



Group Data Privacy Policy

TABLE OF CONTENT

1. DOCUMENT CONTROL SHEET.....2

2. OUR COMMITMENT.....3

3. PURPOSE & SCOPE.....3

4. DATA COLLECTION 3

5. DATA REQUEST BY COMPETENT AUTHORITY 4

6. DATA PROTECTION.....4

7. COMPLIANCE & REPORTING 5

8. POLICY IMPLEMENTATION, AMENDMENT AND REVIEW 5

1. DOCUMENT CONTROL SHEET

Creation Date:	Document Owner:
Department:	Current Version Number:

Revision Record			
Date	Version	Revised by	Description of Change

Review Record				
Date	Version	Reviewed by	Title	Signature

Distribution		
Version	Name	Location

Approvals		
Name	Designation	Signature

2. OUR COMMITMENT

Ooredoo Group is committed to maintaining and improving information security within accepted best practice and minimizing its exposure to risks in order to protect Ooredoo assets and stakeholders across all of Ooredoo Group operations. Ooredoo Group commits to protect its customers' privacy and keeping their personal data safe based on applicable data protection laws and regulations.

This privacy statement has been created to help customers understand how we collect, use, share and protect information.

3. PURPOSE & SCOPE

The scope of this policy is to define our procedures in respect of maintaining the confidentiality, integrity and security of all personal data collected and stored by us through any communication channel. Access to all Ooredoo policies and ethical guidelines are provided to all Ooredoo Group employees. All employees are provided with training to reinforce their understanding and implementation of data privacy and security measures.

This policy applies to all sectors and business units in Ooredoo Group. All Company staff and contractors working either on a permanent or temporary basis are fully responsible for implementing and maintaining this policy throughout the company.

4. DATA COLLECTION

The kind of information Ooredoo collects from customers are the following:

- Personal identification information given to the Company during registration, such as name, national ID number, passport number, address, email, nationality and gender;
- Credit or debit-card information, or other payment information;
- History of customer contact with the Company such as through emails, call center, customer care center;
- Usage information such as time and duration of usage, data usage, incoming or outgoing phone calls;
- Information the Company gets from customer use of services or websites (such as IP address, operating system, browser type, the URLs of the pages you visit on the website, and when the service was used.)

Data must only be collected when there is a legitimate business purpose that is aligned with the strategic intent of the Company. Owner approval has to be obtained when data is requested and collected.

The collected information is used for:

- The processing of services, such as orders and payments;
- Meet Ooredoo legal and regulatory requirements;
- Carrying out market and product analysis and marketing our products and services;

- Offers of new products and services that are relevant to the customer;
- Dealing with requests, enquiries or complaints and other customer care related activities;
- Evaluating our products and services performance;
- Providing protection by confirming identity.

5. DATA REQUEST BY COMPETENT AUTHORITY

Ooredoo is subject to the legal and regulatory requirements, in which it operates and therefore must respond to the requirements of the competent authorities related to information of its customers. If necessary, or following a request of the relevant public authority, we may then keep and give to the relevant authority additional information within the legal framework of the law of Qatar. Ooredoo implements a strict procedure that guarantees both compliance with our obligations regarding collaboration with competent authorities and the protection of the rights to privacy and freedom of expression of the affected parties. Ooredoo will periodically review information about the numbers and types of requests it received from competent authorities.

6. DATA PROTECTION

Ooredoo will implement the necessary actions to ensure that the information it collects and stores is lawfully handled. The collected personal information will be used for authorized purposes and will not be processed for other purposes. Thus, the Company has instituted security measures for providing an appropriate level of security aligned to the nature of the data being processed. As part of the Company's efforts to maintain data privacy and security, the following measures are to be followed:

- Adopting ISO 27001 certified for information security management;
- Adopting ISO 20000-1 certified for information technology service management systems (SMS);
- Providing regular training and awareness initiatives for all employees to guarantee a culture of compliance to internal privacy and security regulation;
- Deploying security controls such as identity authentication, regular network risk assessment and updates, stringent monitoring and detection systems;
- Reporting on data breaches in its annual reporting;
- Carrying out regular cyber-security stress test to measures its performance in all areas of cybersecurity;
- Conducting reviews to this policy and subordinate procedures and standards at least annually or when major changes occur to the Company's or its environment occur to ensure their continuing suitability, adequacy and effectiveness;
- Ensuring that processed data is only shared with authorized users and systems to prevent data misuse. Shared data (both internally and externally) shall not have any linkage to personal identity to the Company's customers;
- Periodically carrying out internal and external audits on its data processing systems.

7. COMPLIANCE & REPORTING

Refusal or any attempted violations of this policy will result in an internal investigation and may lead to disciplinary action being taken. Further or repeated non-compliance can be ground for more stringent measures, such as fines, legal prosecution and/or termination, depending on severity.

Ooredoo's employees must immediately report to their immediate manager in case any breach or suspected breach of this policy has been identified. Kindly refer to Whistleblowing Policy for further reference.

8. POLICY IMPLEMENTATION, AMENDMENT AND REVIEW

This Policy supersedes all previous releases (policy, circular, memos, instructions or any other form) on the subject matter and shall come into effect from the date of signing. Any amendment of this Policy shall be preliminarily approved by the ARC and submitted for review and further approval by the Board.