مصرف قطر المركزي
Qatar Central Bank
State of Qatar • دولـــة قطـــر

Data Handling and Protection Regulation

Regulating the use, storage and processing of data by QCB-regulated Financial Institutions

Contents

PART A: General Provisions

1. Definitions

#	Term	Definition
1	(Semi-)Autonomous Decision-Making Systems	Computational systems, algorithms, or technologies that use data processing capabilities to make decisions or perform actions, either independently (autonomous) or with limited human oversight (semi-autonomous), impacting outcomes related to individuals or entities.
2	Bank Secrecy	As defined in QCB Law.
3	Data Breach	An incident where sensitive, confidential, or protected data is accessed, disclosed, or stolen by unauthorized individuals.
4	Data Privacy Breach	An incident where personal information is accessed, disclosed, or used by an authorized individual in ways that exceed their legitimate permissions or for purposes that are unauthorized, unethical, or illegal.
5	Data Mapping	A process of identifying, cataloguing, and documenting the flow of data within an organization. It involves creating a detailed representation of how data is collected, stored, processed, transferred, and shared across systems, applications, and stakeholders.
6	Data Privacy Officer (DPO)	An employee of a Financial Institution who guides the organization towards adequately protected and compliant operations in matters concerning the Financial Institution processing of personal data according to the applicable laws and regulations.
7	Data Processing	Any process performed on data by a Financial Institution, including but not limited to collecting, transferring, storing, modifying, using, erasing and destroying data.
8	Data Subject	An individual whose Personal Data is collected, processed, or stored by a Financial Institution.
9	External Privacy Policy	A publicly available document that outlines how a Financial Institutions collects, uses, stores, and protects personal data of external parties, such as customers, clients, and website visitors. It is intended to comply with legal and regulatory requirements while informing individuals about their rights and the organization's data handling practices.
10	Financial Institution	An organization regulated by Qatar Central Bank.
11	Internal Privacy Policy	A document designed for use within a Financial Institution to guide employees, contractors, and other internal stakeholders on handling data in compliance with applicable laws, regulations and the organization's standards. It serves as an operational guideline for ensuring data privacy and security.
12	Personal Data or Personal Information	Any information that relates to an identified or identifiable individual, including direct identifiers (like names and ID numbers) and indirect identifiers (like IP addresses, email addresses, or location data).
13	Personal Identifiable Information (PII)	Personal Data that can uniquely identify a Data Subject, such as names, ID numbers, or contact details. This information can directly or indirectly identify a Data Subject.
14	Privacy Impact Assessment	A process undertaken by a Financial Institution in order to establish purposeful processing, retention, and access controls on a process level. The aim of this exercise is to evaluate how a process or system might impact the privacy rights of Data Subjects.

15	Qatar-Based Systems	Systems that Financial Institutions utilize within the Qatar Central Bank Network. These include but are not be limited to: NAPS, QIPS, QMPS, ECC.
16	QCB Law	Law of the Qatar Central Bank and the Regulation of Financial Institutions No. (13) of 2012.
17	Record of Processing Activities (ROPA)	A documented inventory detailing how a Financial Institution collects, processes, stores, and shares personal data, inclusive of PII and SPI.
18	Sector-Specific Security Regulation	QCB Information Security regulations that are applicable to Financial Institutions from a specific subsector within the financial sector in Qatar.
19	Sensitive Financial Information (SFI)	Data that is financial in nature and is associated with a specific customer. This includes but is not limited to: credit card information, account information, transactions, loans and credit scores. Sensitive Financial Information must be classified as per a Financial Institution's highest classification tier.
20	Sensitive Personal Information (SPI)	Personal data that, if disclosed, misused, or accessed without authorization, could result in harm to a Data Subject, including but not limited to financial loss, identity theft, reputational damage, or personal distress. The Qatar Personal Data Privacy Protection Law refers to this as "Personal Data of a Special Nature".
21	Technical Information	Data generated by digital systems that are confidential in nature that include: user credentials, network logs, system logs, application logs and security logs.
22	Third Party	Any organization that is storing, processing, transmitting or handling data on behalf of a Financial Institution.

2. Introduction

As data is a cornerstone of financial operations, the secure handling and protection of sensitive information is a critical activity financial institutions must undertake. The financial sector operates within a highly interconnected ecosystem, where vast volumes of data are generated, processed, and shared daily. From personal customer details to market-sensitive information, the stakes for safeguarding data integrity, confidentiality, and availability are exceedingly high.

The QCB Data Handling and Protection Regulation serves as a comprehensive framework to address these challenges. It is designed to establish clear requirements for the collection, processing, storage, and transmission of data, ensuring alignment with global best practices and compliance requirements. This regulation seeks to safeguard Financial Institutions and the public from the risks associated with data breaches and cyberattacks and also aims to enhance the sector's resilience against emerging threats.

3. Scope

This regulation applies to all Financial Institutions under the supervision of the Qatar Central Bank (QCB) and encompasses all data managed by these institutions. Requirements specified with the verb "must" are obligatory, while those stated with the verb "may" are advisory.

Additional details regarding exemptions applicable to certain Financial Institutions are outlined in Appendix 1.

4. Organizational Governance

4.1 All data collected, stored, or processed by a Financial Institution or through a Third Party on behalf of a Financial Institution must be handled in accordance with QCB Law, this regulation, the Qatar Data Privacy Protection Law and any other relevant laws and regulations.

4.2 A Financial Institution must establish a dedicated data governance business unit, or assign it to an existing function. This business unit's roles and responsibilities include:

4.2.1 Building a data privacy framework and program in line with the requirements of this regulation, the Financial Institution's risk management framework, and industry leading practices.

4.2.2 Collaborating with relevant functions such as information security, risk management, information technology, compliance, and other relevant functions to ensure the necessary protection controls are in place.

4.2.3 Implementing the organization's data privacy policies in coordination with the relevant departments.

4.2.4 Assessing the sufficiency of mitigation controls and working with the relevant departments to implement the controls.

4.2.5 Reporting on matters pertaining to data privacy and its protection to the Data Privacy Officer (DPO).

4.3 A Financial Institution may establish a data governance committee with representation from senior management, risk, information technology, information security, legal and compliance as well as other relevant functions. Such a committee may engage in tasks including:

4.3.1 Reviewing data privacy and protection risks.

4.3.2 Reviewing risk mitigation strategies.

4.3.3 Reviewing Financial Institution's overall posture in data privacy and protection.

4.4 A Financial Institution must appoint a Data Privacy Officer (DPO) who possesses the necessary knowledge and experience in data privacy, notifying QCB of the appointed DPO and submit the required Fit and Proper Form as per QCB Licensing Regulations.

4.4.1 A Financial Institution may appoint a DPO to an existing role, ensuring that it is independent of conflicts of interests and operate independently without being directed in the performance of their tasks.

4.4.2 A Financial Institution must ensure that the DPO is not involved within Financial Institution operations.

4.4.3 A Foreign Financial Institution may appoint a DPO based within their headquarters, ensuring that a Qatar-based representative is assigned responsibility to liaise and facilitate in order to ensure data privacy and protection requirements are met consistently.

4.5 A Financial Institution must ensure its DPO's roles and responsibilities include:

4.5.1 Assessing the Financial Institution's compliance to data privacy and protection requirements as per relevant laws and regulations.

4.5.2 Advising business units on matters pertaining to data privacy and its protection.

4.5.3 Reporting on the Financial Institution's data privacy activities and compliance status to the CEO or the most senior management position.

4.5.4 Liaising between regulators and the Financial Institution in matters pertaining to data privacy and its protection.

4.6 A Financial Institution must ensure its DPO reports directly to the CEO or the most senior management position, who must ensure data privacy and protection risks are communicated to the board.

4.7 A Financial Institution must provide the required training and awareness to promote skill development for its employees and relevant stakeholders to ensure that they regularly update their knowledge of data privacy and management, data classification, data handling, data cataloguing, data stewardship, data backup up, disaster recovery, etc.

5. Framework, policies and procedures

5.1 A Financial Institution must establish an internal data governance policy that applies to all their business processes and operational procedures to ensure proper handling in the collection, classification, security, integrity, storage, retention, access, use, transfer and destruction of data throughout its lifecycle.

5.2 A Financial Institution must ensure that its data governance policy includes:

5.2.1 Identification of all relevant laws and regulations the Financial Institution must adhere to.

5.2.2 Identification of all data processed within the organization.

5.2.3 Maintenance of a data catalogue and associated processes.

5.2.4 Data classification.

5.2.5 Data mapping exercises.

5.2.6 Assessments as per section (10) of this regulation.

5.2.7 Data process ownership.

5.2.8 Data masking standards.

5.2.9 Data retention guidelines.

5.2.10 Data security policy and procedure.

5.2.11 Third Party data protection controls.

5.2.12 Secure data transfer procedures.

5.2.13 Roles and responsibilities for functions and personnel associated with data privacy and protection.

5.3 A Financial Institution must assess requirements of leading data governance standards, while ensuring they maintain compliance with the requirements of this regulation.

5.4 A Financial Institution must publish its External Privacy Policy statement on externally hosted channels, to the extent necessary, informing customers of their rights and how their data will be collected, accessed, processed, shared and retained.

5.5 A Financial Institution must publish its Internal Privacy Policy in an easily-accessible and context-specific manner, to the extent necessary for all staff involved.

5.6 A Financial Institution must develop data mapping procedures to define data assets and their paths through the entities' processes.

5.7 A Financial Institution must establish consent procedures for customer data processing that aligns with processes and technologies utilized within the Financial Institution.

5.8 A Financial Institution must define specific destruction guidelines for data and hardware that has reached the end of its retention period.

5.9 A Financial Institution must align its business continuity plans, disaster recovery plans and backup strategy with the requirements of this regulation and their data governance frameworks, policies, and procedures.

5.10 A Financial Institution must ensure it identifies risks associated with data privacy and the mitigating controls.

5.11 A Financial Institution must maintain a detailed inventory of all assets within its processing environment, including Third Party assets, mapped to its critical processes and services.

6. Data Classification Framework

6.1 A Financial Institution must develop and maintain a data classification policy based on industry leading practices, which includes Financial Institution-wide responsibilities for classifying data.

6.2 A Financial Institution must develop and maintain a data handling guideline that details how to handle data of different classifications. A Financial Institution may utilize the National Cyber Security Agency's National Data Classification Policy.

6.3 A Financial Institution must define the following for each classification level: classification definition, data examples, storage requirements, labelling requirements, cybersecurity controls, physical access controls, logical access controls, data masking requirements, transmission requirements and destruction mechanism.

6.4 A Financial Institution must establish a Record of Processing Activities (ROPA), in a single or multiple records, ensuring documentation includes but is not limited to: data type, data source and destination, Data Subject type (employee, customer, etc.), data classification, data process owner, processing purpose, processing basis (consent, legal and regulatory, contract fulfilment), retention period, Sensitivity Flag (SPI, PII, SFI, etc.), PIA required, internal share list, CIA (Confidentiality, Integrity, Availability) rating, security controls, overall risk rating, Third Party access, storage location, storage medium, processing location, and retention period.

6.4.1 A Financial Institution must conduct annual reviews of their ROPA, or conduct reviews that are triggered by changes to the Financial Institution. These changes may include but are not limited to: organizational restructure, new regulatory requirements, changes to the data processing environment, etc.

6.4.2 A Financial Institution may implement tools that automate updates to their ROPA.

6.4.3 A Financial Institution must document and justify any data excluded from the ROPA and detail the associated risks.

6.5 A Financial Institution must conduct Data Mapping to outline all data assets and their flow across organizational processes.

6.5.1 A Financial Institution must review data maps annually, to ensure current and accurate representation of data flows, or conduct reviews that are triggered by changes to the Financial Institution. These changes may include but are not limited to: organizational restructure, new regulatory requirements, changes to the data processing environment, etc.

6.5.2 A Financial Institution must complete Data Mapping exercises for their environments.

6.5.3 A Financial Institution must document and justify any data or processes excluded from the data map and detail the associated risks.

PART B: Data Handling

7. Data Handling

7.1 A Financial Institution must identify data that is Personally Identifiable Information (PII), Sensitive Personal Information (SPI), Sensitive Financial Information (SFI) and Technical Information, as defined in this regulation.

7.2 A Financial Institution must classify data that is PII and Technical Data, as per the Financial Institution's data classification framework.

7.3 A Financial Institution must classify and manage SPI and SFI as per the highest, most strict classification available.

7.4 A Financial Institution must process PII, SPI and SFI only when one of the following conditions (at least) is met:

7.4.1 The Financial Institution has received explicit consent from the Data Subject.

7.4.2 The processing is necessary for a regulatory or legal activity.

7.4.3 The processing is required for contract fulfilment.

7.5 A Financial Institution must put in place a process to remediate previously collected PII, SPI and SFI that does not adhere to requirement 7.4.

7.6 A Financial Institution must ensure its primary environment, the main data storage and processing environment, for PII, SPI and SFI resides within the State of Qatar.

7.7 A Financial Institution may utilize a primary storage and processing environment for PII, SPI and SFI outside the State of Qatar only after receiving explicit approval from QCB.

7.8 A Financial Institution must adhere to Bank Secrecy requirements, especially when processing SFI as per QCB Law and any other relevant laws and regulations.

7.9 A Financial Institution must limit its data collection activities to data it requires to provide services to the customer, or to adhere to legal and regulatory requirements.

8. Data Security

8.1 A Financial Institution must develop robust data quality controls and validation processes to ensure the accuracy and reliability of processed data.

8.2 A Financial Institution must develop dedicated security controls for all data that is classified as PII, SPI or SFI, while applying requirements as per the Sector-Specific Security Regulation to protect it based on criticality and assumed risks.

8.3 A Financial Institution must update its security controls for all data that is classified as PII, SPI or SFI, while accounting for the changing threat landscape.

8.4 A Financial Institution may utilize tools and technologies to operationalize its data classification and management requirements, while ensuring regular testing and patching of the systems and that they are kept up to date. These include but are not limited to: data discovery tools, data classifier tools, data loss prevention (DLP) tools, etc.

8.5 A Financial Institution must review its data classification on regular basis to mitigate risks of misclassification.

8.6 A Financial Institution must transfer its data through secure and encrypted mediums, as per leading industry standards and the Sector-Specific Security Regulation.

8.7 A Financial Institution must use specialized, reputable and secure physical transportation methods, when transporting data on a physical medium such a documents or storage tapes.

9. Third Party Access

9.1 A Financial Institution is subject to the requirements of this section when data is shared with any Third Party, excluding information shared with Qatar Central Bank and any exceptions detailed within the QCB Law.

9.2 A Financial Institution must assess its Third Party's compliance to relevant data protection laws and regulations, as well as any certifications or audit reports.

9.3 A Financial Institution may only share sensitive information with Third Parties they have non-disclosure and confidentiality requirements in place with, dependent on the associated risks.

9.4 A Financial Institution must ensure that any data breaches or data privacy breaches involving its data are promptly reported by the Third Party involved to a designated representative within the Financial Institution.

9.5 A Financial Institution must include provisions for data protection, confidentiality, and compliance with regulatory requirements within its contractual agreements with Third Parties.

9.6 A Financial Institution must collect consent from customers and employees prior to sharing their information with a Third Party, unless this is shared for legal purposes, regulatory purposes, or contract fulfilment.

9.7 A Financial Institution must inform the customer of the impact of not granting consent to information sharing with the Third Party.

9.8 A Financial Institution must ensure its Third Parties handle data in a manner that meets the requirements of this regulation.

9.9 A Financial Institution must implement risk-based data protection controls for data residing in all environments and data hosted by its Third Parties.

10.Assessments and Reporting

10.1A Financial Institution must document a policy mandating ongoing data handling and management assessments including those defined within this section.

10.2A Financial Institution must subject its primary, secondary, Disaster Recovery (DR) and backup environments to the assessments defined within this section.

10.3A Financial Institution must define a process for conducting Privacy Impact Assessments (PIA) for all sensitive processes, in order to test whether privacy objectives are met and to ensure that data processing adheres to processing requirements, retention requirements and appropriate access controls. The process must include:

- 10.3.1 Defining what a sensitive process is and when a PIA is required.
- 10.3.2 Scoping of processes and technologies within the Financial Institution that require a PIA.
- 10.3.3 Defining data and data flows involved.
- 10.3.4 Assessing privacy risks.
- 10.3.5 Developing mitigation strategies.
- 10.3.6 Reviewing the PIA regularly.

10.4A Financial Institution must conduct a PIA in the following cases:

- 10.4.1 Initiating a new activity that involves a sensitive process.
- 10.4.2 Making changes to sensitive processes in existing activities.
- 10.4.3 Observing significant changes to laws and regulations of relevant jurisdictions that may impact Data Subject privacy.

10.5A Financial Institution must review its PIA methodologies for accuracy and relevance and update as needed.

10.6A Financial Institution must establish a foreign data handling assessment that ensures data stored in, passing through or accessible from foreign jurisdictions continues to meet regulatory requirements and data protection standards.

10.7A Financial Institution must monitor changes in the legal and regulatory landscape of foreign jurisdictions to promptly assess and address any potential impact, on ongoing basis, reporting significant findings to QCB.

10.8 A Financial Institution must develop a procedure that defines the mechanisms by which these assessments will be completed. This must include the following:

- 10.8.1 Assessment owner
- 10.8.2 Assessment stakeholders
- 10.8.3 Timeline and Frequency
- 10.8.4 Expected outcomes and recommendations

10.9A Financial Institution must audit its data handling and management activities, and assess its compliance to data protection laws, regulations and leading industry standards as per the Financial Institution's defined audit cycle.

11.Data Retention

11.1A Financial Institution must ensure its retention of different categories of data considers legal, regulatory, and business requirements.

11.2A Financial Institution must comply to data retention requirements specified in the relevant AML / CFT laws and regulations.

11.3 A Financial Institution must retain data as per the following table:

Data	**Minimum Retention Period**
SFI	10 years
Personal Data, PII and SPI	10 years
Technical Information	1 year
All other data	To be defined by the Financial Institution

11.4A Financial Institution must retain data beyond the minimum retention periods defined within 11.3, if the extended data retention is obligated by a legal or regulatory mandate.

12.Disaster Recovery & Business Continuity Backup

12.1A Financial Institution must establish a Business Continuity and Disaster Recovery plan, emphasizing resilient data protection and privacy safeguards. The plan must include:

- 12.1.1 Local and foreign DR and backup requirements
- 12.1.2 Policy and processes for DR and data backup
- 12.1.3 Data retention periods
- 12.1.4 Backup frequency
- 12.1.5 Data storage and destruction processes
- 12.1.6 Defined trigger events
- 12.1.7 Ongoing testing and assessments

12.2A Financial Institution must integrate its disaster recovery plan process into the Financial Institution's overall governance processes and risk management framework. This includes the development, review, approval, monitoring, escalation, activation and implementation of the disaster recovery plan.

12.3A Financial Institution must ensure continuous availability of critical systems and processes through redundancy controls and failover processes which include but are not limited to: conducting real-time or scheduled backups of critical data, ensuring that backup frequency aligns with the criticality and volatility of the data.

12.4A Financial Institution must implement security controls including robust encryption and data security measures for DR and backups, as per the Sector-Specific Security Regulation.

12.5A Financial Institution must define and implement physical access management controls and processes to protect DR and backup data centers, network equipment rooms, storage sites, servers and workstations, in accordance with the Sector-Specific Security Regulation.

12.6A Financial Institution must regularly test its Business Continuity and Disaster Recovery plans.

12.7A Financial Institution must consider any legal, reputational and operational impediments within its disaster recovery plan.

12.8A Financial Institution must assess jurisdictional, legal, regulatory, political, and environmental risks associated with foreign DR and backup locations.

12.9A Financial Institution must remain responsible and accountable for its disaster recovery readiness activities.

12.10 A Financial Institution must develop a disaster recovery communication plan with relevant stakeholders, including QCB, shareholders, employees, key group entities, Third Parties, customers, regulators and the media.

12.11 A Financial Institution must ensure that business continuity is not disrupted by dependencies on outsourcing contracts with Third Party service providers.

12.12 A Financial Institution must maintain its backup and DR environments as per the following table:

	Local Banks & Insurance Companies	**Branches of Foreign Banks & Insurance Companies**	**Other Local Financial Institutions**	**Branches of Other Foreign Financial Institutions**
Local DR	Mandatory	Qatar-Based Systems – Mandatory Other – Recommended	Mandatory	Qatar-Based Systems – Mandatory Other – Recommended
Foreign DR	Optional. However, the QCB reserves the right to direct any Financial Institution to maintain a foreign DR at its discretion			
Local backup	Mandatory	Mandatory	Mandatory	Mandatory
Foreign backup	Mandatory	Mandatory	Recommended	Recommended

12.13 A Financial Institution must request approval from QCB when it utilizes foreign DR and backup environments, in alignment with section 15 below.

PART C: Data Protection and Privacy

13.Data Privacy Protection Requirements

13.1A Financial Institution must ensure that Personal Data, PII and SPI is:

13.1.1 Processed in compliance to the Law No. (13) of 2016 on Personal Data Privacy Protection.

13.1.2 Processed for an explicit and specified purpose.

13.1.3 Processed in accordance with other QCB regulations including KYC requirements.

13.2A Financial Institution must ensure that the systems and controls address the following:

13.2.1 Ensure the confidentiality, integrity and availability of data and information.

13.2.2 Ensure the accuracy and completeness of data and information.

13.2.3 Have appropriate training for its employees in relation to data security, data protection and privacy protection.

13.3A Financial Institution must deploy systems and controls that enable it to identify, assess, monitor and manage data protection risk.

13.4A Financial Institution must assess privacy protection and data protection controls when processing data in a semi-autonomous or autonomous manner.

13.5A Financial Institution must seek approval from QCB prior to processing data and information within fully autonomous decision-making systems.

14.Customer Data Protection

14.1A Financial Institution may process Data Subject information only when one of the following conditions (at least) is met:

- 14.1.1 The Financial Institution has received explicit consent from the Data Subject.
- 14.1.2 The processing is necessary for a regulatory or legal activity.
- 14.1.3 The processing is required for contract fulfilment.

14.2A Financial Institution must establish proper procedures to obtain consent from its customers to collect, access, process, share, and retain data, unless it is necessary for regulatory activity, legal activity or contract fulfilment. Use cases to acquire customer consent include:

- 14.2.1 Sharing customer data with a Third Party.
- 14.2.2 Using customer data for marketing purposes.
- 14.2.3 Using Sensitive Personal Information.

14.3A Financial Institution must periodically review its consent procedures to ensure that consent is freely given, specific, informed and unambiguous.

14.4A Financial Institution must establish the necessary procedures to ensure that customers:

- 14.4.1 Obtain confirmation of whether their personal data is being processed.
- 14.4.2 Access a copy of the data along with information about the processing in a structured, commonly used, and machine-readable format.
- 14.4.3 Request correction or completion of their data.
- 14.4.4 Request the restriction of processing incorrect or inaccurate personal data.
- 14.4.5 Request the deletion of their data, ensuring that it aligns with data retention requirements defined in this regulation. The Financial Institution shall establish a policy for data deletion that considers the following conditions:
  - 14.4.5.1 Deletion will not impact the overall business continuity of the Financial Institution.
  - 14.4.5.2 Deletion will not impact the contract fulfilment a customer has agreed to.
  - 14.4.5.3 Deletion will not impact the Financial Institution's legal and regulatory requirements.

14.5A Financial Institution processing information associated with a minor must verify that the person giving consent, holds parental responsibility "legitimate interest" for the minor.

14.6A Financial Institution must define rejection use cases for requests made as per requirement (14.4), whilst maintaining the right to reject the requests.

14.7A Financial Institution may define a process for expiring consent and consent renewal, if required by certain activities undertaken by the financial institution.

14.8A Financial Institution must ensure that the customer has the right to refuse and withdraw consent at any time, except where processing is necessary for legal and regulatory obligations or contract fulfilment.

14.9A Financial Institution may establish a consent management portal for customers to view and update the consent they have granted a Financial Institution.

14.10 A Financial Institution must maintain a record of the consent granted including but not limited to the following:

14.10.1 Purpose of Data Processing.

14.10.2 Identity of the person giving consent.

14.10.3 Consent Date.

14.10.4 Consent method.

14.10.5 The External Privacy Policy in force at the time consent was given.

14.10.6 Any documents or forms containing information provided by the consenting party.

14.11 A Financial Institution must inform the customer of the impact of not granting or withdrawing consent on the provision of services to the customer.

15.Foreign Data Storage and Transfer Requirements

15.1A Financial Institution must not store or transfer Personal Data, PII, SPI and SFI to a foreign jurisdiction unless it has received approval from QCB.

15.2A Financial Institution must conduct due diligence on jurisdictions and Third Parties that would require foreign data transfers or storage, which includes but may not be limited to:

15.2.1 A risk assessment which includes risks associated with data security and storing data in foreign jurisdictions.

15.2.2 An examination of the legal and regulatory framework governing data protection and privacy in the foreign jurisdiction.

15.3A Financial Institution must establish mechanisms to control access to data stored in the foreign jurisdiction, including procedures for granting and revoking access, monitoring user activity, and detecting unauthorized access or data breaches.

15.4A Financial Institution must ensure at all times that any transfer of personal data to a foreign jurisdiction maintains an adequate level of protection in accordance with the standards defined within this regulation and any other relevant laws and regulations.

15.5A Financial Institution must identify risks associated with operational processes and systems at separate geographic locations.

15.6A Financial Institution must assess the legal and regulatory requirements of foreign jurisdictions where they process data that may restrict a Financial Institution’s ability to meet regulatory obligations in Qatar.

16.Data Breaches

16.1A Financial Institution must report Data Breaches and Data Privacy Breaches as per QCB's incident reporting guidelines.

16.2A Financial Institution must classify any Data Breach or Data Privacy Beach as an incident and adhere to incident reporting guidelines as directed by the QCB.

16.3A Financial Institution must report Data Breaches and Data Privacy Breaches to QCB and the authorized agencies in Qatar which includes the National Cyber Security Agency and the Ministry of Interior.

16.4A Financial Institution must assess the impact of the breach, upon identification.

16.5A Financial Institution must assess the need to report a breach to its customers.

16.6A Financial Institution must trigger action from relevant stakeholders, including employees and customers, to circumvent potential impact of the breach.

17. Exemptions

17.1A Financial Institution seeking an exemption from any requirement within this regulation must request it from QCB. All exemptions are subject to QCB approval.

17.2A Financial Institution must link its exemption request to a specific requirement in this regulation from which it is seeking a waiver.

17.3A Financial Institution must support its exemption request with a clear and documented business case or rationale.

17.4A Financial Institution must ensure that the appropriate individuals or levels of authority within the Financial Institution consistently approve the exemption.

17.5A Financial Institution must duly record in the Financial Institution's exemptions register any approved exemptions and assign an expiration date – the date by which the exemption will be mitigated or resolved by the Financial Institution seeking the exemption.

17.6A Financial Institution must remain accountable for any risks stemming from approved exemptions.

PART D: Other Regulations

18.Compliance with Secondary Regulations

Along with the QCB Law and this regulation, the Financial Institution must also comply with the below mentioned secondary regulations, and their subsequent amendments, while operating in Qatar:

18.1Sector-Specific Security Regulation.

18.2Cloud Computing Regulation.

18.3AI Guideline.

18.4Regulations or Guidelines that may be issued by QCB, including those related to emerging technology.

18.5Law No. (13) of 2016 on Personal Data Privacy Protection.

Appendix 1: General exemption of requirements to Financial Institutions by Subsector

This table defines the requirements that are not mandatory for all Financial Institutions. QCB strongly recommends that all Financial Institutions adhere to all requirements. However, QCB is offering a degree of flexibility to some Financial Institutions.

The following table lists the requirements that may be considered as recommendations by certain financial institutions.

	Banks & Insurance Companies	**Exchange houses, FinTech Companies, Finance Companies, Investment Companies, Insurance Brokers**
Section 4	None	None
Section 5	None	5.2, 5.6
Section 6	None	6.4, 6.5
Section 7	None	None
Section 8	None	None
Section 9	None	None
Section 10	None	10.3, 10.4, 10.5
Section 11	None	None
Section 12	None	None
Section 13	None	None
Section 14	None	None
Section 15	None	None
Section 16	None	None
Section 17	None	None