SailPoint

SOLUTION BRIEF

Meeting the Challenges of GDPR Compliance

Implementation of the EU General Data Protection Regulation (GDPR) introduces sweeping new set of requirements to ensure the privacy and protection of EU customer data.

New mandates in the GDPR include:

- Stringent rules for the protection, management and control of any EU citizenry personally identifiable information (PII)
- Significant financial penalties for data breaches involving EU citizen PII, ranging from a minimum of €20 million up to 4% of an organization's global annual revenue
- Required material changes in how and where organizations store customer data
- A mandate to report data breaches within 72 hours of discovery
- An increase in an organization's obligation as its opportunity for risk grows

Meeting these challenges requires a holistic approach focused as much on process and planning as technology. SailPoint powers GDPR compliance with identity governance, enabling enterprise organizations to confidently assess risk, strengthen controls, and automate detection and audit processes. Organizations gain full visibility into "who has access to what," and insight into how that access is leveraged. It also gives enterprises the means to not only meet GDPR compliance and other regulatory requirements, but also to realize an improved security posture across the entire enterprise that allows for security to be built into existing processes and procedures that extend both their value and effectiveness.

GDPR compliance is demanding. Enterprises should take a comprehensive approach

that includes coverage of three key challenges:

Assess: Analyze Your Risk to Prioritize Your Response

Do you know where all your sensitive data resides? Or for that matter, who has access to it? In order to govern users' access to data, organizations need a clear view across their entire infrastructure of who their users are and where their at-risk data resides. If an IT team or business owners cannot see all the permissions a user has, they simply cannot make the right decisions about who should have access to what and when. Before you can discover and remove stale and unused access permissions to systems, you need a clear view of all those who have access to sensitive information residing in both structured and unstructured formats.

GDPR compliance means enterprises must:

- Know where all personal customer data is stored
- Identify how access is granted
- Discover current access for employees, contractors, vendors and others

SailPoint enables GDPR compliance by giving organization the means to:

- Discover sensitive data across the entire enterprise, including in unstructured formats such as presentations, and in storage repositories such as files shares and Box
- Identify exposed and stale data
- Identify business data owners
- Discover and remove stale and unused access permissions to systems, reducing risk of data leakage
- Gain visibility into fine-grained permissions
- Monitor user activity for aberrant requests

Assessing risk provides a blueprint for prioritizing and addressing the most immediate organizational security needs. Before you can effectively control and secure your organization's data, you must first identify its owners. Organizations that fail to actively assign accountability to data owners and understand who should have access – and just as importantly, who actually has access – are leaving themselves open to data breaches and regulatory penalties.

Enhance: Strengthen the Controls that Determine Access

GDPR compliance means organizations need to strengthen the controls that determine who has access to specific data, and who does not have access. Removing unwanted and unneeded access to systems, applications and data is imperative. GDPR requirements mean users should have "least-privilege" access to only the minimum resources they need, and access to sensitive data should be highly restricted. The processes that enforce tighter controls and policies to prove security integrity need to be repeatable.

Meeting GDPR standards means building a governance model that aligns access to applications and data based on business need.

SailPoint helps organizations by giving them the means to grant and revoke access to sensitive data in accordance with their GDPR compliant policies, as well as the ability to regularly review and adjust access to data as needed to stay compliant. Other necessary functionality includes the ability to:

- Implement access control policies
- Align identity to data via permissions
- Utilize least-privilege process implementation
- Enforce strong authentication protocols
- Synchronize password management across multiple platforms and devices
- Issue access and recertification policies
- Perform business-driven (identity and data) lifecycle management

SailPoint empowers organizations to implement workflows to ensure appropriate business stakeholders can participate in contributing to approvals, reviews and assessments of access. Removing unwanted or unneeded access to systems, applications and data minimizes the potential for abuse of account privileges.

Automate: Access Decisions Must Now Be Made in Real Time

GDPR not only requires that organizations incorporate least privilege permissions for EU PII citizen data, but also that they be able to detect and remediate violations of that policy immediately. Organizations must also report any data breach involving customer data in fewer than 72 hours. The short timeline and complexity of these required responses means no successful attempt at GDPR compliance can be made without a reliance on automation. Automation is vital when responses need to occur in real time. Automated provisioning and de-provisioning of access is one of the only ways organizations can truly tighten security controls while also enabling business efficiencies.

SailPoint enables enterprises by providing capabilities like automated provisioning and de-provisioning of access, self-service access requests and automated certifications of access. This increased functionality for GDPR compliance includes:

- Ongoing user data access activity monitoring and alerts when out-of-bounds activity is detected
- Data owner enablement and the ability to perform real-time risk-based status checks over the data they manage
- Pre-defined reports that provide IT and compliance departments a quick and detailed view of all data access activity, permission changes and potential non-compliant activity

- Fine-grained audit trails for required forensics in the case of a data breach
- Proactive avoidance and immediate detection of violating permissions
- Automated provisioning and de-provisioning
- Activity monitoring, real-time alerting and remediation

Meeting the challenges of GDPR means mitigating out of compliance access in real time and streamlining your data protection impact assessment (DPIA). Integrating identity context into the organization's current security efforts extends their value and can be used to stop malicious behavior in its tracks. By feeding alerts and events to other security investments and infrastructure such as a security information and event management (SIEM), identity context provides greater visibility into benign versus actual malicious behavior. Identity context also provides security analysts and hunt teams the insight necessary to confront the most pressing security issues, while reducing the time wasted on eliminating false positives from consideration. Identity is how security becomes baked into processes, not brushed on. It's the base from which modern enterprises can function both efficiently and securely.

Conclusion

GDPR is a fundamentally different approach that institutes data protection from a consumer standpoint, as opposed to a business perspective. In other words, it can create enormous challenges for any organization that conducts business with the EU in any capacity. Placing identity governance at the core of your security strategy can give your organization the means to protect access to customer data and mitigate the risks you face from a data breach. Solving GDPR challenges means organizations need to develop a complete picture of where customer data resides, whether it is in a database or a spreadsheet, on a portal or in the cloud. With repositories such as files shares and Box, your organization can increase its visibility and controls around who has access to what, in addition to how that access is being utilized. Meeting the demands of GDPR requires a holistic approach that includes planning and process, as well as technology. SailPoint stands ready to provide your organization with the tools necessary to meet and solve the complex challenges GDPR compliance presents.

SB1118-1808