* 1. **Data management considerations for different regulations**

Here’s a detailed overview of **data management considerations for different regulations** like **GDPR** and **BCBS 239**, along with **realistic examples** that illustrate how organizations must adapt their data governance and management practices to stay compliant.

**1. General Data Protection Regulation (GDPR) – *EU Law for Personal Data Protection***

**Key Requirements:**

* Lawful, fair, and transparent processing of personal data
* Data minimization and purpose limitation
* Data subject rights (access, rectification, erasure, portability)
* Data breach notification
* Data Protection Impact Assessments (DPIA)
* Data security and accountability

**Data Management Considerations:**

| **Area** | **Consideration** | **Example Use Case** |
| --- | --- | --- |
| **Data Classification** | Tag personal data as “sensitive” or “identifiable” | Tag customer names, email addresses, IPs as personal data |
| **Metadata Management** | Maintain lineage and source tracking for personal data | Track how customer data flows across CRM, ERP, and BI tools |
| **Data Minimization** | Store only data that is strictly necessary | Collect just email and name for newsletter, not birthdate |
| **Access Management** | Role-based access to personal data | HR team can access employee data; Marketing cannot |
| **Consent Management** | Capture and store consent status and purpose | Store timestamp of consent for email marketing opt-in |
| **Retention Policies** | Define and enforce data retention/deletion rules | Delete customer data 6 months after account closure |
| **Data Subject Requests** | Enable search and export of data related to a person | Provide full export of customer records upon request |

**2. BCBS 239 – *Basel Committee on Banking Supervision for Risk Data Aggregation***

**Applicable to:**

* Global systemically important banks (G-SIBs)
* Domestic systemically important banks (D-SIBs)

**Key Principles:**

* Governance and infrastructure for risk data aggregation
* Accuracy, completeness, and timeliness of risk data
* Adaptability to changing risks or market conditions
* Data architecture to support risk reporting

**Data Management Considerations:**

| **Area** | **Consideration** | **Example Use Case** |
| --- | --- | --- |
| **Data Governance** | Assign data ownership for risk data | Chief Risk Officer responsible for credit risk data |
| **Data Quality** | Ensure risk data is accurate, complete, and reconciled | Daily reconciliation of credit exposure data |
| **Data Lineage** | Know where risk data comes from and how it’s transformed | Document path of loan data from core banking to risk reports |
| **Timeliness** | Deliver up-to-date risk reports quickly | Near real-time credit risk dashboard |
| **Aggregation Capabilities** | Ability to aggregate risk across legal entities and products | Aggregate risk from retail and corporate divisions |
| **Change Management** | Flexibility to adapt data models to regulatory change | Quickly update models for IFRS 9 or new capital rules |

**Other Regulation Examples:**

**3. HIPAA (Health Insurance Portability and Accountability Act) – USA**

* Protects health information (PHI)
* Requires audit trails, encryption, and access controls

**Example**: A hospital must encrypt patient records and log every access attempt to comply with HIPAA.

**4. CCPA (California Consumer Privacy Act) – USA**

* Similar to GDPR but applies to California residents
* Requires disclosure of data collection and sale practices

**Example**: An e-commerce company must list all third-party data sharing activities on its privacy policy page and allow opt-out.

**5. SOX (Sarbanes-Oxley Act) – USA**

* Focuses on financial data integrity for public companies
* Requires strict controls over financial reporting data

**Example**: A CFO must certify that all revenue numbers in reports are accurate and auditable, with clear data lineage.

**Summary Table**

| **Regulation** | **Focus Area** | **Key Data Management Needs** | **Example** |
| --- | --- | --- | --- |
| GDPR | Personal data privacy | Consent, data minimization, data rights | Right to erasure and data export |
| BCBS 239 | Risk data in banking | Aggregation, accuracy, lineage, timeliness | Daily liquidity risk aggregation across business lines |
| HIPAA | Health data protection | PHI security, auditability, breach notification | Logging access to patient medical records |
| CCPA | Consumer data rights | Transparency, access, opt-out options | Opt-out for data sales via website |
| SOX | Financial reporting | Data integrity, audit trails, reporting governance | Reconciled revenue figures traceable to source systems |