Section 1: Draft Purpose and Scope for Data Governance Plan

Purpose

The primary purpose of FutureMart's Data Governance Plan is to establish a structured and enterprise-wide approach for managing data as a critical asset. This includes ensuring data integrity, privacy, security, and usability across its lifecycle—from acquisition to archiving. The plan supports FutureMart’s goal of delivering a seamless omnichannel customer experience by enabling consistent, accurate, and timely data across digital and physical touchpoints.

By formalizing data responsibilities, standards, and compliance protocols (e.g., GDPR), this plan aims to:

- Protect customer and operational data
- Enable data-driven decision-making
- Support regulatory and ethical data practices
- Foster stakeholder trust and accountability

Scope

This data governance plan applies to all business units and systems within FutureMart that generate, store, process, or consume data. The scope includes:

- **Sales and Customer Service** – Transactional data, customer support interactions, and order fulfillment
- **Marketing and Personalization** – Campaign performance, behavioral analytics, customer segmentation
- **Inventory and Supply Chain Management** – Real-time inventory, warehouse data, and supplier analytics
- **Finance and Accounting** – Financial records, audits, and regulatory data
- **External Data Sources** – Market intelligence, competitive pricing, social media sentiment

It covers all data types (structured, semi-structured, and unstructured), data platforms (CRM, PIM, DWH, streaming systems), and integration points (APIs, ETL, real-time pipelines). This governance extends to data managed through cloud and third-party systems under contractual obligations.

Excellent—thank you for the go-ahead on Section 1. Now let's draft **Section 2: Data Governance Objectives** tailored for FutureMart's architectural ecosystem and business priorities.

Section 2: Data Governance Objectives

Data Quality

Ensure that data across all systems—customer, sales, inventory, marketing, and finance—is accurate, complete, timely, and fit for use. Implement continuous data profiling, cleansing, and enrichment practices, supported by data quality KPIs. Use validation rules, automated quality checks in ETL pipelines, and periodic audits to maintain data reliability across systems such as CRM, PIM, and data warehouse.

Objective: Establish a data quality framework that enforces accuracy, completeness, consistency, and timeliness across all FutureMart systems and business units.

Data Security

Protect sensitive business and customer data—such as payment information, personally identifiable information (PII), and strategic analytics—from breaches and unauthorized access. Utilize encryption, access controls (RBAC), audit trails, and data masking. Incorporate security layers in all critical platforms, such as CRM, OMS, and cloud storage (e.g., AWS, Azure).

Objective: Implement a multi-layered data security strategy that includes encryption, role-based access control, secure transmission protocols, and regular vulnerability assessments.

Data Compliance

Ensure that data collection, storage, processing, and disposal conform to legal, regulatory, and contractual obligations, including GDPR, CCPA, and PCI DSS. Establish clear data retention and user consent policies, with automation support from compliance tools (e.g., OneTrust, TrustArc).

Objective: Develop and enforce data handling practices that ensure FutureMart's full compliance with international data privacy and security regulations.

Data Availability

Ensure data is reliably available to authorized users across departments—operations, analytics, marketing, and finance—without compromising security. Leverage cloud-native high-availability infrastructure and redundancy practices across data stores and analytics platforms.

Objective: Maximize data availability by deploying resilient infrastructure, real-time replication, and proactive monitoring systems.

Data Consistency

Maintain a single source of truth across platforms and departments. Implement master data management (MDM), standardized formats, and synchronized updates across systems like CRM, PIM, and DWH to avoid conflicting or outdated data.

Objective: Standardize data definitions and integrate data synchronization protocols to ensure consistency across all FutureMart data systems.

Data Usage

Promote ethical and optimal use of data for analytics, decision-making, personalization, and customer engagement. Define clear usage guidelines, encourage data literacy, and support business intelligence initiatives using governed data assets.

Objective: Enable responsible and strategic use of data assets by aligning data access and usage policies with business objectives and decision-making needs.

Section 3: Data Governance Framework

◆ Data Governance Roles and Responsibilities

Data Governance Steering Committee

Purpose: Oversee the development and enforcement of data governance policies, resolve escalated issues, and align governance initiatives with business strategy.

Proposed Members:

- Eleanor Vance (CEO) – Executive Sponsor
- Kenji Tanaka (CTO) – Data Systems Oversight
- Julian Blackwood (CFO) – Financial Data Oversight
- Seraphina Dubois (CMO) – Marketing Data Strategy
- Simone Dubois (CHRO) – HR Data Compliance
- Devon Hayes (CSO) – Data Security & Risk
- Alistair Finch (COO) – Operations Alignment
- Ingrid Olsen (VP of Operations) – Fulfillment & Logistics Oversight
- Olivia Carter (VP of Sales) – Customer Data Oversight

Data Stewards

Responsibilities:

- Maintain data quality and integrity
- Perform data validation and profiling
- Collaborate with IT and data users to resolve data issues

Examples:

- Naomi Patel (Director of Software Development) – Product Data
- Marcus Bell (Director of Fulfillment & Logistics) – Inventory Data
- Genevieve Rossi (Director of Customer Service) – Support Data
- Jasper Thorne (VP of Marketing) – Campaign Data

Data Owners

Responsibilities:

- Define data requirements and access policies
- Approve data classification and usage guidelines
- Ensure regulatory compliance for data assets

Examples:

- Clara Bell (Director of Financial Planning) – Financial Planning Data
- Olivia Carter (VP of Sales) – Sales Data
- Astrid Berger (Director of Brand Marketing) – Brand Analytics
- Isabelle Moreau (VP of Finance) – Accounting and Finance Data

---

Data Users

Responsibilities:

- Access, analyze, and use data under compliance guidelines
- Report data quality issues
- Adhere to data usage protocols

Examples:

- Data Analysts, Marketing Specialists, CRM Teams
- Aisha Khan (SEO Specialist), Ethan Reed (Email Marketing Manager)
- Lila Moreau (Customer Support Manager)

◆ Data Governance Policies

Data Collection

- Customer and operational data must be collected transparently and with consent.
- Data must be stored in secure, centralized systems (e.g., CRM, DWH).
- Data must be tagged with metadata for traceability and classification.

Data Usage

- Sales and marketing teams may access only anonymized or aggregated customer data for analysis and campaign optimization.
- All usage must comply with data privacy laws (e.g., GDPR).

Data Retention

- Retain financial and customer data for a minimum of 7 years unless otherwise required.
- Archive inactive customer records after 24 months of inactivity.
- Delete expired records based on predefined data lifecycle rules and compliance mandates.

Data Privacy and Security

- All PII and sensitive data must be encrypted at rest and in transit.
- Role-based access control (RBAC) is mandatory across systems.
- Apply data masking for non-privileged environments and external tools.

Section 4: Data Management Practices

◆ Data Classification

FutureMart classifies data based on sensitivity and intended use to ensure appropriate levels of protection and access control:

Classification Level	**Examples**	**Handling Measures**
Public	Marketing materials, product descriptions, published FAQs	No restrictions. May be shared externally.
Internal	Sales performance reports, team KPIs, internal dashboards	Shared within departments. Requires corporate email access.
Confidential	Customer profiles, order history, campaign metrics	Encrypted at rest and in transit. Role-based access. Data masking for reports.
Restricted	Financial data, PII, login credentials, payment info	Multi-factor authentication (MFA), least-privilege access, encryption, DLP tools, and audit logging.

Policy: All data assets must be tagged with classification metadata. Periodic classification audits will ensure up-to-date tagging across systems like CRM, OMS, and DWH.

◆ Data Quality Management

To ensure reliability and usability of data across departments:

- Implement validation rules in ETL pipelines (e.g., dbt, Talend) for type checking, null handling, referential integrity, and range constraints.
- Monitor KPIs like data completeness, timeliness, accuracy, and duplication rates.
- Enable alerting systems for anomalies in critical datasets (e.g., inventory counts, financial transactions).
- Establish issue resolution workflows via data stewards.
- Conduct quarterly data quality audits and business-led reviews.

Policy: Data quality dashboards will be embedded in BI tools like Looker and Power BI for ongoing visibility and resolution prioritization.

◆ Data Integration

FutureMart leverages diverse systems and platforms. Standard practices include:

- Use of APIs and standardized data contracts for integration across CRM (e.g., Salesforce), ERP, OMS, and marketing platforms.

- ETL tools (e.g., Apache Nifi, Talend) and event streaming frameworks (e.g., Kafka, Kinesis) for batch and real-time data sync.
- Conformance to a centralized data schema using canonical formats (e.g., JSON/Avro/XML) to enable consistent transformation logic.
- Implement data lineage tracking and source mapping in metadata management tools (e.g., Alation, Collibra).

Policy: All integration points must comply with FutureMart's API standards and metadata tagging policies to ensure interoperability and traceability.

◆ Data Documentation

To maintain structural clarity and institutional memory across evolving systems:

- Define and maintain a central metadata repository documenting schema definitions, data dictionaries, business glossary, lineage, and owners.
- Ensure automated documentation of changes through Git-enabled dbt workflows.
- Make documentation accessible to all roles—from analysts to engineers—via intranet or governance platforms (e.g., Confluence, Collibra).
- Include data definitions in all analytics and BI tools for transparency and usability.

Policy: All new data assets and pipelines must be documented prior to production deployment and reviewed quarterly.

Section 5: Data Security and Privacy Policies

◆ Data Encryption and Masking Policy

Purpose: To ensure the confidentiality and integrity of sensitive data during storage and transmission.

- **Encryption at Rest**: All databases (e.g., CRM, PIM, DWH) must use AES-256 encryption. Cloud storage (e.g., AWS S3) must have server-side encryption (SSE) enabled.
- **Encryption in Transit**: All data transferred between internal systems or to external vendors must use TLS 1.2+ protocols.
- **Key Management**: Encryption keys are rotated regularly and managed via secure KMS solutions (e.g., AWS KMS, Azure Key Vault).
- **Data Masking**: Sensitive fields (PII, financials) must be masked in non-production environments and in business-facing dashboards when full visibility is not required.

Policy: All structured and semi-structured sensitive data must be encrypted and masked per classification level. Developers must use masked test datasets in dev/test environments.

◆ Data Access Control Policy

Purpose: To enforce least-privilege access and ensure sensitive data is only accessible to authorized personnel.

- **Role-Based Access Control (RBAC)**: Access to data is granted based on roles (e.g., Analyst, Engineer, Steward) defined in the IAM system.
- **Single Sign-On (SSO)**: Integrated across all enterprise systems to enforce secure and unified identity management.
- **Multi-Factor Authentication (MFA)**: Required for all administrative accounts and users accessing sensitive data systems.
- **Access Reviews**: Quarterly audits of data access logs are conducted, and access privileges are reviewed and adjusted as needed.
- **Segregation of Duties**: Ensure data stewards, developers, and end-users have distinct access levels.

Policy: Any request for elevated data access must go through documented approval workflows involving data owners and compliance officers.

◆ Data Incident Management Policy

Purpose: To establish a clear and rapid response protocol for handling data breaches, unauthorized access, and security anomalies.

- **Detection**: Use of real-time monitoring tools (e.g., AWS Security Hub, Splunk) to detect anomalies or suspicious activity.
- **Incident Response Team**: Cross-functional team including CSO, IT Security, Legal, and affected business unit leads.
- **Response Plan**:
    1. **Identification** – Detect breach and determine its scope and source.
    2. **Containment** – Isolate compromised systems or data flows.
    3. **Eradication** – Remove root cause or affected systems.
    4. **Recovery** – Restore from backups and validate integrity.
    5. **Notification** – Notify internal stakeholders and regulators (e.g., under GDPR) within required timeframes.

- **Post-Incident Review**: Conduct after-action review, update policies or controls, and train involved teams on findings.

Policy: All employees must report suspected data incidents immediately to the security team via predefined escalation channels. Simulated breach drills will be conducted bi-annually.

Section 6: Compliance and Legal Considerations Policies

◆ Policy for Data Regulatory Requirements

Purpose: To ensure that FutureMart complies with all applicable legal and regulatory obligations governing the use, storage, transfer, and disposal of data.

Applicable Regulations:

- **General Data Protection Regulation (GDPR)** – Covers all personal data of EU citizens; mandates user consent, data minimization, access rights, and breach notification.
- **California Consumer Privacy Act (CCPA)** – Governs data privacy rights of California residents, including rights to access, delete, and opt-out of data sales.
- **Payment Card Industry Data Security Standard (PCI DSS)** – Applies to all systems handling credit/debit card transactions; enforces encryption, access control, and monitoring.
- **CAN-SPAM & CASL** – Regulates marketing communications in the U.S. and Canada, including opt-in/opt-out mechanisms and contact transparency.
- **SOX (Sarbanes-Oxley)** – Applies to financial data integrity and audit trails for publicly traded companies (if applicable post-merger expansion).
- **ePrivacy Directive** – Applies to cookies and electronic marketing within the EU, often in tandem with GDPR.

Policy: All data handling workflows must be reviewed for compliance by legal counsel. Regulatory changes must be tracked by the Compliance Office and integrated into operational procedures quarterly.

◆ Data Auditing and Reporting Policy

Purpose: To establish transparent and consistent mechanisms for auditing data access, usage, and compliance with internal and external requirements.

- **Audit Trails**: All access to sensitive data (PII, financials) must be logged and monitored through SIEM tools like Splunk or AWS CloudTrail.

- **Automated Reporting**: Generate periodic compliance dashboards to track GDPR/CCPA metrics, data quality KPIs, and access anomalies.
- **Internal Audits**: Conduct semi-annual audits across data warehouses, CRM systems, and external integrations to assess policy adherence.
- **External Compliance Reviews**: Legal and audit teams will coordinate annual reviews with third-party auditors (e.g., for PCI DSS certification).

Policy: All audit logs must be retained securely for a minimum of 7 years. Non-compliance incidents must be reviewed within 30 days of detection.

◆ Data Retention and Disposal Policy

Purpose: To retain data only for as long as necessary and ensure secure and compliant disposal practices.

Retention Guidelines by Category:

- **Customer PII** – Retained for 5 years post-last interaction (per GDPR “data minimization” and “storage limitation” principles)
- **Financial Records** – Retained for 7–10 years (in accordance with SOX and tax audit needs)
- **Marketing Campaign Data** – Retained for 3 years for historical analysis and ROI measurement
- **Employee Records** – Retained for 6 years following termination (as per labor laws)

Disposal Procedures:

- Use certified data destruction tools for electronic disposal (e.g., DoD 5220.22-M for drives)
- Schedule automated purges from databases with audit verification
- Document disposal actions in the central compliance system

Policy: Data retention schedules must be documented in the metadata catalog, and disposal procedures must be validated annually by the security and legal teams.

Section 7: Additional Components of the Data Governance Plan

◆ Data Governance Tools and Technologies

To ensure consistent enforcement, monitoring, and optimization of data governance across the enterprise, FutureMart will adopt the following tools:

- **Metadata & Data Cataloging**:

    - *Collibra* – Enterprise-wide data catalog, lineage tracing, and governance workflows
    - *Alation* – Metadata discovery, stewardship assignment, and data literacy enablement
- **Data Quality Monitoring**:
    - *Great Expectations / Monte Carlo* – Automated data validation and anomaly detection
    - *dbt (data build tool)* – Transformation logic validation with built-in documentation
- **Security & Compliance Tools**:
    - *OneTrust / TrustArc* – GDPR and CCPA compliance automation
    - *AWS Security Hub* – Cloud security monitoring and incident tracking
- **Integration & Transformation**:
    - *Apache Nifi, Talend, dbt* – Scalable ETL/ELT pipelines with lineage and governance hooks
- **Audit & Access Monitoring**:
    - *Splunk, AWS CloudTrail* – Audit trails, anomaly detection, and compliance reporting

---

◆ Data Governance Training and Awareness

FutureMart will roll out a structured training and awareness program to embed a culture of data stewardship across all departments:

- **Role-Based Training**:
    - Data Stewards: In-depth workshops on quality, metadata, and remediation
    - Analysts & Users: Practical usage guidelines, consent handling, and access protocols
    - Executives: High-level compliance and data monetization strategies
- **Onboarding Modules**: New hires receive a mandatory data governance orientation.
- **Awareness Campaigns**: Quarterly newsletters, gamified knowledge assessments, and spotlight stories on data governance wins.
- **Certification Pathways**: Internal certification for "Certified Data Steward" and "Governance Champion" roles.

◆ Performance Metrics and Reporting

To measure and improve the effectiveness of data governance, the following KPIs and dashboards will be monitored:

- **Data Quality Metrics**:
  - Accuracy (% valid entries)
  - Completeness (% missing values)
  - Consistency (record sync rate across systems)
- **Security & Compliance Metrics**:
  - Number of access violations detected
  - Time to resolve data incidents
  - % of systems with active encryption and access logging
- **Governance Operations Metrics**:
  - Policy coverage rate (% of data domains with approved governance)
  - Metadata completeness score
  - % of users trained on governance protocols
- **Reporting Structure**:
  - Monthly metrics reviewed by the Data Governance Steering Committee
  - Quarterly summary to the executive leadership team
  - Ad-hoc dashboards for auditors and compliance teams

◆ Implementation Plan

The implementation will follow a **phased, iterative rollout** with centralized coordination and business-unit-level execution.

Phase 1: Planning & Foundation (Months 1–2)

- Finalize governance roles, charter, and tools
- Set up central governance platform (e.g., Collibra)
- Establish governance steering committee cadence

Phase 2: Pilot and Training (Months 3–5)

- Launch governance in 2 domains (e.g., Customer Data, Inventory)

- Begin role-based training
- Collect feedback and refine practices

Phase 3: Enterprise Rollout (Months 6–10)

- Expand to all departments and data domains
- Fully integrate quality and compliance monitoring
- Conduct baseline audits

Phase 4: Optimization and Continuous Improvement (Ongoing)

- Annual governance reviews and KPI benchmarking
- System upgrades and integration of advanced governance AI tools
- Refresh training and documentation annually

Resource Allocation:

- Tools: Collibra, dbt, OneTrust, Splunk
- Personnel: Governance Leads, Stewards, Analysts
- Budget: CapEx for tools; OpEx for training and consulting
