White Paper

Security, Risk and Governance

A Single Global Privacy Framework for Risk Reduction & Value Creation

MICRO FOCUS

Table of Contents

page

The Micro Focus Single Global Privacy Framework for Risk Reduction and Value Creation has five critical technology capabilities to support an organization's digital transformation journey, and is underpinned by an advanced analytics ecosystem to provide deep information insight.

Introduction

Digital transformation has created a revolution, but with its increased benefits come increased risks to personal information. In response, several countries have enacted privacy and data protection legislation to protect consumers.

In this environment, organizations need a privacy protection framework that is broad enough to cover the needs of global privacy requirements, yet flexible enough to support the needs of enterprises in different stages of maturity—and, it requires analytics at the core. Micro Focus is uniquely suited to help customers reduce these risks, yet create value while meeting privacy requirements. The Micro Focus® Single Global Privacy Framework for Risk Reduction and Value Creation has five critical technology capabilities to support an organization's digital transformation journey, and is underpinned by an advanced analytics ecosystem to provide deep information insight.

Digital Transformation Drives Privacy Concerns

The digital revolution is changing our lives. Social media, digital collaboration, and online shopping all make life easier and richer. Users have wholeheartedly adopted digital platforms and shared information about their interests, desires, and connections. The information now available in the digital universe is a goldmine for enterprises.

In fact, total enterprise data volume is growing exponentially and will reach an estimated 163 zettabytes by 2025. That's ten times the estimated 16 zettabytes of data generated in 2016[1]. The insight from this data drives modern corporations, enabling analysts not only to understand and serve customers better, but also to identify and understand trends and respond to them faster than before.

However, the digital transformation is also a significant vulnerability when it comes to protecting privacy. Among the massive volumes of data captured by enterprises is personal information that, if shared without consent or stolen, could lead to loss of trust, brand damage, and penalties from ever-stricter privacy regulations. In the age of digital transformation, this risk exposure is exponentially more dangerous. With enterprises capturing personal information, health information, and more new classes of sensitive data than ever before, even data that doesn't appear to be sensitive at face value could be combined with other pieces of data to reveal identity.

The Global Privacy Movement

2018 was the year when privacy became mainstream news and consumers realized the price they pay for the convenience of digital services. Around the world, consumers saw their privacy protections evaporate. Social media users saw their data sold without their consent. Data breaches in major organizations brought the vulnerability of enterprise systems and their inability to protect personal data to center stage.

1 *Data Age 2025: Don't Focus on Big Data; Focus on the Data That's Big, IDC, April 2017*

As consumers became aware of the vulnerability of their personal information online, regulators and legislators worldwide took notice.

2018 was also the year when the most stringent privacy regulation to date, the European Union's General Data Protection Regulations (GDPR), came into effect. The GDPR—with its stricter rules, stiff penalties, and global reach—was a milestone in the protection of consumer privacy and provided a template for other countries and states in their pursuit of privacy protections.

The Challenges of Global Privacy Requirements

In several countries, we have seen the advance of major privacy and data protection legislation to protect consumers in the digital universe. The state of California, the world's 5th largest economy by GDP and home to some of the largest tech companies in the world, has passed a sweeping consumer privacy bill similar to the GDPR. The California Consumer Privacy Act[2] (CCPA), which takes effect on January 1, 2020, will require companies around the world to observe specific regulations when handling the personal data of California residents.

Brazil has also just passed its own General Data Protection Law[3] or LGPD (acronym derived from original Portuguese). Similar to both the GDPR and CCPA, LGPD applies to any company that has a branch in Brazil or offers services to the Brazilian market and collects and treats the personal data of data subjects located in the country, regardless of the nationality. And that's just the beginning. Both Argentina and India have bills in final stages being considered in their legislatures, and other countries have started their own working groups to consider privacy matters.

A Patchwork without a Framework

These new national laws will join the ranks of existing data protection and privacy legislation already in effect, such as PIPEDA in Canada, Australia's Privacy Act, Japan's APPI, and many others. This, together with healthcare and financial legislation with heavy emphasis on data protection and privacy (such as such as HIPAA and NYDFS), presents organizations with an extremely challenging privacy compliance environment. Even laws that might be considered "similar" have significant differences. Each one has different requirements, obligations, and penalties—many of which are open to interpretation. The end result is that enterprises are faced with a complex patchwork of overlapping privacy legislation without a unified technology framework to address them.

Current Privacy Protection Approaches Fall Short

Enterprises are between a rock and a hard place. The insights of data analytics and the flexibility of hybrid IT are essential to their business. But the digital transformation that is key to their business success and competitive advantage is also a major vulnerability when it comes to privacy protection. CEOs and CIOs are rightly concerned that privacy protection could become a hindrance to their digital transformation and, consequently, to their competitive advantage and business success—especially when considering most solutions that are currently available.

Organizations must ensure that they are starting their privacy protection journey correctly. Laying a solid foundation and asking the right questions is critical to understanding how a company is affected by each article within privacy regulations.

2 *GDPR matchup: The California Consumer Privacy Act 2018, July 2018, IAPP*
3 *GDPR matchup: Brazil's General Data Protection Law, Oct 2018, IAPP*

A successful privacy framework must be comprehensive, flexible, automated, and transparent. This framework must be able to identify, analyze, govern data and identities, act on data based on policy, and secure data, identities, and apps.

Current approaches to addressing global privacy are ineffective and handicap an enterprise's ability to gain competitive advantage. Today's privacy enforcement solutions are often a loose collection of point products from multiple vendors, which increases maintenance costs, management resources, and security risk. As a result, businesses often can't answer common questions such as: Where is data most vulnerable to misuse? How do I implement the most appropriate protection? How are the identities managed to ensure privacy? Can I ensure the "right to be forgotten"? What applications and users should have access to sensitive data?

The fragmented nature of the global privacy landscape has led to an equally fragmented readiness status for enterprises. For example, European Union businesses might have already conducted a personal data assessment and know what data they possess and where it is stored. They must now act upon that data and plan for its governance and protection throughout the entire information lifecycle. On the other hand, enterprises in other regions or verticals might only be starting their journey.

In this environment, organizations lack a flexible framework that can scale out globally to meet the needs of enterprises at all maturity levels, while offering consistency and reusability as privacy requirements evolve. Without a repeatable framework, an approach might not be broad enough or reliable enough to meet future application needs or be able to respond to new data types that become the focus of new rules and regulations.

The Technology Building Blocks of a Privacy Framework

Organizations must ensure that they are starting their privacy protection journey correctly. Laying a solid foundation and asking the right questions is critical to understanding how a company is affected by each article within privacy regulations. It helps to answer and address critical questions such as:

- What is my readiness status?
- Where is the information and sensitive personal data that will fall under these regulations?
- How can I respond to legal matters requiring information under my management?
- How do I best ensure that structured and unstructured sensitive data is protected, stored, and backed up securely across my hybrid IT real estate?
- How do I govern data, identities, and access centrally according to policy and enforce it across the enterprise?
- Can I report a breach within the timeline required by the GDPR and similar legislation?
- How do I reduce my overall risk profile?
- Can I provide a platform where users can self-manage accounts and privacy controls?

Attributes of a Single Framework

As enterprises attempt to meet new privacy requirements, the outline of a successful privacy framework becomes clearer. It needs to be broad enough to encompass the extensive needs of global privacy requirements and flexible enough to meet the needs of enterprises in different stages of maturity. It requires analytics at the core, to speed data discovery of billions of records and the automation of policy enforcement over large volumes of data. This framework needs to be:

- **Comprehensive:** It should take into consideration the needs of the entire enterprise, particularly in the areas of risk assessment and classification; information, identity, and access governance; and encryption and identity protection.
- **Flexible:** Regardless of the current level of maturity, a flexible, scalable framework should offer the ability to address today's mandates and then adapt as they evolve, to lower the risk of abuse and compromise—no matter what any new legislation will bring.
- **Automated:** Automation of governance and security controls is essential when enforcing policies across an enterprise's hybrid IT infrastructure on billions of records, especially in environments with limited resources.
- **Transparent:** Privacy controls cannot slow down the business. Instead, they must accelerate opportunities for value creation through handling data responsibly and appropriately, such as optimizing business efficiency through greater insights.

Any privacy protection program should take into consideration the needs of enterprises in order to succeed in today's competitive environment. The program needs a broad, scalable, flexible framework to meet an enterprise's varied needs, while also enabling controls that can become a source of value creation for the company, rather than a hindrance.

Key Functionality Requirements of a Single Framework

Let's look deeper into the actual functionality needed in a single technology framework that's flexible enough to serve a broad range of privacy regulations. This framework must be able to:

1. **Identify:** One of the biggest problems for enterprises is to assess their risk profile. They must understand their privacy readiness and risk exposure in relation to all major privacy regulations that they might be subject to. This means identifying information that might be relevant to privacy requirements in a streamlined/automated fashion and assessing the current access control policies to sensitive data.
2. **Analyze:** Enterprises must have built-in analytics to automatically identify and classify structured and unstructured data for disposition that might be subject to privacy requirements. They must assess activities that are outliers to the norm and spot anomalies in user activity. The framework must combine real-time analytics and guided optimization to help ensure that information is backed up, in order to deliver cost savings while meeting privacy requirements.

The Micro Focus Single Global Privacy Framework is flexible enough to meet the needs of broad privacy legislation for enterprises in different phases of maturity, but is specific enough to offer a step-by-step guide to risk reduction.

Micro Focus has an integrated portfolio that addresses all key areas of protecting data privacy, underpinned by an advanced analytics ecosystem to provide deep information insight for automated policy setting.

3. **Govern data and identities:** Governance is the beginning and end of a privacy compliance program. Technology tools for security or for disposing of data are useless if they aren't governed and appropriately managed. Through data, identity, and access governance, enterprises can centrally define policies and perform privacy case management, implement personal data and access controls, implement privacy compliance risk systems, and provide comprehensive employee training.
4. **Act on data based on policy:** Once enterprises define how they will locate and govern their sensitive data, they are able to act on the data based on governance policies. Enterprises must be able to protect data using encryption, but still enable data to be used for business processes and analytics. They must implement access policies to this data and implement data quality maintenance with deletion/suppression and effective breach response.
5. **Secure data, identities, and apps:** Organizations need to take a holistic approach to protect identities, apps, and data. They need to assure security and governance professionals that they have reduced breach risk, are guarding the privacy of individuals and their data, and are complying with regulatory and jurisdictional regulations—at scale, with ease, insight, and confidence.

Micro Focus: A Single Global Privacy Framework for Risk Reduction and Value Creation

Micro Focus has an integrated portfolio that addresses all key areas of protecting data privacy, underpinned by an advanced analytics ecosystem to provide deep information insight for automated policy setting. Micro Focus is uniquely suited to help customers reduce risk while creating value when meeting privacy requirements around the world.

The Micro Focus Single Global Privacy Framework for Risk Reduction and Value Creation has five critical technology capabilities to support an organization's journey[4]. It's flexible enough to meet the needs of broad privacy legislation for enterprises in different phases of maturity, but is specific enough to offer a step-by-step guide to risk reduction.

4 *Based on Pricewaterhouse-Coopers (PwC) framework for evaluating GDPR technology, Feb 2017*

Identify

Personal Data Assessment
Quickly and cost efficiently determine what data falls in scope of privacy regulations, and then apply policies to move, redact, encrypt and dispose of personal data in accordance with privacy policy.

Analyze

Defensible Disposition
Automatically identify structured and unstructured data for disposition that may be subject to privacy rights to erasure requirements, leading to lower storage costs and lower risk.

Backup and Recovery
Combine real-time analytics and guided optimization to help make sure information is backed up at the right time, in the right way, on the right medium to deliver cost savings while meeting privacy requirements.

Govern

Policy-Based Governance
Effectively apply and enforce data and identity-based policies to manage information privacy and access, while streamlining and driving cost efficiencies.

Litigation Management
Maintain legal preparedness by being able to quickly and accurately respond to litigation and investigations with the right information in the right time, lowering risk of data spoliation.

Act

Encryption
Provide a proven, standards-based approach that meets criteria for use of data masking to protect personal data, without breaking existing business process.

Breach Detection, Response & Reporting
Enable analysts to investigate alerts faster and with better insights using analytics-driven, guided investigation tools, accelerating detection and remediation to comply with notification guidelines.

Secure

Breach Prevention
Find known and unknown threats in real-time through powerful correlation and context, integrated with the leading user behavior analytics solution. Close security gaps and prevent high-value data loss by protecting personal data at data field level, preventing unauthorized access, and automatically identifying application vulnerabilities.

The Micro Focus Global Privacy Framework enables companies not only to reduce risk, but also to speed up their digital transformation and increase operational efficiencies and value creation.

By using a broad framework, Micro Focus enables customers to streamline information classification by automatically identifying the most critical and sensitive data. The identification and categorization of data will enable them to apply governance policies, detect and respond to data breaches, optimize backup and recovery, and ultimately protect data in use, in transit, and at rest.

Mapping Micro Focus solutions to the Global Privacy Framework for Risk Reduction and Value Creation
Micro Focus delivers a flexible, modular, intelligent set of solutions that help customers identify and take action on data that might be subject to privacy regulations. Our market-leading security and information management and governance software is mapped to eight specific privacy use cases that help to support an organization's global privacy programs.

Micro Focus delivers a flexible, modular, intelligent set of solutions that help customers identify and take action on data that might be subject to privacy regulation

Mapping Micro Focus Solutions to the Global Privacy Framework for Risk Reduction and Value Creation

Micro Focus delivers a flexible, modular, intelligent set of solutions that help customers identify and take action on data that might be subject to privacy regulations. Our market-leading security and information management and governance software is mapped to specific privacy use cases that help to support an organization's global privacy programs.

Personal Data Assessment	Defensible Disposition	Backup and Recovery	Policy-Based Governance
Determine data in scope of privacy regulations; apply policy to move, redact, encrypt and dispose of personal data in accordance with privacy policy.	Automatically identify structured and unstructured data that may be subject to privacy rights to erasure, leading to lower storage costs and risk.	Combine real-time analytics and guided optimization to help ensure data is backed up to deliver cost savings while meeting privacy requirements.	Effectively apply and enforce data and identity-based policies to manage information and access, while streamlining and driving cost efficiencies.
▪ **Micro Focus ControlPoint** ▪ **Micro Focus Structured Data Manager**	▪ **Micro Focus ControlPoint** ▪ **Micro Focus Structured Data Manager**	▪ **Micro Focus Adaptive Backup and Recovery Suite**	▪ **NetIQ Identity Governance** ▪ **Micro Focus Secure Content Management Suite** ▪ **Micro Focus Digital Safe**

Litigation Management	Encryption	Breach Detection, Response & Reporting	Breach Prevention
Maintain legal preparedness to quickly, accurately respond to litigation and investigations with right info in the right time, lowering risk of data spoliation.	Provide a proven, standards-based approach that meets criteria for use of data masking to protect personal data, without breaking business process.	Enable analysts to investigate faster, with better insight via analytics-driven tools, accelerating detection & remediation to comply with notification guidelines.	Find threats real-time, prevent data loss at field level, prevent unauthorized access and automatically identify application vulnerabilities.
▪ **Micro Focus Digital Safe Suite**	▪ **Voltage SecureData** ▪ **Voltage SecureMail**	▪ **ArcSight & UBA** ▪ **Voltage SecureMail**	▪ **NetIQ Identity & Access Management** ▪ **Voltage SecureData** ▪ **Voltage SecureMail** ▪ **Micro Focus Fortify**

Identify

PERSONAL DATA ASSESSMENT

By automating and removing costly and error-prone manual processes (such as data mapping of structured and unstructured data, and personal data analysis and tagging), Micro Focus classification technologies simplify the critical first step of meeting privacy legislation requirements, which have historically been a barrier to accomplishing this task. Our solutions enable an understanding of your privacy readiness and risk exposure, identifying information that might be relevant to specific regulatory requirements in a streamlined, automated fashion, and can systematically apply policies to applicable information for security, data protection, and lifecycle management purposes.

Analyze

DEFENSIBLE DISPOSITION

Answering the critical question, "How do I identify information for disposition that might be subject to 'the right to be forgotten'?" is accomplished with rich Micro Focus analytics. Our solutions bridge formerly distinct data silos, deliver granular insight into information, and surface highly critical and sensitive data (such as personal information) that might be subject to privacy legislation.

BACKUP AND RECOVERY

Micro Focus combines real-time analytics and guided optimization to help ensure that information is backed up at the right time, in the right way, and on the right medium, based on its relative importance to privacy requirements—delivering cost savings while meeting strict recovery and service-level expectations.

Govern

POLICY-BASED GOVERNANCE

The application and enforcement of policies to manage information throughout its lifecycle can be achieved using Micro Focus information governance solutions. Armed with deep insight into customer data, organizations can streamline and drive cost efficiencies into the process of protecting, leveraging, and taking action on this information. Micro Focus can also help you meet regulatory mandates by managing the data retention, supervision, surveillance, and disposition across your electronic communications channels. Identity and access governance are also key aspects of privacy compliance that Micro Focus provides. Micro Focus identity solutions help any organization run effective access certification campaigns and implement identity governance controls to meet compliance mandates, while proactively mitigating risk.

LITIGATION MANAGEMENT

Micro Focus can also enable organizations to respond quickly and accurately to litigation, with the right information at the right time. We provide solutions to help organizations maintain legal preparedness and to quickly and accurately respond to legal matters, investigations, early case assessment, eDiscovery, and legal hold applications. Our solutions can also lower the risk of accidental data spoliation, reduce the time of eDiscovery, and lower the costs related to the manual review of information.

Act

ENCRYPTION

The GDPR and other legislation provide guidelines around the use of encryption and pseudonymization as appropriate approaches to mitigate risks associated with the processing of sensitive personal data. Micro Focus provides proven, standards-based solutions to protect sensitive personal data that meets these criteria without breaking existing business process. Micro Focus technology preserves business functionality and data value for analytics, serving encryption and pseudonymization requirements while filling the requirements for full anonymization and "the right to be forgotten."

BREACH DETECTION, RESPONSE, AND REPORTING

Micro Focus solutions provide an industry-leading way to automatically detect the early stages of attacks by filtering out false positives, using big data analytics across multiple data control points. These solutions enable organizations to put in place granular controls and monitoring, as well as to rapidly and effectively comply with notification guidelines in the GDPR and many other privacy laws, giving them the means to stop data breaches as they happen.

Micro Focus solutions provide an industry-leading way to automatically detect the early stages of attacks by filtering out false positives, using big data analytics across multiple data control points.

With Micro Focus, firms are able to scale analytics initiatives by working on encrypted data that allows analytics to be performed, but is useless to attackers.

Secure

BREACH PREVENTION

Micro Focus solutions also support the need to deploy cyber-security technologies to identify vulnerabilities, close security gaps, and prevent high-value data loss through a breach. These solutions enable organizations to protect structured and unstructured sensitive data-at-rest, data-in-motion, and data-in-use throughout the enterprise.

IDENTITY AND ACCESS MANAGEMENT

With Micro Focus identity and access management solutions, enterprises can quickly and cost-effectively integrate identity and access policies across local, mobile, and cloud environments. Micro Focus IAM solutions use integrated identity information to create, modify, and retire identities and control their access.

APPLICATION SECURITY

Through Micro Focus application security solutions, application vulnerabilities can be automatically identified in source code and with recommendations to code-level changes, to remediate these vulnerabilities. These solutions include capabilities to automatically protect running .NET and Java applications from known vulnerabilities, add critical support to help deliver strong applications development, and help mitigate key areas of risk in business processes.

Privacy as an Enabler of Digital Transformation and Value Creation

The Micro Focus Global Privacy Framework for Risk Reduction and Value Creation enables companies to not only reduce risk, but also to speed up their digital transformation and increase operational efficiencies and value creation.

Micro Focus enables enterprises to map the lifecycle of data, from when data comes into the enterprise; how it is handled, stored, protected; and how it is treated at the end of life. By modeling and taking control of the lifecycle of data, enterprises are not only taking steps toward privacy protection, but are also building the essential blocks to manage personal data in a way that helps them make more informed decisions—creating a better experience for both customers and stakeholders.

Streamlining data governance also enables enterprises to find redundant data, data that can be disposed of, and data that should be moved to more efficient repositories. This encourages firms to replace legacy systems and adopt flexible cloud services, enabling rather than hindering the digital transformation.

Another enabler of digital transformation is the improved security. By securing data, identities, and apps, enterprises gain the confidence needed to speed up digital transformation. Micro Focus is uniquely suited to help organizations take a holistic approach to protect identities, apps, and data. Very few vendors can assure security and governance professionals that they are protected against breach, guarding the privacy of individuals and their data, and complying with regulatory and jurisdictional regulations—at scale, with ease, insight and confidence.

With Micro Focus, firms are able to scale analytics initiatives by working on encrypted data that allows analytics to be performed, but is useless to attackers. They can accelerate the adoption of cloud services and move more workloads to the cloud by having consistent data and identity security across hybrid IT and securing app development.

A Proven Track Record Protecting Data Privacy

Just as technology has introduced a crisis of confidence around personal data privacy, technology is an essential part of the solution. To avoid fines and join the 'privacy practices hall of fame,' you need a trustworthy partner whose tools adhere to industry best practices and who also has the experience and knowledge to help you keep your customers and your company safe.

With its broad set of tailored, integrated solutions, Micro Focus has a proven track record of helping best-in-class enterprises such as Lenovo, Experian, the European Space Agency, Rackspace, and more with their data governance and privacy protection needs. With powerful, on-premises and cloud solutions for every use case across our broad Security, Risk Management, and Governance portfolio, you can join major global organizations who trust Micro Focus with the governance and protection of their customers' private data.

See how at:

Micro Focus Security Risk and Governance

GDPR & Beyond Portal

Assessment: Technology Readiness for GDPR

MicroFocus Whitepaper: How GDPR can be a strategic driver for your business

Or request a free trial.

Contact us at:
www.microfocus.com

With its broad set of tailored, integrated solutions, Micro Focus has a proven track record of helping best-in-class enterprises such as Lenovo, Experian, the European Space Agency, Rackspace, and more with their data governance and privacy protection needs.