# Micro Focus Data Privacy Manager

## Manage and protect privacy throughout the lifecycle of data

**Key Benefits**

- **Time-to-Compliance:** Built-in classification libraries, pre-set rules and discovery speed implementation.
- **Transparency:** Data privacy governance from a single pane of glass across Hybrid IT.
- **Productivity:** Manage and protect data on production databases without stopping business operations.
- **Usability:** Protect data while keeping it usable for analytics and business processes.
- **Defensible Disposition:** Document actions step-by-step and product compliance reporting.

### The Privacy Challenges of Data-Driven Businesses

Today's data-driven businesses rely on analytics insights for creating customer value, maximizing operational efficiencies and achieving competitive advantage. More data than ever before is captured and flows throughout the entire enterprise, from millions of IoT smart devices at the edge of the network, through thousands of applications, to repositories on-premises, and on public and private cloud. But among the terabytes of data captured by enterprises, there is highly sensitive information that if breached, could be the ultimate nightmare of corporate executives. Breaches can and do lead to loss of revenue and a decline in brand loyalty which companies and valued employees have worked tirelessly to build up over the years.

The challenge is that as data moves across modern IT in ever growing volumes, current security and privacy controls—with no coordination between silos and no central policy management—become ineffective. Businesses don't know what this sensitive data is, where it's located, where it flows, who is using it and they have no central control over their data privacy policy management and governance. Raising the stakes, GDPR and other privacy legislation make data privacy requirements stricter, increasing penalties for data breaches and requiring central control of sensitive data usage and disposition for reliable privacy controls.

A new approach is needed where sensitive data is identified, classified and protected from a central location through a single pane of glass, applying the appropriate level of

privacy controls to data according to its sensitivity and usage needs.

**The Need for Data Privacy Management**
In order to achieve sensitive data privacy in this new environment, businesses need to orchestrate and govern data privacy at a higher level, achieving complete visibility and creating greater efficiencies that eliminate gaps in controls and integrates enterprise policy consistently. By engaging key stakeholders such as business, IT, governance, compliance and security, enterprises can create a holistic view of data privacy policy across its lifecycle and security needs. This comprehensive "Data Privacy Management" approach allows organizations to automate the process and define appropriate enterprise-wide privacy policy based on the sensitivity of the data and create a balance between risk exposure and the need to use data for competitive advantage.

The critically important capabilities of data privacy management include the ability to identify and classify sensitive data anywhere in the enterprise. The ability to automate and to manage sensitive data centrally by policy, to apply the necessary protection to data while maintaining usability for business processes, and the creation of audit reports for control attestation to maintain regulatory privacy compliance.

**Introducing Micro Focus Data Privacy Manager**
Micro Focus Data Privacy Manager integrates two industry-leading Micro Focus information governance and security products, Structured Data Manager and SecureData, to provide a comprehensive solution to address the privacy governance needs of enterprises with sensitive structured data. The Data Privacy Manager solution enables customers with the ability to manage and protect sensitive structured data throughout its lifecycle, from discovery and classification to protection and reporting.

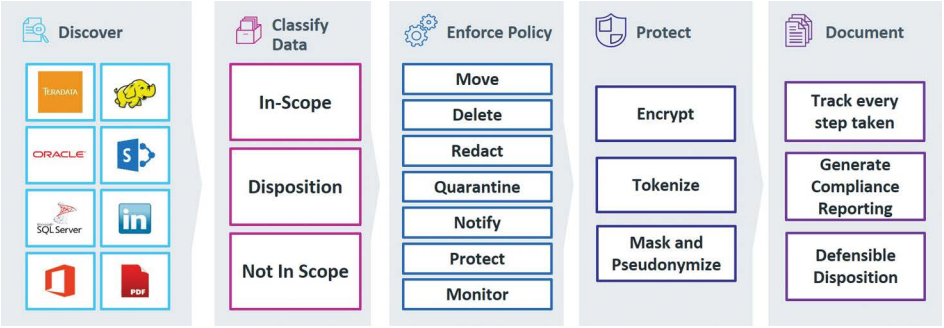


**Figure 1.** Data Privacy Manager

**Data Privacy Governance from a Single Pane of Glass**
The Data Privacy Manager enables enterprises to discover sensitive data throughout Hybrid IT and classify in-scope data for disposition. Data is then dispositioned based on pre-set policies, defining archival, protection, deletion and other dispositions.

The Data Privacy Manager adds end-to-end data privacy protection to sensitive data by leveraging Hyper Format Preserving Encryption (FPE), protecting data over its entire lifecycle—from the point at which it's captured and throughout its movement across the extended enterprise, without gaps in protection. Hyper FPE de-identifies data, rendering it useless to attackers, while maintaining its usability and referential integrity for data processes, applications and services.

Completing the process, Data Privacy Manager records actions taken in the process and can produce detailed reports for compliance audits. Most of all, it performs all these functions through a user-friendly interface that allows structured data to be managed throughout the enterprise from a single pane of glass.

**Data Privacy Manager Main Features**

- Discover: Find sensitive structured data in active and inactive systems across the enterprise.
- Classify: Analyze and classify data such as names, social security numbers, IDs and more based on-pre-set libraries.
- Enforce: Enforce centrally-set privacy and security policy and manage data across the enterprise from a single pane of glass (e.g., move, delete, quarantine, notify or protect).
- Protect: Mask or Pseudonymize sensitive data using encryption and tokenization, protecting privacy while keeping it usable for business processes and analytics.
- Document: Document every action taken throughout the process and generate reports for compliance audits.

**Micro-Focus: Industry-Leading Information Governance and Security Portfolio**
Micro Focus has one of the most comprehensive information governance and security portfolios in the world. Our solutions allow businesses to manage, govern and secure information; detect and respond to data breaches and govern identity and access. Information governance and security solutions in our portfolio include:

- Unstructured Data Management: ControlPoint is an advanced file analysis tool facilitating information governance for connected data sources around unstructured data. ControlPoint simplifies the definition and application of policy—regardless of data format or location.

- **Automated Content Classification:** Content Manager is a governance-based enterprise content management system designed to help government agencies, regulated industries and global organizations manage their business content from creation to disposal.
- **User Behavior Analytics (UBA):** ArcSight User Behavior Analytics (UBA) enables security analysts to minimize the risk and impact of cyberattacks in real time. ArcSight UBA detects unknown threats through purpose-built security analytics by creating a baseline of normal user and entity behavior and identifying anomalies associated with users and entities as they occur.
- **Identity Governance:** Identity Governance is a solution that helps any organization run effective access certification campaigns and implement identity governance controls to meet compliance mandates while proactively mitigating risk.
- **Application Security:** Fortify offers end-to-end application security solutions with the flexibility of testing on-premises and on-demand to cover the entire software development lifecycle, enabling time to market by building security in.

**The Data Privacy Manager was formed by the integration of 2 leading products:**

Micro Focus Structured Data Manager enables the complete management of structured data across its lifecycle. Structured Data Manager (SDM) can discover sensitive data in on-premises, cloud or hybrid systems and classify in-scope data for disposition. SDM enables policy-based disposition of data, defining archival, protection, deletion or any other disposition based on pre-set company policy. Completing the process, Structured Data Manager records all actions taken and can produce detailed reports for compliance audits. SDM performs all that through a user-friendly interface that allows structured data to be managed throughout the enterprise from a single pane of glass.

Micro Focus Voltage SecureData provides an end-to-end data-centric approach for enterprise data protection. By leveraging Hyper Format Preserving Encryption (FPE), SecureData protects data over its entire lifecycle—from the point at which it's captured and throughout its movement across the extended enterprise, without gaps in security. SecureData "de-identifies" data, rendering it useless to attackers, while maintaining its usability and referential integrity for data processes, applications and services.

Data protection and usability: Hyper FPE delivers data protection while maintaining usability for analytics and business processes, ensuring protection without loss of competitive edge. Hyper FPE encrypts virtually unlimited data types, including IDs, VINs or bank accounts, while preserving their formats, so they can flow through existing databases and applications. Hyper FPE also maintains relationships, context and meaning of data so that analytics can be performed on de-identified data powering big data, cloud, and IoT initiatives.

Whether customers are trying to comply with legislation such as GDPR, protect big data projects, adopt hybrid IT, or just protect legacy systems, the Data Privacy Manager provides for management and protection of structured data privacy throughout its lifecycle. Enterprises are able to comprehensively discover, classify, protect, manage and audit sensitive data across the organization: in the cloud, legacy systems, and production or storage servers.

Contact us at **CyberRes.com**
Like what you read? Share it.



CyberRes
A Micro Focus line of business