Regulatory Compliance Assistant - Sample Policy Document - Version 1.0

Date: June 7, 2025
Author: John Richardson
Subject: Data Retention and Privacy Policy Compliance

Section 1: Introduction
This document outlines the policy of Oracle LLC regarding the collection, storage, processing, and retention of personal data in compliance with relevant data privacy regulations, including but not limited to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Our commitment to data privacy is paramount, ensuring that all data handling practices adhere to the highest standards of security and transparency.

Section 2: Data Collection and Usage
2.1 Lawful Basis: All personal data collected is processed on a lawful basis, such as consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests.
2.2 Purpose Limitation: Data is collected only for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
2.3 Data Minimization: We ensure that personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Section 3: Data Retention Periods
3.1 General Principle: Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and regulations.
3.2 Specific Categories:
- Customer transaction data: Retained for 7 years as per financial regulatory requirements.
- Employee HR records: Retained for 5 years post-employment termination.
- Marketing consent records: Retained until consent is withdrawn or for a maximum of 3 years of inactivity.
3.3 Deletion Procedures: Upon expiration of the retention period, data is securely deleted or anonymized in a manner that prevents re-identification.

Section 4: Data Security and Access
4.1 Security Measures: We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including encryption, pseudonymisation, and regular security audits.
4.2 Access Control: Access to personal data is restricted to authorized personnel who have a legitimate need to access the data for their job functions. All access is logged and regularly reviewed.

Section 5: Rights of Data Subjects
Data subjects have the right to access, rectification, erasure, restriction of processing, data portability, and to object to processing. Requests regarding these rights should be submitted to privacy@yourcompany.com.

Section 6: Compliance Review
This policy is reviewed annually and updated as necessary to reflect changes in legal or regulatory requirements, or our data handling practices. All employees are required to undergo annual compliance training.