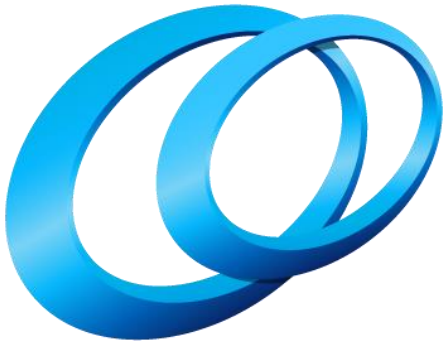

oraclecms
customer management solutions

DATA PROTECTION POLICY

Version:	v 1.9
Date of version:	12/09/2024
Created by:	James Paul
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
23/04/2017	1.0	Casey Eldib	Basic document outline
24/04/2017	1.1	James Paul	Reviewed/modified
18/07/2017	1.2	James Paul	Updated
09/08/2018	1.3	Fiona Nicholls	Updated/reviewed
03/09/2019	1.4	Di Parker	Reviewed/updated
13/09/2020	1.5	Mark Needham	Reviewed
09/09/2021	1.6	Mark Needham	Reviewed/updated
09/09/2022	1.7	Mark Needham	Reviewed/updated
12/09/2023	1.8	Mark Needham	Reviewed/updated
11/09/2024	1.9	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. INTRODUCTION

This Data Protection Policy outlines the principles and practices to safeguard the confidentiality, integrity, and availability of personal and sensitive data. The policy applies to all employees, contractors, and third parties handling data on behalf of the organisation.

2. SCOPE

This policy covers all personal data processed by the organisation, including but not limited to employee data, customer data, and vendor information. It applies to all systems, networks, and devices used for data storage, processing, and transmission.

3. PRINCIPLES OF DATA PROTECTION

1. **Lawfulness, Fairness, and Transparency:**

   - Data must be processed lawfully, fairly, and in a transparent manner.
   - Individuals will be informed about how their data is collected, used, and stored.

2. **Purpose Limitation:**

   - Data will only be collected for specified, explicit, and legitimate purposes.
   - Any secondary use of data will require consent or a lawful basis.

3. **Data Minimisation:**

   - Only the data necessary for the intended purpose will be collected and processed.

4. **Accuracy:**

   - Steps will be taken to ensure the accuracy and currency of data.
   - Inaccurate data will be rectified or deleted promptly.

5. **Storage Limitation:**

- Data will not be retained longer than necessary for the purposes for which it was collected.
- Secure disposal methods will be used for obsolete data.

6. **Integrity and Confidentiality:**

- Appropriate technical and organisational measures will be implemented to prevent unauthorised access, alteration, or loss of data.

4. ROLES AND RESPONSIBILITIES

1. **Data Protection Officer (DPO):**
    - Oversees data protection compliance and serves as the primary contact for data protection queries.
    - Monitors and audits data processing activities.
2. **Employees and Contractors:**
    - Must adhere to this policy and related procedures.
    - Report data breaches or risks promptly to the DPO.
3. **Third Parties:**
    - External vendors and partners must comply with data protection obligations as outlined in contracts or agreements.

5. DATA SUBJECT RIGHTS

Individuals have the following rights concerning their data:

- **Access**: The right to access their personal data held by the organisation.
- **Rectification**: The right to request correction of inaccurate or incomplete data.
- **Erasure**: The right to request deletion of data where lawful.
- **Restriction**: The right to restrict processing under certain conditions.

- **Portability**: The right to obtain and reuse their data across different services.
- **Objection**: The right to object to processing, particularly for direct marketing

6. DATA SECURITY MEASURES

- **Access Control:**
    - Implement role-based access controls and authentication mechanisms.
    - Regularly review and update access permissions.
- **Encryption:**
    - Use encryption for data storage and transmission to protect sensitive information.
- **Incident Response:**
    - Establish and maintain an incident response plan for data breaches.
    - Notify affected individuals and authorities as required by law.
- **Training and Awareness:**
    - Conduct regular training programs for employees on data protection principles and practices.

7. DATA TRANSFERS

- Ensure compliance with data transfer regulations when transferring data across borders.
- Use secure transfer methods and standard contractual clauses where required.

8. MONITORING AND REVIEW

- Regular audits will be conducted to ensure compliance with this policy.
- The policy will be reviewed annually or when significant changes occur in data protection laws or practices.

9. NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Legal actions may also be pursued where applicable.

10. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 11th September 2024.

The owner of this document is CTO, who must check and, if necessary, update the document at least once a year.

Chief Technical Officer