MICRO FOCUS

A Global Framework for Privacy Protection and Value Creation

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.

The Global Privacy Movement

2018 was the year when privacy became mainstream news and consumers realized the price to 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. As consumers became aware of the vulnerability of their personal information online, regulators and legislators worldwide have taken 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.

Key Functionality Requirements of a Single Framework

Any privacy protection program needs to be broad, scalable and flexible enough to meet an enterprise's varied needs, while also enabling controls that can become a source of value creation for the company. Additionally, there are key functional requirements that are 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 may be subject to. This means identifying information that may be relevant to privacy requirements in a streamlined/automated fashion assessing the current access control policies to sensitive data.

Flash Point Paper

Information Management and Governance
Security

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 understand how a company is affected by each article within privacy regulations and help 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?*

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.

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.
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 to implement data quality maintenance with deletion/suppression and effective breach response.
5. **Secure identities, applications, and data:** 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 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® delivers a flexible, modular, intelligent set of solutions that help customers identify and take action on data that might be subject to privacy regulation.