CASE STUDY

Enhancing Data Security and Compliance
with Microsoft 365 Sensitivity Labels

November, 2024

Authored By: Rajesh Lohar
Emai: rajesh.lohar@ignatiuz.com

Introduction

Microsoft 365 Sensitivity Labels are an essential feature of Microsoft 365's Information Protection (MIP) framework, designed to help organizations classify, protect, and manage sensitive data. These labels enforce protection actions such as encryption, access control, and information-sharing restrictions, enabling organizations to ensure that sensitive information is handled securely while complying with global regulations such as GDPR, HIPAA, and CCPA.

This case study explores how a global technology leader with operations in over 20 countries and 15,000 employees implemented a complex Microsoft 365 Sensitivity Labeling solution to address data protection needs across various regions and business units.

Problem Statement

The client, a leading technology company, handles a diverse range of sensitive data, including personal information, intellectual property, financial records, and legal contracts. With a global workforce, the company operates in several highly regulated sectors and must ensure compliance with local and international data privacy regulations. Managing sensitive data across departments, regions, and compliance frameworks posed significant challenges, especially when balancing automation with manual oversight of labeling processes. The company sought to streamline its data protection efforts, improve collaboration, and ensure compliance across all levels.

Challenge

1

Diverse Sensitivity Needs Across Business Units:

The Legal Department required strict protection for contracts, third-party agreements, and intellectual property. The R&D Department managed highly sensitive product designs, patents, and research data. The HR Department handled employee data, payroll information, and health records. Meanwhile, Sales & Marketing needed to secure customer data while ensuring smooth internal collaboration.

2

Compliance with Multiple Regulatory Frameworks:

The company operates across various regions, requiring compliance with different data protection regulations, including GDPR (EU), CCPA (California, USA), and HIPAA (healthcare data in the U.S.).

3

Compliance with Multiple Regulatory Frameworks:

The company operates across various regions, requiring compliance with different data protection regulations, including GDPR (EU), CCPA (California, USA), and HIPAA (healthcare data in the U.S.).

4

Compliance with Multiple Regulatory Frameworks:

The company operates across various regions, requiring compliance with different data protection regulations, including GDPR (EU), CCPA (California, USA), and HIPAA (healthcare data in the U.S.).

5

Compliance with Multiple Regulatory Frameworks:

The company operates across various regions, requiring compliance with different data protection regulations, including GDPR (EU), CCPA (California, USA), and HIPAA (healthcare data in the U.S.).

Project Details

To address these challenges, the organization implemented a comprehensive Microsoft 365 Sensitivity Labeling framework. This involved designing and applying a series of customized sensitivity labels, setting up automated policies, and establishing manual workflows to ensure that sensitive data was classified and protected in alignment with the company's diverse needs.

1

Label Design:

A layered framework was developed, incorporating global, department-specific, and region-specific labels. Global labels included Public, Internal, and Confidential. Department-specific labels were tailored to areas like Legal, R&D, HR, and Customer Data. Region-specific labels included Confidential classifications based on local regulations, such as EU (GDPR), US (CCPA), and HIPAA.

2

Label Policies:

A combination of automatic and manual labeling was implemented, with automatic labeling policies for detecting PII, GDPR, and CCPA-related data, and manual labeling for highly sensitive content like legal and R&D data.

3

Policy Enforcement:

Policies for encryption, access control, and sharing restrictions were applied to ensure that labeled content was adequately protected.

4

Cross-Department and Regional Collaboration:

Labeling was customized for various departments, and cross-department workflows were set up to ensure proper use of labels. The project involved close coordination between departments like Legal, R&D, HR, and Sales to manage their specific needs.

5

Monitoring and Reporting:

Continuous auditing was implemented through audit logs and tools like Content Explorer, allowing the organization to monitor label application and ensure compliance.

Solution Summary / Results and Benefits

1 Improved Compliance: The labeling system ensured that the company adhered to regulatory requirements, including GDPR, CCPA, and HIPAA, with automatic labeling applied to data governed by these laws.

2 Enhanced Data Security: With automated encryption and access controls based on sensitivity labels, sensitive data was better protected from unauthorized access and breaches.

3 Efficient Collaboration: Teams could collaborate securely on documents, knowing that appropriate restrictions were in place based on the sensitivity of the information.

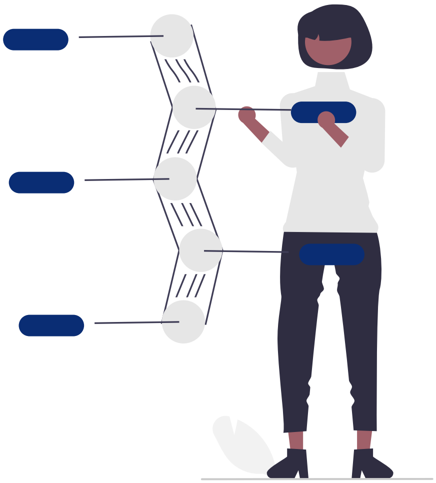
4 Reduced Risk of Mislabeling: By automating the labeling process for certain data types (e.g., PII, GDPR-related data), the company minimized the risk of human error while allowing manual labeling for more critical data.

5 Scalable Solution: The framework was designed to scale across a global workforce, ensuring consistent label management and policy enforcement across all departments and regions.

6 Audit and Monitoring: The implementation of auditing and monitoring tools allowed the company to ensure that labels were applied correctly and that sensitive data was handled according to policy.

Conclusion

Through the implementation of Microsoft 365 Sensitivity Labels and a carefully designed labeling framework, the organization successfully addressed its data protection challenges across multiple departments and regions. By balancing automated labeling with manual oversight, the company ensured secure data management, complied with complex regulatory requirements, and enabled efficient collaboration across its global workforce. This solution not only helped protect sensitive information but also improved the organization's ability to collaborate securely while maintaining compliance in a highly regulated environment.



Resources

For further details on setting up and managing Microsoft 365 Sensitivity Labels, please refer to the following resources:

Click Here → Sensitivity Label Configuration Policy

Click Here → Sensitivity Label Configuration

Click Here → Label Assignment for Existing and New Groups