OVERVIEW OF OOREDOO TUNISIA POLICIES

ooredoo

DATA PROTECTION POLICY

The Data Protection Policy applies to all OT employees, consultants, Contractors and Third Parties who process personal data on behalf of Ooredoo Tunisie.

It aims at ensuring that the rules and processes adopted by OT to process personal data are compliant with the provisions of Law no. 63 of the 27 July 2004 and subsequent texts.

It outlines the major requirements and rules OT shall abide by in the processing of Personal Data like the identification of a data processor and a data controller prior to each processing operation, obtaining the consent of the data subjects before processing their data and obtaining the necessary authorizations from the National Authority for the Protection of Personal Data prior to processing sensitive data.

CODE OF ETHICS AND BUSINESS CONDUCT

This Code defines the code of behavior and norms all OT personnel shall follow in their workplace.

It sets for example the major conflict of interests situations that the employees shall avoid.

It determines the relationship the employees shall have with the external stakeholders like Customers, Suppliers and Community.
The Code of Ethics and Business Conduct describes as well the work environment in OT stating the norms the Company adopts when dealing with harassment, health and safety, smoking, political activities and any other similar issue.

THE WHISTLEBLOWING POLICY

The Whistleblowing Policy provides employees, Contractors, Customers and Suppliers with the means through which they can report any violation of laws, regulations or the Company's Internal rules.

It outlines the major reporting channels employees can use to report actual and perceived violations/misconducts/wrongdoings, the way the whistleblowing reports are assessed and the alleged misconducts are investigated.

It provides that the whistleblowing reports will be kept confidential and that employees will be protected against all forms of retaliation.

RELATED PARTY TRANSACTIONS POLICY

The Related Party Transactions Policy has been designed to regularize the Related Party transactions which could, if not regularized, lead to conflicts of interests or to any other illegal situation.

This Policy defines the Related Party transaction as being a transfer of resources, services or obligations between Related Parties, regardless of whether a price is charged or otherwise.

It determines the persons that can be considered as a Related Party to the Company such as its Board Chairman, its Chief Executive Officer or one of its Directors or shareholders.

The Policy also lists the different types of the Related Party transactions namely transactions at arm's length and transactions which are not at arm's length and explains the major differences between them.

ANTI-MONEY LAUNDERING POLICY

The Anti-Money Laundering Policy applies to all OT services, including Mobile Money Services, for all customer types including existing and new mobile wallets, and all types of transactions conducted by MM's customers and partners.

The Anti-Money Laundering Policy has been developed so as to assist relevant banks and other financial institutions that are working with the Company specifically in the provision of Mobile Money Services (MMS) to adhere to Laws, Guidelines and Regulations from Central Bank and other statutory requirements on Anti-Money Laundering and combating terrorist financing as per the Agreement with the relevant banks.

It details the responsibilities of The Company and its AML and Compliance function under Finance Directorate which mainly relate to the implementation of the highest standards of anti-money laundering / terrorist financing / Combating Financing Terrorism (AML / CFT) and to ensuring a successful cooperation with the competent authorities, paying due regard to customer confidentiality and data protection obligations.

The Policy also highlights the role of OT employees and Third Parties in the implementation of the AML standards like assisting the AML and Compliance function by providing it with access to the required documents and records and by reporting any suspicious behavior that could lead to or be a result of AML/CFT activities.