adnovum

Leveraging Data Management for a Competitive Advantage

"Proper management of data in the cloud and on-prem, can facilitate decision-making and enable digital transformation."

In light of ongoing data breach incidents and stricter data management regulations, organizations are increasingly aware of data management not just as being an IT task but a strategic business imperative. Establishing a clear cloud data management strategy can help your organization to prevent risks, overcome regulation compliance barriers and make accurate decisions, and in the process, secure a strong competitive advantage.

A successful Data Management Strategy includes the following aspects:

- DATA PRIVACY AND GOVERNANCE
- DATA DISCOVERY AND CLASSIFICATION
- DATA PROTECTION AND SECURITY

ABOUT ADNOVUM

We offer our customers a comprehensive range of tailored IT services ranging from IT architecture and security consulting to design, implementation and maintenance of customized business and security solutions. Our offerings have been deployed by leaders in the finance, insurance, public and several other sectors.

30 years in empowering businesses to master their digital potential

Trusted by over 120 entities worldwide

1000+ projects for customers in Europe and Asia, 400 releases per year

Protecting over 500 portals

Securing > 80% of Swiss e-banking transactions

Manage > 7 million digital identities for customers, partners, employees, IoT devices

OUR SERVICES

- ✓ Application & Cloud Services
- ✓ Consulting
- ✓ Cybersecurity
- ✓ Digital Inovation
- ✓ Digital Solutions

Adnovum Singapore Pte Ltd
3 Shenton Way, Shenton House, #23-03, S068805
Locations: Zurich (HQ) I Bern I Budapest I Ho Chi Minh City I Lausanne I Lisbon I Singapore

☎ +65 6536 0668
✉ info@adnovum.sg
www.adnovum.com

DATA PRIVACY AND GOVERNANCE

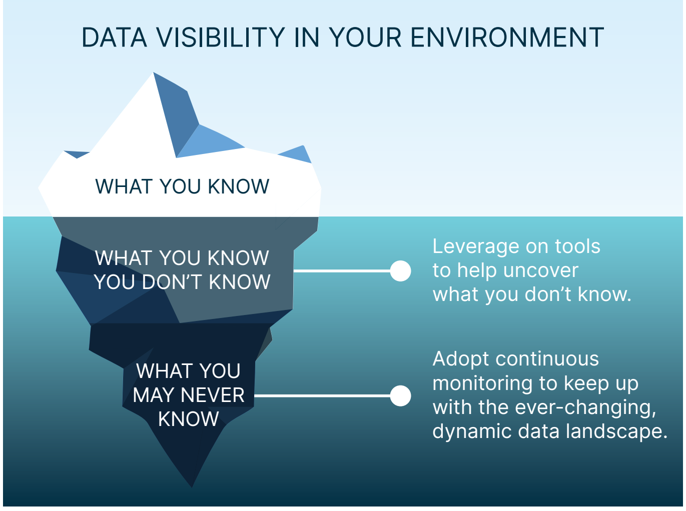
Managing Compliance in the Constantly Evolving Regulatory Landscape

Hefty fines and other impacts from non-compliance have caused significant shifts in organizations' attitudes towards compliance strategies, viewing them more as investments rather than a cost. Effective data security takes into account the sensitivity of various datasets and corresponding regulatory compliance requirements. It identifies the importance of various datasets and applies the most appropriate security controls. However, complying with regulations is challenging for various reasons, some of which include:

- **Resource-intensive adaptability:** Implementation of necessary procedures to manage massive amounts of data, which includes tracking from creation to destruction, and handling the storage of data according to specific criteria, could be both time-consuming and expensive.
- **Evolving requirements:** While GDPR is intended to improve decision-making and risk assessment, it would be difficult to identify and manage multi-jurisdictional retention requirements, if data is stored on multiple locations by cloud service providers.
- **Extraterritorial application:** Global companies including those in Singapore have to comply with GDPR as it is applicable to all EU citizens regardless of their location or the locations of the organization.

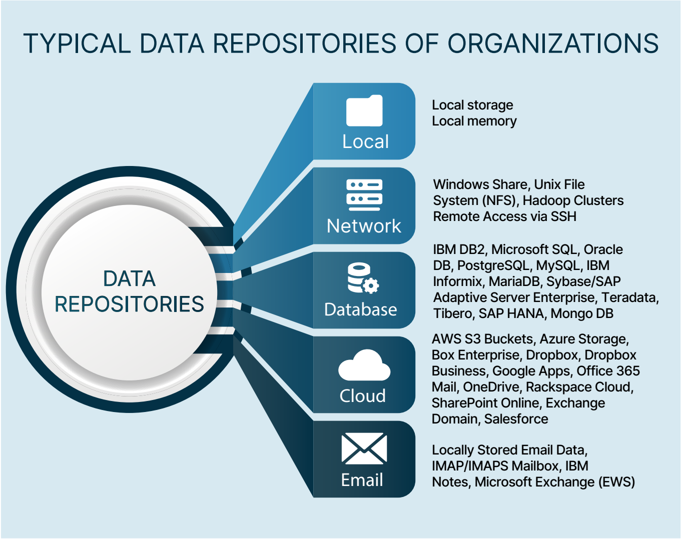
Adnovum experts assist security and privacy teams in handling personally identifiable information and aligning their security activities and systems with global regulations. They help organizations to plan incidence response plans. Our solutions also meet all regulatory compliance demands, including local and international regulations such as Data Protection Act Singapore, GDPR, PCI, HIPAA, POPA, etc.

DATA DISCOVERY AND CLASSIFICATION


DATA VISIBILITY IN YOUR ENVIRONMENT
WHAT YOU KNOW
WHAT YOU KNOW YOU DON'T KNOW
WHAT YOU MAY NEVER KNOW

Leverage on tools to help uncover what you don't know.

Adopt continuous monitoring to keep up with the ever-changing, dynamic data landscape.



Local storage
Local memory

Windows Share, Unix File System (NFS), Hadoop Clusters
Remote Access via SSH

IBM DB2, Microsoft SQL, Oracle DB, PostgreSQL, MySQL, IBM Informix, MariaDB, Sybase/SAP Adaptive Server Enterprise, Teradata, Tibero, SAP HANA, Mongo DB

AWS S3 Buckets, Azure Storage, Box Enterprise, Dropbox, Dropbox Business, Google Apps, Office 365 Mail, OneDrive, Rackspace Cloud, SharePoint Online, Exchange Domain, Salesforce

Locally Stored Email Data, IMAP/IMAPS Mailbox, IBM Notes, Microsoft Exchange (EWS)

Key Functions of Data Discovery and Classification

- **Improve data security in the cloud:** Knowing what, where, how sensitive data is, as well as about the threat actors, allows you to identify risk levels, prioritize your efforts, prepare and execute effective data protection strategies.
- **Support regulatory compliance across borders:** Through solutions like multi-country cloud strategy, etc., we help ensure that confidential data is discovered then classified to comply with various regulations such as PDPA, HIPAA, GDPR, and others.
- **Optimize business operations**: A well-organized data process will give you a deeper understanding of your data, and risk management by allowing you to evaluate the effect of a data breach if it happens, and provide useful capabilities for record retention and legal discovery.

Privacy Officer as a Service (POaaS)

Adnovum can provide a Privacy Officer as a Service for your company. As a result, Adnovum will be your first point of contact for questions related to the processing of personal data.
Among other tasks, the POaaS delivers the following:

- Check and evaluate data processing in the cloud, on-prem and hybrid
- Document the processing of data
- Assess the technical and organizational measures related to data security
- Check on ordered processing of third parties' data; including cross-border data processing agreements, contractual protection, and more
- Consult on the processing of personal data
- Prepare employees with trainings and awareness campaigns
- Communicate with supervisory authorities and affected parties

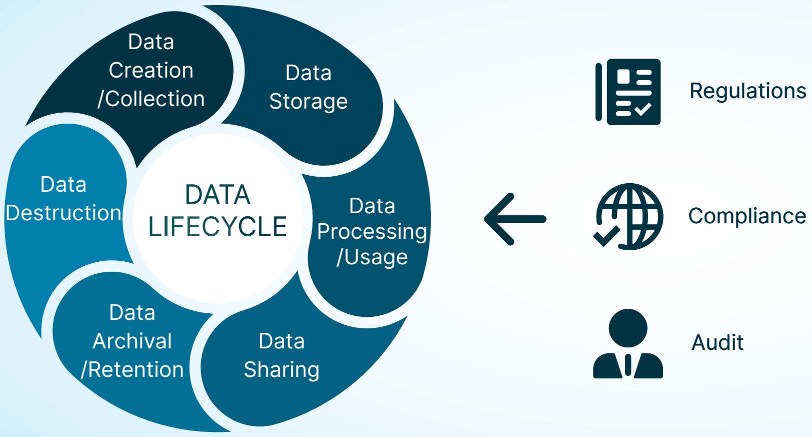
DATA PROTECTION AND SECURITY

Data breaches incur destructive consequences, including financial loss, reputation damages, operational disruption, legal action, and loss of sensitive data. According to IDC, organizations endure an average total cost of US$ 3.86 million for every data breach incident in 2020.

The following are some of the most common reasons for targeted data breaches:

- Exploiting system vulnerabilities
- Weak passwords
- Structured Query Language (SQL) injection
- Spyware
- Phishing
- Drive-by downloads
- Broken or misconfigured access controls

The Role of Data Lifecycle Management



> “A data lifecycle management strategy enables organizations to manage compliance at each stage, by specifying a range of technologies and services that can keep costs under control. It also mitigates the risk of non-compliance.”

Adnovum assists you in the implementation of data protection requirements throughout your data life cycle management.

- **Analysis:** Enables you in identifying and analyzing assets (data, data flows, systems and processes) and creating an overview of your data landscape. Next, we develop a plan and big picture scope with measures and activities, specifically for your situation and organization setup.
- **Implementation:** Assists you with the implementation of the defined measures and activities and provides consultation regarding the implementation of tools and processes to ensure compliance with data protection regulations (e.g. GDPR, PDPA, etc.)
- **Monitoring:** Supports you in developing and establishing a monitoring process to ensure that the defined measures work as intended, including testing and certification.

A Comprehensive Security Strategy Transforms an Organization’s Agility and Competitiveness

Cybersecurity is not a static challenge; the threats to a business's IT environment evolves over time, just like the technology required to resist such attacks. For example, benefiting from the coronavirus pandemic, hackers expanded their campaigns of attacks against businesses worldwide with 238% rise in attacks on banks, and a 600% increase in attacks on cloud servers from January to April 2020 alone (Forbes, 2021).

For security and IT leaders, new data security challenges include limited visibility, sophisticated cyberattacks, and a growing skills shortage, all while working to meet regulatory compliance. Yet, overcoming these challenges could create opportunities for an organization.

SECURITY CONTROL FUNCTIONS

	Preventive	Detective	Corrective
Definition	Any measure of security implemented that is deterrent in nature, and prevents security threats or unauthorized activities from occurring.	Any measure of security implemented to detect, notify and/or send an alert regarding security threats or unauthorized activities upon occurring.	Any steps, measures and/or procedures taken to **repair damages, and restore services, resources and capabilities** to a good state after any security threat or unauthorised activity has occurred.
Example	Biometric checkpoints, security patrols, antivirus software, firewalls, IPSs, separation of duties.	Surveillance sensors for unauthorised activities, IDSs, honeypots, SIEMs.	Vulnerability patching, quarantine virus, activating BCP failover/disaster recovery, incident response plan, and corporate communications for data breach.

A Complete Security Strategy From Management to Architecture and Technology

- Information Security Management: Adnovum's Information Security Management can assist in strengthening your cloud and data security management with the implementation of information security policies and concepts, as well as project-related support, risk assessments, vulnerability scans or penetration testing. In addition, we can take care of those aspects for you in the role of an Information Security Officer as a Service.
- Security Architecture and Technology: At the beginning, we will conduct a thorough analysis of the security requirements of a solution. This is crucial for its successful design and implementation. Upon completion, the system needs to be assessed periodically, to withstand ever-evolving cyber-security threats.

NEXT STEPS – GAINING THE COMPETITIVE ADVANTAGE

"Adnovum empowers businesses in mastering their digital potential to build trust, confidence and beyond."

ISO
ISO 27701

GDPR

DATA PROTECTION ASSURED

PCI

- ✓ Organizational/compliance certification to open up business growth potentials.
- ✓ Good understanding of data security, privacy and protection laws and regulations applicable to your organization, territory and services offered. This creates the foundation to achieve certifications in industries and areas targeted for growth.
- ✓ Demonstration of a comprehensive organization-wide Data Security, Privacy and Protection Management Program could enhance your business culture.
- ✓ Robust enterprise-level capability and maturity to data security, privacy and protection can keep your customer data and valuable intellectual property information from falling into the wrong hands and stay ahead of the competition.
- ✓ Readiness and effectiveness to remediate, notify, communicate, report and recover when a data breach incident occurs. This helps protect brand image and mitigates fallout matters.
- ✓ Continuous monitoring and good cyber security hygiene protects your organization against advanced cyber attacks.

OUR CUSTOMER

InfoSec for Finance Regulatory Authority of Singapore

The eGov Secure Collaboration Suite (SCS) enhanced data security via the implementation of 2FA, E2EE and policy-based security controls.

Adnovum Singapore Pte Ltd
3 Shenton Way, Shenton House, #23-03, S068805
Locations: Zurich (HQ) I Bern I Budapest I Ho Chi Minh City I Lausanne I Lisbon I Singapore

☎ +65 6536 0668
✉ info@adnovum.sg
www.adnovum.com