Ooredoo Palestine

Data Privacy Policy

Table of Contents

1. Definitions

For the purposes of this Policy, the following words and expressions shall, unless the context otherwise requires, have the below meaning:

OP, Ooredoo Palestine, The Company	Wataniya Palestine Mobile Telecommunications (Ooredoo Palestine)
Data Privacy	The protection of personal and sensitive data and information from disclosure, unauthorized access, unauthorized use, alternation, and destruction.
Customer	Any legal and/or natural person that receives products and/or services from Ooredoo Palestine (including, without limitation, to all recent, future, and potential customers).
Personal Data	Any data/information relating to an identified or identifiable person, it also includes data/information, once collected, relates to an identified or identifiable person. Personal Data shall not include any data that has been rendered anonymous and of which a person cannot be identified.
MTIT	The Palestinian Ministry of Telecom and Information Technology or any other entity that serve as a regulator.
Information Security Unit	The unit that coordinates the ISSC agenda, minutes of meetings, and action items, as well as owns OP IS policies.
Personal Data Breach/Incident/Privacy Incident	A security breach that leads to the accidental, unlawful, or unauthorized access, use, disclosure, interception, loss, or destruction of Personal Data.
Cookie	A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.
Incident Handling and Response Team	A group of experts tasked to respond and investigate any Incident and/or Personal Data Breach quickly and effectively. Their primary goal is to investigate and mitigate the impact of Personal Data Breaches and/or Incidents.
Information Security Steering Committee (ISSC)	It is a committee that consist of OP CEO, CTO, HR, Corporate Services director, ERM, and General Counsel to oversight and review all information security related matters, risks, protection, and mitigation. Structure, rules and responsibilities of the committee are defined within ISSC charter.

Integrity	Ensuring that information is complete and accurate to its original purpose
Availability	Ensuring that information is available/accessible to those who need them, and when they are needed.
Separation of Duties (SOD)	No user shall be given privileges to misuse Ooredoo Palestine services, products, or systems on their own.
User Authority Matrix (UAM)	An important tool that manages access rights to systems and sensitive data.

2. Purpose

Ooredoo Palestine is committed to respect Personal Data, and to comply with all related applicable laws. This policy is intended to set out the measures taken by Ooredoo Palestine towards the protection of Personal Data and is designed to inform the concerned parties about the data Ooredoo Palestine collects, uses, discloses, and processes data.

3. Scope

3.1. This policy applies to any transaction that may involve the collection and processing of Personal Data occurring between Ooredoo Palestine and its Customers, Employees, Partners, or Third Parties including, without limitation, all products, and services Ooredoo Palestine provides now and may provide in the future and using any of Ooredoo Palestine's channels. The collection and processing of data shall be for the purpose of providing the requested services/products, and to develop and improve the services/products as necessary.

3.2. This Policy applies to all Customers, Ooredoo Palestine employees, and all relevant external parties conducting business with Ooredoo Palestine regardless of their geographical locations.

3.3. The ISSC shall be the committee responsible for the implementation of this Policy, review and update as necessary.

4. Governance

- Ooredoo Palestine has adopted a governance model that aims to protect Personal Data, Data Privacy, and information security. Such model provides sufficient resources and expertise to control and manage this process. The model consists of three key actors, and the structure has been designed to ensure the sufficient resources, policies, and controls required to handle and protect Personal Data. The model consists of the Information Security Steering Committee ISSC, Corporate Information Security Function, and Technical Team (namely, the Security Team, Physical Safeguards, and Incident Handling and Response Team).
- OP shall develop data governance framework policy to ensure that Ooredoo Palestine's internal procedures for processing Personal Data comply with the provisions Law by Decree No. 15 for the year 2017 on Electronic Transactions, Law by Decree No. 10 of 2018 on

Cybercrimes (as amended by Law by Decree No. 38 for the year 2021), and Cabinet Resolution No. (3) for the year 2019 one the Personal Data of Citizens

4.1. Information Security Steering Committee (ISSC)

Information Security Steering Committee (ISSC) is responsible for reviewing all matters related to Personal Data, Data Privacy and information security, including, all related risks, protection, and mitigations. The ISSC has the full responsibilities and powers set to manage and handle all aspects of Personal Data, data privacy and information security within Ooredoo Palestine, and shall be responsible for providing strategic directions to the employees/staff.

In fulfilling its responsibilities, the ISSC shall endeavor to maintain free and open communication between its members.

4.2. Information Security (IS) Unit

Ooredoo Palestine has an Information Security Unit that handles and monitors the compliance and implementation of IS policies and conducts frequent reviews on the systems that may contain any Personal Data. The frequency of these are identified within IS policies. reviews may be conducted quarterly, semi-annually, annually.

The Corporate IS function also aims to reach the right User Authority Matrix (UAM) and the Segregation of Duties (SoD), and to ensure the highest security measures are adopted on the critical systems that may contain any Personal Data.

4.3. Technical Teams

Technical Team handles all Personal Data privacy and security, it consists of multiple teams, namely, the Security Team, Physical Safeguards, and Incident Handling and Response Team, these teams work together to implement the security controls and measures outlined in the information security policies and procedures.

4.3.1 Security Teams

Ooredoo Palestine prevents unauthorized access to the information it collects through having technical and administrative experts. These technical experts, specialize in cyber security, are responsible for the security systems that prevent the unauthorized access to the information, and to ensure that the environment and infrastructure are safe against any cyber-attack. To achieve this, OP must comply with information security policies that identify several information security controls to improve the preventions of unauthorized access and Personal Data Breach, and the Security Team is responsible for assigning specialized vendors/third parties to conduct security checks on Ooredoo Palestine's products and services.

4.3.2 Physical Safeguards

Ooredoo should set controls based on physical and environmental security policy in order to prevents the unauthorized physical access to the information that it collects through having Physical Safeguards in place. Protecting Personal Data is one of the top priorities

at Ooredoo Palestine. Thus, the employees should be trained on the significance of that protection, and on the appropriate access to the information channels.

4.3.3 Incident Handling and Response Team

Ooredoo Palestine maintains security and incident response plans to handle incidents involving in Personal Data Breach and information security which may hinder Confidentiality, Integrity, and availability of data.

5. Personal Data collected by Ooredoo Palestine

5.1 Personal Data include but not limited to the following:

- Customers submits/writes/discloses using Ooredoo Palestine's forms, including data given/inserted when registering to use any Ooredoo Palestine's websites, stores, mobile applications, products, services, requesting, applying for, or enrolling in any service (including, but not limited to, competitions and contests), contacting us, or reporting a problem. Personal Data may, without limitation, include data such as the Customer's name, identification number, address, phone number, and email address.
- Employees' data, such as payroll information, bank accounts, health Insurance Information, performance records, contracts, and personal contact information details. Partners and third parties that might have access to sensitive data, or their data might be processed by OP such as contract details, bank accounts, contact information, systems, and IT environment.

5.2 Ooredoo Palestine shall have the right to retain and store a full record of Customers, Employees, partners, and third-party communications and information in transactions they conduct through Ooredoo Palestine websites, applications, execution of orders, all information about view/visit/activities at Ooredoo Palestine's sites including, websites, applications, and stores and the materials they view and/or download.

5.3 Account Information

The concept of data minimization should be implemented, Ooredoo Palestine should collect the needed information only.

Ooredoo Palestine collects Personal Data and information to enable its customers, Employees, Partners, or Third Party to establish an account with Ooredoo Palestine. Such data may be collected at any Ooredoo Palestine's stores, websites, applications, retail outlets, over the phone or online, or by any of Ooredoo Palestine's teams such as, without limitation, direct sales, tele-sales, marketing, customer services, Procurement, HR, IT.

Account Information includes All types of personal data such as name, address, contact information, ID and/or license number, any other local governmental ID or passport information, company registration number (if applicable and for B2B purposes), relevant authorization documents, and payment information.

All above data are used to verify the Customer's identity, and to comply with applicable laws.

5.4 Service and device usage information.

Ooredoo Palestine collects Personal Data and information regarding Customer's actions/behaviors once they visit Ooredoo Palestine's stores, websites, use its products and/or services, applications, phone calls, and the used devices information. Such information is collected to manage Customer's services, prepare accurate billing statements, improve Customers' experiences, inform Customers about any updates, special promotions and/or communicate offers regarding its products and services.

5.5 Performance and diagnostic data

Ooredoo Palestine collects information about the network performance through Users and customers usage. For instance, Ooredoo Palestine inspects signal strength, calls and data failures, and other technical issues, it further, exploits/uses this information for network planning enhancement, engineering, technical support, quality assurance, and services functionality improvement.

6. Data Processing

6.1 Ooredoo Palestine process and utilizes Personal Data to enhance its services and/or products to achieve its objectives, which include but not limited to:

- Sustaining and enhancing current services and/or products.
- Innovating and introducing new services and/or products.
- Delivering personalized services and/or products.
- Evaluating performance metrics.
- Engaging in communication and managing the relationship with other parties such as customers, employees, and third party.

6.2 Marketing and promotions

All marketing promotions at Ooredoo Palestine are conducted in accordance with applicable laws.

6.3 Sharing and Disclosing Information

Ooredoo Palestine has the right to share Personal Data to other parties (including, without limitations, vendors, partners, and subcontractors), for the purposes of providing them with products and/or services that they have ordered or subscribed to or may be of interest to them (including, without limitation, to any new service and/or product to be provided by or through Ooredoo Palestine).

Ooredoo Palestine has also the right to disclose any Personal Data or information to any official, legislative and/or governmental body, and/or in compliance with any applicable laws and regulations.

If any other information is needed to other purposes than those set out in this Policy, Ooredoo Palestine shall obtain the Customer's consent in advance.

6.4 Ooredoo Palestine third party vendors and partners

1- Ooredoo Palestine may, for business purposes, contract with vendors, partners and other third parties. Personal Data and information may be disclosed to such parties if it is essential to perform work on behalf and/or for the benefit of Ooredoo Palestine. The disclosure and processing of data may help in credit/debit card processing, billing, shipping, repairs, customer service, auditing, and marketing of Ooredoo Palestine's products and services.

2- To protect any shared Personal Data, Ooredoo Palestine requires any third party to protect such data and to exclusively use it for the agreed purpose.

3- Ooredoo Palestine should ensure that all necessary clauses are included in the contracts with vendors, third parties, and partners so that they are obliged to apply adequate data privacy measures and controls to maintain confidentiality and protection of personal data, these measures and controls are addressed in Ooredoo Palestine Information Security Policy, Third Party Security Policy, Remote Access policy, and Access control policy.

Unless agreed otherwise, Ooredoo Palestine does not permit the vendors and partners to use it for their own marketing purposes.

The accountable department at OP must ensure that the necessary conditions are included in the contractual agreement including:

i. Data processor's responsibilities in case of data breaches,
ii. Right to audit the third party,
iii. Data ownership,
iv. Need to obtain the OP's approval for the appointment/change of subcontractors,
v. Third party to sign NDA according to OP applicable IS policies.

6.5 De-identified and aggregated information.

Ooredoo Palestine may provide aggregated information to certain parties for market research and development purposes, without sharing personal data that reveals the Customers Employees, Partners, and third Parties. This would support the development of Ooredoo Palestine's new products and/or services, improve existing services and/or products, and assist the understanding of Customers choices and preferences.

7. Customer Satisfaction and Protection

7.1. Creating and maintaining a trusted and safer environment

When Customers register on to any OP site or application, their Personal Data and information shall be collected for purposes of identification and verification to strengthen security measures and avoid compromising Customers' accounts.

7.2. Customer service and support

Unless any applicable laws and/or regulations state otherwise, Ooredoo Palestine shall provide a notice to Customers when their calls may be monitored or recorded by Ooredoo Palestine when they contact customer service. The recording and monitoring of calls can be used to the enhancement and training of Ooredoo Palestine's employees, and to protect Customers from any fraudulent actions/claim and misconduct.

Furthermore, Ooredoo Palestine may access any information about the Customer's used devices (without limitation, computer and/or phone) once the Customer contacts technical service support for the purposes of providing the necessary services and/or support. Information can also be utilized to offer any new product, service, update, and/or enhancement.

8. Customers Rights

1- Customer has the right to revoke his consent, block marketing calls, or stop receiving promotional messages by calling the customer service center or visiting Ooredoo Palestine's stores.

2- Customer Personal Data will be collected for legitimate purposes and will not be subsequently processed in a manner incompatible with this Policy.

3- Ooredoo Palestine is committed to the privacy rights and the protection of Customer's Personal Data.

4- Customer has the right to request the restriction of the processing of his/her Personal Data under specific conditions. However, there may be situations in which Ooredoo Palestine has the legal right to refuse such request.

5- Customers have the right to access their personal updated data.

6- Customer has the right to request Personal Data that Ooredoo Palestine has about him/her.

7- If a Customer suspects that any of their Personal Data has been breached by Ooredoo Palestine, he/she has the right to submit a complaint through the relevant communication channels, customer service center.

8- Customer's Personal Data will be used for the purpose of providing the Customer with the requested services and/or product.

9- Customer consent can be obtained in any possible way such as, without limitation, phone, SMS, or form approval though the website.

10- Customer has the right to verify the accuracy of his/her information and ask for update or correction.

Note: That these rights may be limited, depending on the concrete circumstances, as legally mandated.

8.1. Disabling cookies

There are a variety of ways which can limit the collection of certain information such as deleting or disabling Cookies on devices.

For instance, majority of the internet browsers have a feature that allows the users to erase the stored Cookies, block all Cookies or receive a warning before Cookies are stored. However, Customers shall acknowledge that disabling Cookies may also hinder them from using specific features on the websites, including ordering products and/or services, and maintaining an online account.

8.2. Disabling location services

Location services can be disabled on majority of devices in the settings menu, however, Ooredoo Palestine shall have the right to determine the location for purposes of legal and analytical purposes.

9. Regulatory Obligations

9.1 Legal process & protection:

Based on official requests and/or orders received from governmental/legislative bodies (such as, Public Prosecution Office and/or court orders) agencies, Ooredoo Palestine may be obliged to satisfy such requests, which may require the disclosure of certain Customers Personal Data.

9.2 Terminated accounts deletion:

Ooredoo Palestine retains and disposes Personal Data and information in accordance with relevant applicable laws and regulations.

10. Training and Awareness

Ooredoo Palestine reserves the right to use Customer's Personal Data , and information to conduct training and awareness related to information security (such as, without limitation, data privacy training) to its employees, vendors, and staff.

11. Inquiries, Suggestions, and Complaints

For any inquiries, complaints, or recommendations about the Policy, Customers may contact Ooredoo Palestine through any of the below communications channels:

- https://ooredoo.ps
- Tel: 00970 - 568- 003 – 000
- WhatsApp: 00970 – 566 – 111 - 111
- Email: info@ooredoo.ps

- Instagram: https://www.instagram.com/ooredoops/
- Facebook : https://www.facebook.com/OoredooPs/

12. Policy Review

12.1. Ooredoo Palestine reserves the right, for whatever reason, and at any time, to make any amendments and/or changes to this Policy. Upon any amendment or change to the Policy, Customers can view the Policy on Ooredoo Palestine's website once they occur, and this will be announced on Ooredoo Palestine's website in accordance with applicable laws and regulation.

12.2. Ooredoo Palestine conducts periodic review every two years to ensure that the policy and implementation of this policy remain relevant, effective, and compliant with evolving legal and regulatory requirements, technology updates, continuous improvement, and organizational needs over time.

12.3. If there are changes and amendments proposed on the current version of the Policy, such changes and amendments shall be agreed on by all relevant parties inside OP, including the ISSC, and the Board of directors.

12.4. The review record of this Policy will be updated through adding the changes and amendments, if any.

13. References:

	Reference	Version
1	IS Processes Approval Sheet	
2	Information Security Steering Committee Charter (ISSC)	**Draft**
3	Information Security Organization and Responsibilities	**2.0**
4	Personnel Security	**2.0**
5	Physical and Environmental Security Policy	**2.0**
6	Acceptable Use Policy	**1.6**
7	Access Control Policy	**2.0**
8	Password Management Policy	**2.0**
9	Systems Acquisition, Development and Maintenance Policy	**1.3**
10	Remote Access Policy	**1.4**
11	Communication and Network Security Policy	**2.0**
12	Operating System & Database Security Policy	**1.3**
13	Security Monitoring Policy	**2.0**
14	Information Security Incident Management Policy	**1.4**
15	Data Protection	**0.2**
16	Information Assets Classification	**1.2**
17	Third Party Security Policy	**1.0**
18	Law by Decree No. 15 for the year 2017 on Electronic Transactions.	
19	Law by Decree No. 10 of 2018 on Cybercrimes (as amended by Law by Decree No. 38 for the year 2021).	
20	Cabinet Resolution No. (3) for the year 2019 one the Personal Data of Citizens	