MENA FINANCIAL CRIME COMPLIANCE GROUP

Engaging with multi-stakeholders to find solutions to promote leading AML/CTF practices.

A Practical Guide: Establishing a Privacy and Data Protection Framework

March 2021

TABLE OF CONTENTS

This document builds on international leading practices as well as the expertise of MENA FCCG's Technical Working Committee to provide practical overview of data protection and privacy fundamentals. It does not however address all privacy requirements, nor does it constitute legal advice.

1.0 INTRODUCTION

Privacy and protection of personal data is a key concern for both customers, organizations, and regulators. Customers expect organizations to treat their personal information as private and confidential, to effectively safeguard their personal data, and to use it only to provide and operate financial services, and for other purposes as required by law or regulation. MENA regulators are increasing focusing on how organizations manage personal data in their possession from the point of data collection and up to data disposal while also enhancing customer rights, including rectification of their personal data, data access, and objection to processing where appropriate (Reference Annex (I): Data Protection Legislation in MENA Countries[1]). Accordingly, protection of personal data and associated customer trust has become a competitive advantage and a critical focus area for risk managers.

By definition, personal data is any data related to an identified or identifiable individual used to identify a particular person. Examples include: full name, personal identification number, driver's license number, bank account number, passport number, email address, location data, or one or more of their physical, physiological, intellectual, cultural, or economic characteristics or social identity (Reference Annex (II) - personal data). Privacy and data protection generally go hand-in-hand. Privacy is a fundamental human right and defined as the right of any individual to control their own personal information while data protection is the process of safeguarding personal information from corruption, compromise, or loss as well as ensuring its availability.

The purpose of this Guide, along with the Privacy Self-Assessment Questionnaire, are intended to increase compliance awareness of the key elements for building an effective Privacy and Data Protection Framework as necessary to meet evolving regulatory expectations and harness customer trust.

[1] MENA FCCG will update this annex as necessary to reflect new/revised regulatory requirements.

2.0 PRIVACY AND DATA PROTECTION PRINCIPLES

A Privacy and Data Protection Framework should seek to achieve the following key principles:

I. **Legality, Fairness, and Transparency –** Personal data should be processed fairly, transparently, and lawfully. An individual's personal data should not be processed unless there are lawful grounds for doing so and the individual should be informed as to how and why their personal data is being processed either upon or before collecting it.

II. **Data Minimization and Limitation –** Data collected should be limited to minimum data necessary for the purpose of collection only. Personal data should also be processed only for the purpose initially collected. Any further processing should require customer consent unless there is a legal basis such as fulfilling a regulatory request.

III. **Accuracy –** Personal data should be accurate and, where appropriate, kept up to date. Incorrect data should be rectified as soon as possible. Organizations are advised to develop ongoing processes for data update and making channels available for customers to update their data (e.g. face to face and online).

IV. **Data Retention –** Data should not be kept longer than is necessary for the purpose for which it was collected while taking into consideration regulatory record retention requirements.

V. **Rights of Data Subjects –** Organizations should implement appropriate processes to ensure timely response to data subject rights' requests as applicable. Data subjects are the individuals to whom the personal data belongs; these include customers, employees, Board members, and third parties.

VI. **Security -** Personal data should be protected against unauthorized or unlawful processing, accidental loss, destruction or damage through appropriate technical and organizational measures.

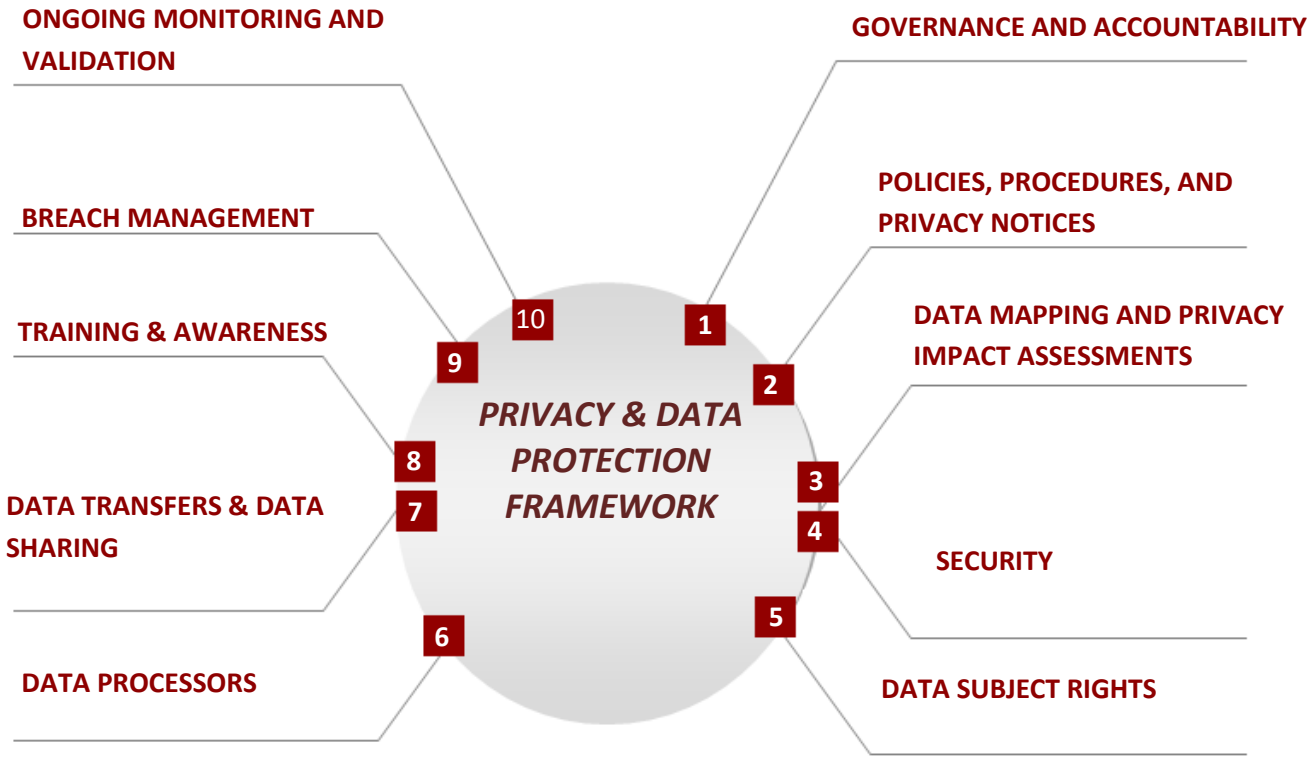
VII. **International Data Transfers –** When transferring data to a territory outside the organization's country, effective due diligence and controls should be in place to ensure an adequate level of protection.

VIII. **Accountability –** Accountability is the ability to demonstrate compliance with all the above principles and is required under the EU's General Data Protection Regulation (GDPR) and other data protection regulations worldwide. Accountability mechanisms include policies, procedures, guidelines, checklists, training and awareness activities, transparency measures, technical safeguards, and other mechanisms that mitigate internal and external privacy and data protection risks.

The following sections will explain how the above principles can translate into actual processes.

3.0 KEY ELEMENTS OF AN EFFECTIVE PRIVACY AND DATA PROTECTION FRAMEWORK

Privacy and Data Protection compliance is a journey and requires ongoing awareness and understanding of personal data processing operations and embedding privacy management throughout the organization. A one-size-fits-all approach is also not the answer. However, the following represents the key elements based on international leading practices.



3.1 GOVERNANCE & ACCOUNTABILITY

Governance and accountability are fundamental to building a strong data protection & privacy framework; key elements are summarized below:

3.1.1 Board Vision & Strategy

Data protection and privacy should be a regular topic discussed at Board Level given the global emergence of technology, increased privacy laws, and global reach of customers. In addition, privacy and data protection should be placed at the core of the organization's vision. This is achieved through senior management commitment and ongoing staff training and awareness. As part of its oversight, the Board should ensure management understands the privacy environment and its implications to the organization's business model. Meaningful and appropriate Management Information (MI) must be provided to the Board that would allow it to exercise effective oversight. This includes number of data breaches, results of mock data breaches, employee data privacy training statistics, and related audit and review results and high risk policy violations.

3.1.2 Territorial Scope

Organizations should consider the privacy laws impacting their organization and the implications of extraterritorial reach. Organizations that have offices, affiliates, or subsidiaries in multiple jurisdictions, face a greater likelihood of various data privacy regulations impacting them. To build a baseline, organizations should focus on where personal data is likely to be stored, collected, or processed as well as focus on common areas including Marketing, Human Resources, Finance, IT / Systems and applications. Understanding where the data flows using the data mapping exercise described in this document (section 5) can help identify applicable requirements.

3.1.3 Accountability and Roles and Responsibilities

Organizations should look to build Privacy and Data Protection Units responsible for the overall data protection and privacy activities. When deciding on the appropriate privacy model, organizations may choose between a Centralized, Decentralized, or Hybrid model to develop their privacy strategy. A centralized model utilizes a single channel function leaving one team responsible for privacy. Decentralized model delegates key responsibilities to lower tiers of organizational structure. A Hybrid model combines both centralized and decentralized, typically used where organizations have multiple offices or entities. Key elements to consider when scoping the size and structure are:

I. **Data Protection Officer (DPO)** - Organizations should look to appoint a DPO who is 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.

II. **Privacy and Data Protection Champions -** To further safeguard data, organizations should designate champions that are responsible for privacy and data protection within their divisions/department/sections. It is expected to have a Champion for each division (e.g. HR, IT, Marketing, Credit…etc.)

III. **Data Privacy Governance Committee –** A governance committee should be formed, with adequate Terms of Reference to discuss privacy incidents, issues, and risks. The formation of a committee also demonstrates a tone at the top and senior management commitment.

DPO APPOINTMENT – KEY CONSIDERATIONS	
WHAT ARE THE KEY ROLES?	▪ Ensuring compliance with privacy and data protection regulatory requirements ▪ Fostering a privacy and data protection culture and communicating personal data protection policies to stakeholders ▪ Overseeing the process for responding to data subject requests to exercise their rights ▪ Managing personal data protection-related queries and complaints ▪ Alerting management to any risks that might arise with regard to the personal data handled by the organization ▪ Ensuring compliance with regulatory requirements in relation to any breach based on the incidence response plan ▪ Liaising with regulatory authorities on personal data protection matters, if necessary
HOW SHOULD THE DPO BE APPOINTED?	A DPO should ideally be an appointment from senior management. Their responsibilities can be taken on by one employee, a group of employees, or outsourced. When outsourcing the DPO function, the organization should still ensure that an individual appointed from senior management remains responsible to work with the outsourced DPO.

3.2 POLICES, PROCEDURES, AND PRIVACY NOTICES

The documentation infrastructure is crucial to tie data privacy principles and allow proper functioning of the organization by establishing boundaries of behaviour, outlining processes, and defining rules. To build a strong data protection framework, the below should be considered:

I. **Policies & Procedures** – At a minimum, the organization should consider creating 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.

II. **Assessments & Assurance –** Self Assessments should be conducted and documented to assess privacy and data protection controls across various business lines. (You may refer to MENA FCCG Privacy and Data Protection Assessment Questionnaire available at http://menafccg.com/publications/).

III. **Privacy Monitoring Program –** A Privacy Monitoring Program should be created and documented to 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 ongoing enhancements in light of evolving risks such as revised regulatory requirement and breach scenarios.

IV. **Data Protection Clauses –** Organizations should ensure they have a suite of data protection clauses to 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.

V. **Retention Schedules –** Retention standards should be documented to ensure all personal data are retained for only as long as necessary taking into consideration applicable regulatory requirements.

VI. **Privacy Notice –** The organization's Privacy Notice, posted on its website, should accurately reflect how an organization collects and uses data. The content of a Privacy Notice can differ from one country to another. However, in all cases the Privacy Notice should be clear and easy to understand and should not contain any jargon.

PRIVACY NOTICE – KEY CONSIDERATIONS	
CONTENT	To ensure alignment with leading practices, consider including the following in your Privacy Notice: ▪ The contact details of your Data Protection Officer (if applicable) ▪ 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 (if applicable) ▪ The retention periods for personal data ▪ The rights available to individuals in respect of the processing ▪ The right to withdraw consent (if applicable) ▪ The right to lodge a complaint with the supervisory authority (where

	applicable) ▪ The source 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 (if applicable)
REVIEW AND UPDATE	Remember, the Privacy Notice needs to be regularly reviewed and updated. For example, if the organization plans to use personal data for a new purpose, the Privacy Notice needs to be updated and communicated to data subjects.

Privacy Notice - Examples of Good and Bad Practice	
Poor Practices: • "We may use your personal data to develop new services" (it is unclear what the "services" are or how the data will help develop them) • "We may use your personal data for research purposes" (it is unclear what kind of "research" this refers to) • "We may use your personal data to offer personalized services" (it is unclear what the "personalization" entails)	**Better Practices:** "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" (it is clear in this example the kind of processing the organization is going to undertake)

Demonstrating accountability and embedding privacy and data protection across the organization's processes involves a wide array of policies and procedures. However, the role of the Privacy and Data Protection Officer can differ; examples follow:

ROLE OF THE PRIVACY AND DATA PROTECTION OFFICER – EXAMPLES	
Developed by the Privacy Officer while seeking input from key stakeholders	• Privacy and Data Protection Policy • Privacy Notice • Training Curriculum • Privacy and Data Protection Impact Assessment Guidelines • Policy/procedure for secondary uses of personal data
Influenced by the Privacy Officer but created by other stakeholders	• Direct Marketing Procedures • Employment Policies • Records retention schedules
Made available to the Privacy	• Internal Audit Results

Officer upon completion for record retention and validation purposes	• IT Security Assessment Results • Business Continuity Plans

3.3 DATA MAPPING & PRIVACY IMPACT ASESSMENTS (PIAs)

This section describes some of the tools that can be used to demonstrate data privacy principles and to ensure day to day activities take into consideration privacy and data protection.

3.3.1 Data Mapping / Records of Processing Activities

Data Mapping, i.e. maintaining a record of data processing activities, is a requirement for many organizations under GDPR and a best practice for even those that are not required to apply it. Additionally, the Supervisory Authorities may request records of the processing activities within an organization, and the production of a data map is one piece of information that could help fulfil their request. Once a list of processing activities has been compiled, it is easier for organizations to justify their processing or determine where lawful basis needs to be obtained. This exercise is considered an evidence that an organization takes the privacy by design and default principles seriously. In essence, an organization that constructs a data flow map of a new technology or process is better prepared to inject privacy protections at an early stage in process.

Benefits of a Data Mapping:

I. **Privacy Notices** – Based on data mapping, an organization can provide more accurate privacy notices that articulate the types of processing it conducts over personal data in its possession.

II. **Security** – understanding where personal data is located and flowing throughout the business is the first step to understanding risks which allows for proper security safeguards and controls to be put in place.

III. **Data Subject requests** – As part of data subject rights**,** customers may ask what data your organization is collecting and where it is being sent, having a record of processing activities makes it easier to respond in a timely manner.

IV. **Data Breach response** – Having a central data register helps to respond more appropriately to a breach and understand what data may have been exposed based on areas impacted by the breach.

3.3.2 Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a practical tool to help identify and address data protection and privacy concerns at the design and development stage of a project or business change. It is designed to help you analyse, identify, and minimise privacy risks to individuals whenever a new

system, product, service or business process is introduced or where changes are proposed to existing processes and systems.

A PIA also helps organizations meet individuals' expectations of privacy and data protection and help avoid reputational damage which might otherwise occur. There can also be financial benefits; identifying a potential issue or problem early on generally means a simpler and less costly solution.

However, a PIA does not have to eradicate all risks, but should help in minimizing and determining whether or not the level of privacy and data protection risk is acceptable in the circumstances, taking into account the benefits the new / revised process, product, service etc. intends to achieve. Conducting a PIA is generally a legal requirement for any type of processing that is likely to result in high risk to individuals under some data protection laws.

3.4 DATA SECURITY - TECHNICAL & ORGANIZATIONAL MEASURES

The organization should ensure application of appropriate technical and organizational measures for the protection of personal data including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. Some examples of security measures to implement include:

I. **Access Management –** having proper access management controls limit access to personal data for authorized employees. Separation of duties and privilege principles ensure users have action only in accordance with their roles.

II. **Pseudonymization and Encyption –** Pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. Encryption entails using an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble or decrypt the information.

III. **Incident Response Management (IRP) –** A mature IRP addresses phases of an incident including preparation, identification, containment, recovery and lessons learnt. Data protection laws require notification to authorities and affected data subjects under certain conditions and time frames; for example, GDPR requires organizations to report to authorities within 72 hours after becoming aware of a breach. A strong process for incident response identifies potential data breaches in a timely manner.

IV. **Third Party Risk Management –** Third Party Risk Management enables organizations to appropriately identify key controls that must be implemented by data processors reducing privacy risk.

V. **Data Leakage Prevention –** Data Leakage Prevention (DLP) is defined as the practice of detecting and preventing the unauthorized disclosure of data. Certain regulatory requirements in the MENA region mandate banks enforce measures to address the

risk of unauthorized downloading of customer data and loss of data containing sensitive information by implementing endpoint DLP solutions. An effective DLP solution helps organizations understand the types of data to protect, monitor the journey of the data including channels of data leakage and ultimately prevent data leakage such as blocking certain types of messages/files from leaving the organization's domain. DLP solutions can mitigate malicious intent, negligence, as well as accidental disclosure of data.

3.5 DATA SUBJECT RIGHTS

A key element of Privacy and Data Protection is data subject rights. Countries have implemented different approaches in relation to data subject rights including the scope and the timeframes within which these rights should be fulfilled by the organization. Examples of key rights are listed below:

I. **Right to information -** This right provides the data subject with the ability to ask the organization for information about what personal data (about him or her) is being processed and the rationale for such processing.

II. **Right to access -** This right allows the data subject to see or view their own personal data, as well as to request copies of the personal data.

III. **Right to rectification -** This right provides the data subject with the ability to ask for modifications to his or her personal data in case the data subject believes the personal data is not up to date or accurate.

IV. **Right to withdraw consent –** Data subjects should have the ability to withdraw a previously given consent for processing of their personal data.

V. **Right to object to decisions made solely on automated basis –** an automated decision making is any form of automated processing of personal data (including profiling) that produces a legal effect on or significantly affects the data subject. This right provides the data subject with the ability to object to a decision based on automated processing. Using this right, an individual may ask for his or her request to be reviewed manually, because he or she believes that processing of his or her loan may not consider his/her unique situation.

VI. **Right to be forgotten / deleted -** This right provides the data subject with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right, and depends on the organization's retention schedule in line with other applicable laws

VII. **Right for data portability -** This right provides the data subject with the ability to ask for transfer of his or her personal data. As part of such request, the data subject may ask for his or her personal data to be provided back (to him or her) or transferred to another organization.

CONSIDERATIONS ON DEVELOPING POLICY ON HANDLING DATA SUBJECT REQUESTS TO EXERCISE THEIR RIGHTS

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

- 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.

RIGHT TO OBJECT TO AUTOMATED DECISION MAKING – ISSUES TO CONSIDER

"Solely"

Solely means a decision-making process that 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.

Remember: the question is whether a human reviews the decision before it is applied and has discretion to alter it, or whether they are

	simply applying the decision taken by the automated system.
"Significant"	A decision producing a significant effect is something that 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: ○ Automatic refusal of an online credit application. ○ E-recruiting practices without human intervention. ○ 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.

3.6 DATA PROCESSORS

A controller or processor of personal data have different roles and responsibilities and therefore it is important for organizations to know which role they play. Under GDPR and other privacy and data protection laws, the data controller has greater responsibilities in relation to protecting the privacy and rights of data subjects.

Controllers determine the purposes and means of the processing of personal data. In essence, they make decisions about processing activities, whilst processors are third parties that process data based on the controller's instructions.

When a controller appoints a processor, they should conduct sufficient due diligence and insert appropriate data protection clauses to clearly define the role and specific purposes when the processor can process personal data. Under GDPR and some privacy laws, a controller should conduct privacy impact assessments when they instruct processors to carry out high risk data processing activities. Finally, in the event of a data breach, controllers must notify the Supervisory Authorities and the data subjects whenever a breach results in the rights and freedoms of the data subjects being put at risk. A processor on the other hand, must notify the relevant controller impacted by the breach.

CONTRACTS WITH DATA PROCESSORS - KEY CONSIDERATIONS

Consider including the following in your contracts with data processors:

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

CONTROLLER AND PROCESSOR - MAIN DIFFERENTIATOR

Remember: The controller determines the business purpose, i.e. the 'why' for which the data shall be used and the means, i.e. the 'how' the data are processed. The processor, on the other hand, is bound by the instructions given by the controller and only acts 'on behalf of' the controller while processing the controller's data.

3.7 DATA TRANSFERS AND DATA SHARING

As a general rule, cross border transfers are permissible when transferring data to a country with adequate data protection laws. Organizations should review their data flow maps to understand where cross border transfers occur. Once the assessment is complete, organizations should review if the jurisdictions are adequate as deemed by data protection laws. If not, they should ensure sufficient due diligence is conducted as well as incorporate appropriate safeguards and contractual clauses into agreements.

3.8 TRAINING AND AWARENESS

A strong privacy and data protection culture enables employees in an organization to contribute towards a common goal with confidence and purpose. All employees should be aware of their

roles and responsibilities in safeguarding personal data. There are numerous ways to continuously enhance and improve the privacy culture, these include:

I. **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. Internal Circulars, workshops and brochures are recommended as continuous methods of raising awareness and enforcing commitment to protect personal data.

II. **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.

III. **Hiring Procedures** - Employees (full/part time employees, contractors & third parties staff members) should be made aware of their roles and responsibilities towards protecting the organization's information assets, and should be aware of key threats to these assets. Privacy responsibilities must be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

Remember, training, awareness, and capacity building is a journey. The organization should ensure its training and awareness addresses all levels and commitment to privacy and data protection cascades top down across the organization.

TRAINING AND AWARENESS – KEY CONSIDERATIONS		
TARGET	**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

3.9 BREACH MANAGEMENT

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can occur due to various reasons such as malicious activity, human error, or computer system error.

Organizations should develop and implement a personal data breach management process to address breach incidents. The plan should include appropriate procedures governing all the following key activities; containing the breach, assessing the risk, reporting the incident, evaluating the response, and recovery to prevent future breaches.

Breach Management – Key Steps for effective management	
Containment:	▪ Ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring. ▪ If the breach is still occurring, establish what steps need to be taken immediately to minimize the effect of the breach and contain the breach from further data loss (e.g. restricting access to systems or close down a system etc.) ▪ Implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of backups to restore data, changing passwords etc.) ▪ Inform the Compliance Committee of the Board /Risk Committee of the Board if the severity and likely impact of the breach 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 in your Data Security Breach Log.
Risk Assessment:	To help the organization determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for individuals are likely to occur and the seriousness of these consequences. Key issues to consider: ▪ 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? Were preventions in place to prevent access/misuse? (e.g. encryption) ▪ How many individuals are affected by the data breach?

	▪ What could the data tell a third party about the individual? Could it be misused regardless of what has happened to the data? ▪ What actual/potential harm could come to those individuals? E.g. physical safety, reputation, finances, identity theft, other private aspects to their life ▪ Are there wider consequences to consider?
Evaluation and Response	When the organization's response to a data breach has reached a conclusion, the organization should: ▪ Undertake a full review of both the causes of the breach and the effectiveness of the response. ▪ The full review should be reported to the Privacy and Data Protection Committee for information and discussion as soon as possible after the data breach has been identified. ▪ 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. ▪ The Committee should monitor progress against the actions appropriately.

3.10 ONGOING MONITORING & VALIDATION

- **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.

ANNEXES

I. Data Protection Legislation in MENA Countries

II. Personal data (Customer and Employee)

III. MENA FCCG Privacy and Data Protection Assessment Questionnaire

Annex (I): Data Protection Legislation in MENA Countries

Algeria

DATA PROTECTION LEGISLATION

Data Protection in Algeria is governed by law No. 18-07 dated 10 June 2018 on the protection of individuals in the processing of personal data ("Law 18-07") which was published in the Official Gazette in July of 2018.

KEY DEFINITIONS

- Definition of personal data: any information, irrespective of its medium, concerning a person identified or identifiable, in a direct or indirect manner, in particular by reference to an identification number or to one or more specific elements of their physical, physiological, genetic, biometric, psychic, economic, cultural or social identity.
- Definition of sensitive personal data: Sensitive personal data is defined under the law as personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership of the person concerned or relating to his health, including his genetic data.

AUTHORITY

Law 18-07 shall create, with the President of the Republic, an independent administrative authority for the protection of personal data. This national authority is responsible for ensuring that the processing of personal data takes place in accordance with Law 18-07.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer under Law 18-07.

REGISTRATION

The personal data controller must be registered on a national data protection register kept by the national authority. In addition, any processing operation of personal data, is subject to a declaration or prior authorization of the national authority.

DATA PROCESSING

The processing of personal data may only be carried out with the express consent of the relevant person. Such prior consent is not required in certain cases exhaustively listed in Law 18-07. For example, when data processing is needed:

- To comply with a legal obligation applicable to the relevant person or to the personal data controller
- To perform a contract to which the relevant person is a party or to perform pre-contractual measures taken at the request of the relevant person.
- To achieve a legitimate interest of the data controller or the recipient of the data.

DATA SUBJECT RIGHTS

- Right to prior information - Right of access - Right of rectification - Right of opposition

DATA TRANSFER

- The authority shall authorize cross-border transfers of personal data outside of Algeria, after ensuring the recipient country has adequate data privacy measures.
- Data controllers can transfer data across borders to a country without adequate data protection measures in certain cases. For example:
    - If the data subject explicitly provides his consent to the transfer
    - For the performance of a contract between the data subject and the data controller, or pre-contractual procedures on the request of the data subject.
    - Based on receiving a license from the authority for the transfer.

BREACH NOTIFICATION

There is no obligation for a breach notification by the data controller to the regulator or the data subjects.

Bahrain

DATA PROTECTION LEGISLATION

Bahrain enacted Law No. 30 of 2018 with respect to Personal Data Protection (**PDPL**) in July 2018. The PDPL came into force in August 2019.

KEY DEFINITIONS

- Definition of personal data: Personal data is defined under the PDPL as any information of any form related to an identifiable individual, or an individual who can be identified, directly or indirectly, particularly through their personal identification number, or one or more of their physical, physiological, intellectual, cultural or economic characteristics or social identity.
- Definition of sensitive personal data: Sensitive personal data is a subset of personal data. It is personal data which reveals, directly or indirectly, the individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life. Sensitive personal data requires more rigorous treatment by data controllers

AUTHORITY

Under the PDPL, the Personal Data Protection Authority (**Authority**) will have power to investigate violations of the PDPL on its own, at the request of the responsible minister, or in response to a complaint. At the interim, the Ministry of Justice is assuming the responsibilities of the Authority pending the establishment of the latter.

DATA PROTECTION OFFICERS

Data controllers may voluntarily appoint a data protection officer. The Authority's Board of Directors may also issue a decision requiring specific categories of data controllers to appoint data protection officers. However, in all instances, the data controller must notify the Authority of such an appointment within three days of its occurrence.

REGISTRATION

The Authority must create a register of data protection officers. To be accredited as a data protection officer, an individual must be registered in that register.

DATA PROCESSING

Processing of personal data can only occur with the consent of the data subject, unless the processing is necessary:

- to implement a contract to which the data subject is a party;
- to take steps at the request of the data subject to conclude a contract;
- to implement an obligation required by law, contrary to a contractual obligation or an order from a competent court;
- to protect the vital interests of the data subject; or
- to exercise the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject.

Processing of sensitive personal data is also prohibited without the consent of the data subject, except under limited conditions (e.g. is required by the data controller to carry out their obligations, is necessary for the protection of the data subject, etc.)

DATA SUBJECT RIGHTS

- Right of objection to the processing for direct marketing purposes - Right to protest against the process that causes material or moral damages to the information owner or others - Right to protest against the resolutions that are made pursuant to manual processing - Right to protest to claim modification, concealing, and erasing

DATA TRANSFER

- Transfers of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries need to be listed by the Authority and published in the Official Gazette.
- Data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data under certain conditions including: the transfer occurs pursuant to a permission to be issued by the Authority on a case-by-case basis, if the data subject has consented to that transfer, or there is a legitimate and vital interest for the transfer, etc.

BREACH NOTIFICATION

The PDPL contains a general requirement on the data protection officer to notify the Authority of any breach under the PDPL of which that the data protection officer becomes aware.

Morocco

DATA PROTECTION LEGISLATION
Morocco enacted Law No 09-08, in 2009 on the protection of individuals with regard to the processing of personal data.

KEY DEFINITIONS

- Definition of personal data: Personal data is defined as any information regardless of their nature, and format, relating to an identified or identifiable person.
- Definition of sensitive personal data: Sensitive personal data is defined under the law as personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership of the person concerned or relating to his health, including his genetic data.

AUTHORITY
The relevant authority is the Data Protection National Commission - CNDP (*Commission Nationale de Protection des Données Personnelles*).

DATA PROTECTION OFFICERS
There is no requirement for a data protection officer under the Data Protection Law.

REGISTRATION
The processing of personal data is subject to a prior declaration to be filed with the Personal Data Protection Commission, and to the prior authorization of the CNDP when the processing concerns Sensitive data, or Genetic data, or Data including the National Identity Card number, or when using Personal data for purposes other than those for which they were initially collected.

DATA PROCESSING
As a general rule, the processing of a personal data must be subject to the prior consent of the relevant data subject. However, the processing of personal data can be performed without the consent of the relevant data subject provided that the information relates to the:

- Compliance with a legal obligation.
- Execution of a contract to which the relevant data subject is party or in the performance of pre-contractual measures taken at the request of the latter.
- Protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent.
- Performance of a task of public interest or related to the exercise of public authority.
- Fulfillment of the legitimate interests pursued by the person in charge of the processing or by the recipient.

DATA SUBJECT RIGHTS

- Right to be informed at the time of data collection.
- Right to not receive direct marketing without consent.
- Right to restriction, correction, or deletion of personal data.
- Right to request access to their personal data and related information about how/why it is being processed.
- Right not to be subject to automated decision making.

DATA TRANSFER

- Prior authorization from the National Commission is required before any transfer of personal data to a foreign state. Further, the person in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject, unless
    - The data subject has expressly consented to the transfer
    - The transfer and subsequent processing is required for any task highlighted under the exemptions listed in the “Data Processing” section

BREACH NOTIFICATION

The law does not set out any obligation to notify the CNDP or the concerned individual in the event of a data security breach.

Qatar

DATA PROTECTION LEGISLATION
Qatar has implemented Law No. (13) Of 2016 Concerning Personal Data Protection. The Data Protection Law provides that each individual shall have the right to privacy of their personal data.

KEY DEFINITIONS

- Definition of personal data: Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.
- Definition of sensitive personal data: Sensitive personal data means personal data consisting of information as to a natural person's ethnic origin, health, physical or mental health condition, religious beliefs, relationships, and criminal records.

AUTHORITY
Qatar Ministry of Transport and Communications (MoTC).

DATA PROTECTION OFFICERS
There is currently no obligation for organizations in Qatar to appoint a data protection officer. There is an obligation on the data controller to specify processors responsible for protecting personal data, train them appropriately on the protection of personal data and raise their awareness in relation to protecting personal data.

REGISTRATION
There are currently no registration requirements in Qatar.

DATA PROCESSING
The data controller is free to process data without the consent of the data subject in the following circumstances:

- Executing a task related to the public interest as per the law.
- Implementing a legal obligation or an order rendered by a competent court.
- Protecting vital interests of Individual.
- Achieving purposes of scientific research which is underway for public interest.
- Gathering necessary information for investigation into a criminal offense, upon an official request of investigative bodies.

DATA SUBJECT RIGHTS

- Withdraw consent to the processing of their personal data.
- Object to certain processing activities.
- Issue requests for the deletion or correction of their personal data.
- Request access to their personal data and related information about how/why it is being processed.
- To be notified when any inaccurate data may have been disclosed in relation to them.

DATA TRANSFER

- Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realizing a 'lawful purpose' for the controller or for the third party to whom the personal data is sent.
- Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines 'trans-border data flow' as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

BREACH NOTIFICATION

- Controllers should report the personal data breach to the Compliance and Data Protection (CDP) Department at Ministry of Transport and Communications without delay and within 72 hours of becoming aware of it, if the personal data breach could cause damage to individuals' personal data or privacy.
- Controllers should notify the individuals of the personal data breach without delay and within 72 hours of becoming aware of it if the personal data breach could cause serious damage to their personal data or privacy.

Tunisia

DATA PROTECTION LEGISLATION

Law n° 2004-63 dated July 27, 2004, on the Protection of Personal Data, regulates personal data.

KEY DEFINITIONS

- Definition of personal data: Personal data is defined as all information regardless of their origin or form and which directly or indirectly allows to identify or make identifiable a natural person, with the exception of information related to public life or considered as such by law.
- Definition of sensitive personal data: There is no clear definition of sensitive personal data, but the law listed some personal data the processing of which is either prohibited, or would question the data subject's prior consent or the national authority's authorization. Such as; criminal history and proceedings, criminal prosecution, penalties, preventative measures or judicial history, in addition to data concerning racial/genetic origins, religious beliefs, political opinions, union/philosophical activism, health and scientific research.

AUTHORITY

The National Authority for Protection of Personal Data (the Instance) was created by Decree n° 2007-3003 of November 27th, 2007.

DATA PROTECTION OFFICERS

Under Tunisian law, there is no reference to Data Protection Officers.

REGISTRATION

Any processing of personal data shall be subject to a prior declaration filed at the headquarters of the National Authority for Protection of Personal Data, or by any other means leaving a written record.

DATA PROCESSING

Among the main prerequisites for the legitimate processing of personal data is the informed consent of the data subject, which means that the processing of personal data cannot be carried out without the express and written consent of the data subject. This consent shall be governed by the general rules of law if the data subject is incompetent or unauthorized or incompetent to sign.
Additionally, and in the spirit of child protection, Tunisian law has provided extra protection to personal data relating to children as this kind of data cannot be carried out without the consent of the child's agent and after authorization of the juvenile and family court judge.

DATA SUBJECT RIGHTS

- The right to consent and to withdraw consent in regards to processing of personal data.
- The right of access of the data subject.
- The right to object to the processing of personal data related to the data subject.

DATA TRANSFER

- The transfer of personal data is generally prohibited or subject to strict measures, including prior authorization (submitted to the National Authority for Protection of Personal Data), and the explicit consent of the person in question, which is mandatory.

- The international transfer of personal data may not take occur if the foreign country does not provide an adequate level of protection. In every case, the authorization of the Instance is required before the transfer of personal data.

BREACH NOTIFICATION

There are no breach notification obligations prescribed by the Law.

Annex (II) - Personal Data

A. Customers' Data:

1. Names:
   a. Full Name
   b. Mother's name
   c. Alias (aka)
2. Personal Identification Numbers:
   a. National or Social Security Number (e.g. SSN)
   b. Passport Number
   c. Residence Permit Number
   d. Visa Permit Number
   e. Driver's License Number
   f. Taxpayer Identification Number (TIN)
   g. Other Government Identification Numbers
3. Personal financial data:
   a. Account Number or Customer ID Number (unique identifying number)
   b. Safety Deposit Box Number
   c. Credit/Debit Card Number
   d. IBAN
   e. Personal Identification (PIN). Codes used to authorize electronic use of a financial transaction card
4. Personal address information:
   a. Home Address
   b. Mailing Address (P.O. Box/zip code)
   c. Electronic Mail Name or Address
   d. IP Address
5. Personal Telephone Numbers:
   a. Home Telephone Numbers
   b. Mobile Telephone Numbers
6. Biometric data - **Special Category / Sensitive Data**
   a. Finger Vein Recognition - **Special Category / Sensitive Data**
   b. Digital Signatures
   c. Facial Geometry - **Special Category / Sensitive Data**
   d. Photographic Images (particularly of face or other identifying characteristics)
7. Internet account numbers, or Internet identification names:
   a. Login Names

b. Social Media IDs (e.g. Facebook, Tweeter, LinkedIn)

8. Vehicle Information:
   a. Vehicle registration number
   b. Vehicle license plate number

B. Employees

1. Biographical data
2. Radio frequency identification (RFID) data (access card/badge) - **Special Category / Sensitive Data**
3. Security clearance
4. Financial information
5. Criminal record - **Special Category / Sensitive Data**
6. Home address
7. Grievance information - **Special Category / Sensitive Data**
8. Disciplinary records
9. Leave-of-absence reason
10. Payroll and benefits information
11. Employment information
12. Educational information
13. Health information - **Special Category / Sensitive Data**

Annex III. MENA FCCG Privacy and Data Protection Assessment Questionnaire

Refer to MENA FCCG website / Compliance Tools at:

http://menafccg.com/publications/

About MENA FCCG

MENA FCCG is a voluntary body that seeks to bring collective action in the fight against money laundering and terrorist finance in the region. The group comprises 13 banks from nine MENA countries, including; Bahrain, Egypt, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia and the UAE.

www.menafccg.com
Send inquiries to:info@menafccg.com