must take appropriate measures to ensure the security of processing,
- Processor must only engage a sub-processor with the prior consent of the Data Controller and a written contract,
- Processor must assist the Data Controller in allowing data owners to exercise their rights as applicable,
- Processor must assist the Data Controller in meeting its regulatory obligations in relation to the security of processing and the notification of personal data breaches,
- Processor must delete or return all personal data to the Data Controller as requested at the end of the contract, and
- Processor must submit to audits and inspections by the Data Controller.

7. DATA TRANSFERS & DATA SHARING

Organizations must make sure all the following are met:

- Ensure data transfers and data sharing are in compliance with regulatory requirements
- Implement proper safeguards for data transfers such as contractual clauses for the protection of personal data transferred
- Obtain the data owner consent on the transfer where required under local legislation

Many data protection laws 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, data protection laws require additional safeguards such as approval of the designated data protection authority

8. TRAINING AND AWARENESS

- **Hiring Procedures** - privacy and data protection responsibilities must be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.
- **Training & Awareness –** at a minimum, all employees should receive data privacy training on an annual basis. Some employees with greater exposure to personal data may require additional or specialized training.
- **Newsletters –** on a regular basis, it is recommended to create data protection content as part of existing newsletters or stand alone. The newsletter should be informative regarding current privacy news, recent fines, and lessons learnt.

Key Steps for Effective Management

Containment	• Ascertain severity of the breach and whether the breach is still occurring • If breach still occurring, establish steps to be taken immediately to contain the breach • Implement appropriate steps required to recover any data loss where possible • Inform the Board /Committee of the Board if severity warrants such • Seek expert or legal advice if it is believed that illegal activity has occurred or likely to occur. • Ensure regulatory reporting within prescribed timeframes • Ensure actions and decisions are fully documented and logged
Risk Assessment	• What types and volume of data are involved? • Is there sensitive data impacted with the breach? • Has the data been unofficially disclosed, lost, or stolen? • How many individuals are affected by the data breach? • What actual/potential harm could come to those individuals? • Are there wider consequences to consider?
Evaluation and Response	• Undertake full review of both the causes of the breach and the effectiveness of response. • If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified, appropriate action plans must be actioned and monitored to implement needed improvements.

10. ONGOING MONITORING AND VALIDATION

Key Considerations

- **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.
- **KPIs/KRIs:** these include but are not limited to number of data breaches, number of audit findings, privacy and data protection training completion rates, and results of mock breach exercises.
- **Benchmarking against Best Practice:** the organization should maintain a process for keeping abreast of best practice developments in order to identify areas for enhancement to continue to add value and ensure effectiveness of the program.
- **Record Retention:** the organization should maintain documentation of monitoring results and reviews as necessary to demonstrate compliance to regulators.

MENA FCCG

Making a Collective Impact

MEMBER BANKS

STRATEGIC PARTNERS

EU CHAPTER STRATEGIC PARTNERS

ALLIANCES

http://menafccg.com/publications/

Questions and Open Discussion

Privacy & Data Protection:
A Competitive Advantage

البنك العربي
ARAB BANK