FREE GUIDE

The Three Pillars of Comprehensive Compliance

Organizations face unprecedented challenges in managing regulated data. At Integral, we understand that comprehensive compliance in sensitive data management rests on three fundamental pillars:

Data Privacy

Process Controls

Physical Controls

useintegral.com

hello@useintegral.com

Integral

Data Privacy

Integral

OVERVIEW

Data privacy is the foundation of compliance across various sectors dealing with regulated data, requiring organizations to protect personal information from unauthorized access, use, or disclosure while navigating a complex web of regulations such as GDPR, CCPA, CPRA, GLBA, and FCRA.

Implementing robust data privacy measures requires a multi-faceted approach including data minimization, advanced de-identification and anonymization techniques, comprehensive risk assessment and mitigation, and regular data classification and audits. By prioritizing data privacy, organizations not only meet regulatory requirements but also build trust with stakeholders, creating a strong foundation for responsible data use and innovation.

Leverage Integral's expertise for comprehensive data privacy

Integral's automated processes utilize an "expert-in-the-middle" approach, assessing privacy risks, streamlining workflows, and suggesting tailored remediations.

BEST PRACTICES

- **Conduct thorough pre-acquisition evaluations of datasets**
- **Implement robust access controls based on the principle of least privilege**
- **Regularly update security measures to address emerging threats**

KEY COMPONENTS

Regulatory Compliance

(e.g., GDPR, CCPA, etc.) Ensuring adherence to various data protection laws. This involves implementing specific requirements of each applicable regulation.

Deldentification

Applying methods to remove or obscure personal identifiers in datasets. This process preserves data utility while reducing the risk of individuals being identified from the information.

Data Minimization

Limiting data collection and retention to only what's essential for specific purposes. This reduces privacy risks and simplifies compliance by decreasing the volume of sensitive information managed.

Classification and Audits

Categorizing data based on sensitivity and conducting periodic reviews of data handling practices. This ensures appropriate security measures are applied to different data types.

Process Controls

Integral

OVERVIEW

Process controls are crucial for maintaining data privacy across organizations, encompassing documented procedures, workflow management, and regular audits. These controls ensure consistent handling of sensitive information, reduce human error, and create a traceable chain of data interactions.

Implementing robust process controls helps organizations navigate complex regulatory landscapes like GDPR, CCPA, and HIPAA while fostering a culture of privacy awareness and significantly reducing the risk of data breaches.

Effective process controls require a multi-layered approach

Clear policy documentation, role-based access management, regular training, and continuous improvement not only meet regulatory requirements but also build trust with stakeholders.

BEST PRACTICES

- Implement comprehensive data classification and handling procedures
- Establish clear roles and responsibilities for data privacy management
- Conduct regular privacy impact assessments and process audits
- Maintain up-to-date documentation of all data-related processes

KEY COMPONENTS

Policy Management

Developing, implementing, and maintaining comprehensive data privacy policies. This involves creating guidelines for data collection, use, storage, and disposal, ensuring alignment with regulatory requirements and organizational goals.

Access Control

Implementing role-based access control (RBAC) and principle of least privilege. This involves defining and managing user roles, permissions, and access rights to sensitive data and systems.

Data Handling Procedures

Establishing standardized processes for data collection, processing, storage, and deletion. This includes data minimization practices, retention policies, and secure data transfer protocols.

Incident Response Planning

Developing and regularly testing incident response plans. This ensures the organization can quickly and effectively respond to data breaches or privacy violations, minimizing impact and meeting regulatory reporting requirements.

Physical Controls

Integral

OVERVIEW

Physical controls are essential in protecting data privacy by securing the tangible assets, facilities, and hardware that store or process sensitive information. These controls create a crucial first line of defense against unauthorized access, theft, and environmental threats to data integrity. Implementing robust physical controls helps organizations comply with regulations like GDPR, HIPAA, and PCI-DSS, which mandate the protection of physical assets containing personal data.

Effective physical control strategies involve a combination of facility security measures, device management protocols, environmental safeguards, and stringent access policies.

Implement physical controls strategically

Prioritize physical security measures based on data sensitivity and regulatory requirements. Focus on high-risk areas first to maximize protection while optimizing resource allocation.

BEST PRACTICES

- Implement multi-factor authentication for facility and server room access
- Maintain a comprehensive inventory of all assets containing sensitive data
- Employ surveillance and regular security audits in data storage areas
- Establish and enforce clear desk and clear screen policies

KEY COMPONENTS

Facility Security

Implementing physical barriers, surveillance systems, and access control measures to protect facilities housing sensitive data. This includes security personnel, biometric access controls, and visitor management systems.

Device Management

Securing all hardware devices that can access, store, or process sensitive data. This involves asset tracking, encryption of mobile devices, and secure disposal methods for outdated equipment.

Environmental Controls

Protecting data center infrastructure from environmental threats. This includes implementing fire suppression systems, climate control, and power management to ensure data integrity and availability.

Physical Access Logs

Maintaining detailed logs of physical access to sensitive areas. This creates an audit trail for investigations, helps identify unusual patterns, and supports compliance with regulatory requirements for physical security documentation.

THANK YOU

Ready to maximize your regulated data strategy?

Integral empowers companies to quickly leverage regulated data and drive innovation while maximizing compliance.

Get in touch!

hello@useintegral.com