oraclecms
customer management solutions

DATA PROCESSING REVIEW PROCEDURE

Version:	v 1.9
Date of version:	08/07/2024
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
11/09/2023	1.8	Mark Needham	Reviewed/updated
08/07/2024	1.9	Mark Needham/Metin Unal	Review and modified

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Data Processing Review Procedure is to ensure that all data processing activities at OracleCMS are conducted in compliance with relevant data protection laws and internal policies. This procedure outlines how data processing practices are reviewed, assessed, and maintained for effectiveness, security, and regulatory compliance.

2. SCOPE

This procedure applies to all data processing activities conducted by OracleCMS, including:

- Collection
- Storage
- Access and sharing
- Processing and analysis
- Disposal of personal and sensitive data

The objectives of the review procedure are to:

- Ensure compliance with applicable data protection laws (e.g., **Digital Personal Data Protection Act (DPDPA)**, **GDPR**, etc.).
- Assess and mitigate risks related to data processing activities.
- Confirm that personal data is processed fairly, lawfully, and transparently.
- Evaluate the security measures in place to protect personal and sensitive data.
- Monitor and assess third-party data processors for compliance with OracleCMS data protection policies.

.

3. REVIEW FREUQNECY AND TIMING

Annual Reviews: Data processing activities will be reviewed at least once annually to assess compliance, data security, and risk management measures.

Ad-Hoc Reviews: Reviews will also occur when there are significant changes to:

- Business operations
- Data processing systems or platforms
- Data protection laws or regulations
- Data protection incidents or breaches

Post-Project Review: Following the completion of any major project involving personal data, a review of the data processing procedures will be conducted.

4. REVIEW PROCESS

The Data Processing Review will be conducted in the following stages:

Stage 1: Preparation

- **Identify Data Processing Activities**: Identify all data processing activities carried out by OracleCMS, including third-party services used to process personal data (e.g., cloud storage providers, contractors).
- **Compile Relevant Documentation**: Gather relevant documents, such as Data Processing Agreements (DPAs), security policies, data flow diagrams, and risk assessments.

Stage 2: Assessment

- **Data Protection Compliance Check**: Ensure that all data processing activities comply with applicable data protection regulations, such as:
    - **Lawful Basis for Processing**: Ensure that data processing has a lawful basis (e.g., consent, contract, legitimate interest).
    - **Purpose Limitation**: Confirm that data is only processed for specific, legitimate purposes.
    - **Data Minimisation**: Review data collection practices to ensure only necessary data is processed.
    - **Data Subject Rights**: Verify that processes are in place to uphold data subjects' rights (e.g., access, rectification, erasure).
- **Security Measures Evaluation**: Review the security measures in place for protecting data, including:
    - **Encryption** of data in transit and at rest
    - **Access controls** (e.g., role-based access, authentication)
    - **Incident response procedures** for data breaches
    - **Data backups and recovery** practices
- **Third-Party Review**: Review Data Processing Agreements (DPAs) with third-party processors and ensure they meet OracleCMS's security and compliance requirements.

Stage 3: Documentation of Findings

- **Risk Assessment**: Document any risks identified during the review process, including data security risks, compliance gaps, or inadequate controls.
- **Non-Compliance Identification**: Identify any areas of non-compliance with data protection laws and internal policies.
- **Mitigation Measures**: Document corrective actions required to address identified risks or non-compliance, including timelines and responsible parties.

Stage 4: Reporting and Action Plan

- **Internal Reporting**: A summary of the review findings and corrective action plan will be reported to the **Chief Information Officer** senior management, and relevant stakeholders.
- **Action Plan**: An action plan will be developed to address non-compliance or identified risks. This plan will include specific actions, responsible individuals, timelines, and performance metrics.
- **Follow-Up**: A follow-up review will be conducted to ensure that corrective actions are implemented and effective.

5. KEY ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)):

- Responsible for overseeing the entire data processing review process.
- Ensures that reviews are conducted in compliance with data protection laws and OracleCMS policies.
- Communicates the findings of the review to senior management and takes corrective actions where necessary.

Data Processing Teams:

- Participate in the review process by providing necessary documentation, access to systems, and responding to queries.
- Assist in identifying risks and implementing corrective actions.

IT Security Team:

- Reviews the security measures in place for data processing systems.
- Provides input on technical safeguards, including encryption, access controls, and incident response.

Legal and Compliance Team:

- Ensures that data processing activities comply with applicable data protection laws.
- Assists in reviewing third-party contracts and Data Processing Agreements (DPAs).

6. RECORD KEEPING AND DOCUMENTATION

Review Reports: All review reports, findings, and action plans will be documented and retained for a minimum of **five years**.

Audit Trail: A comprehensive audit trail will be maintained for all data processing activities, including decisions made, corrective actions taken, and the rationale for those decisions.

7. Policy Review

This Data Retention Policy shall be reviewed annually or more frequently as necessary to ensure its effectiveness and compliance with regulatory requirements.

8. Validity and Document Management

This document is valid as of 8th July 2024.

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

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to unacceptable or unauthorised use of information assets
- Number of incidents related to inappropriate employee training or awareness programs regarding acceptable use of information assets

Chief Technical Officer