SailPoint

WHITE PAPER

# Addressing The Data Privacy Landscape with Identity Governance

## Securing Identity: The Foundation for Compliance

As the landscape surrounding protecting private and or confidential data continues to change – from the increasing number and complexity of regulations to the escalating costs of compliance – deploying strong, more automated identity governance takes on new urgency. Establishing a strong identity governance practice addresses a fundamental common denominator – identity and access control – across all compliance requirements, now and moving forward.

> **Protecting access to relevant data is at the core of data privacy – and strong identity governance is at the core of protecting access.**

## The Changing Data Privacy Landscape

Because of the confluence of several factors – particularly as it relates to achieving compliance with data privacy regulations – the business need for strong, more automated identity governance is growing.

The data landscape has become more complex. There is not just more enterprise data, but also shifting locations, critical application interdependencies, and growing inherent value in the data itself. There is more sensitive data than ever across applications, data repositories, and public clouds in every geography, many with their own set of data privacy regulations. Critical business applications are increasingly interdependent and require machine-to-machine access to private data. E-commerce payment transactions for example automatically pass private data entered on your website thru bank systems and third-party clearinghouses.

**IDC predicts that by 2022,**

**90%** **of all new apps will feature microservices architectures; and**

**35%** **of all production apps will be cloud-native.**

Source: IDC Directions 2019

**A fine of over €14 million was recently issued to a German company, where data policies are very strict. The company was accused of using an archive system for the storage of personal data of tenants that did not provide for the removing of personal data which in fact was no longer required, and who had access to that data.**

The increasing volume of private data coupled with its escalating value has both positive and negative business ramifications. The benefit is that businesses can leverage data to better understand and service clients, design new products, and make data-driven decisions. The downside is that cyber-criminals are targeting private data, both Personally Identifiable Information (PII) as well as valuable company data like financials, trade secrets, patents, etc. Sad testimony to the increasing value of private data is the rise in advanced malware attacks and publicly disclosed breaches.

.

Managing identity governance is challenged by the shifting nature of today's workforce, which is more mobile, more remote, and more dynamic than ever. Organizations want the flexibility of more temporary, contractor and service provider relationships. Employees continue to look for more flexibility in workstyles. They want the same simple and rapid access across different devices, and the ability to change locations and devices as required to do their jobs. The rise of shadow IT, where departments such as DevOps circumvent established access and identity governance practices in pursuit of more speed and flexibility, is a good example of the challenges presented by today's workforce.

In a 2019 survey of over 1,200 workers in the U.S. **30% work remotely full-time.**

Source: State of Remote Work 2019

As digital transformation initiatives accelerate there is far more non-human, automated access to data – which also requires identity management. Extended, distributed infrastructure-as-a-service (IaaS) and workloads running across public clouds – both for the enterprise directly but also for invoking third party services – relies on machine-to-machine access provided automatically. The emergence of robotic process automation (RPA) is another good example of the increasing need for securing automated access.

## Compliance Is an Oncoming Train

Data privacy regulations will continue to grow in number, scope, and subsequent financial risks to the enterprise. Achieving and maintaining regulatory compliance can easily get out of control – especially when there are so many data privacy laws that have been established and many more on the horizon. Protecting data by securing access to it requires a strong identity governance practice which addresses many fundamental regulatory requirements and lays a solid foundation for compliance moving forward.

**Over 80 countries have adopted comprehensive data privacy laws**

Source: Privacypolicies.com, https://www.privacypolicies.com/blog/privacy-law-by-country/

Industry or sector specific regulations have been around for some time. Some of the more noteworthy include HIPAA in the U.S., and globally, PCI DSS for protecting private credit card data. Both these regulations call for:

- Control of access and identities;
- Knowing where your sensitive data is;
- Knowing who has access;
- Managing that access with different levels of identity controls and policies;
- Tracking and recording access for required audits.

Many high-profile regulations focus on protecting consumer data and require breach disclosures. The paradigm is the E.U.'s GDPR, which came online May 25, 2018. In the U.S., there is the California Consumer Privacy Act (CCPA) of January 1, 2020. Other countries have also enacted their own data privacy and breach regulations:

- Brazil's General Data Protection Law (Lei Geral de Proteção de Dados or LGPD);
- South Africa's Protection of Personal Information (POPI);
- Philippine's' Data Privacy Act of 2012 (PDPA);
- Australia's Federal Privacy Act and Privacy Principles (APPs).

## Compliance Starts with Visibility on PII Data

Out-of-the-box policies help you find and classify Personally Identifiable Information (PII), whether in file storage or cloud – AWS, Azure, and GCP).

Identify PII data residing on-premise or in public clouds, e.g. AWS, Azure, GCP.

Identify stale PII data or data stored in inappropriate locations.

Identifying PII data that has open access or does not have a data owner so you can take steps to control access.

## HIPAA and Identity Governance

Deliver timely, appropriate access to patient records by giving healthcare providers greater visibility and control over who has access to what, when and where.

Reduce operational costs by streamlining access to systems and applications and improving data sharing between clinicians.

Enable compliant data sharing by mitigating risk of exposing sensitive information to unauthorized users.

Drive compliance through process documentation for audits.

Source: Comprehensive Identity Management for Healthcare (2018)

**77%**

**of organizations do not have full visibility on user access**

Source: SailPoint, 2019 Identity Score Report

Beyond the identity access controls stipulated in the examples above, consumer-oriented regulations also call for:

- Access by the consumer to all data collected about them;
- Ability to delete their data and opt out of the sale of their personal data;
- Provisions to move their data to another service provider;
- The right to be forgotten, and, in the case of a breach, the notification of all parties within a specified and limited period.

**SailPoint Helps Automate Protection of Data**

AI-driven recommendations to help you decide appropriate access.

Automatically detect job changes such as transfers or terminations and launch the workflow to change or remove access privileges.

Flag high-risk access requests to managers and automate low risk requests.

Complete, auditable record of who requested access to which systems and who approved or denied request.

Rapidly respond to auditor requests using historical identity data to investigate and diagnose user access.

Lessen the burden on IT by assigning the rightful data owner to manage access.

Source: Comprehensive Identity Management for Healthcare (2018)

Finally, many regulations are based directly on standards such as SP NIST 800-53 or ISO/IEC 27001. These standards are unambiguous on the priority given to protecting access and identity; both have entire sections dedicated to access control. NIST 800-53 (Rev4) for example is organized around 18 families of controls, of which access control figures prominently with 25 specific categories. These access categories include:

- Access Control Policy and Procedures (AC-1)
- Separation of Duties (AC-5)
- Least Privilege (AC-6)
- Session Termination (AC-12)
- Remote Access (AC-17)
- Access Control for Mobile Devices (AC-19)

**How SailPoint Addresses NIST 800-53 Least Privilege**

**Detect and revoke** unauthorized access rights

**Limit access** to authorized users

**Validate** user access on a regular basis

**Require** a manager or data owner to approve all access changes

Source: Are You Prepared to Comply with CCPA (2019)

**Global enterprises reported an average of $4.1 million in financial loss due to a security breach in the last year. The average cost of a single stolen record was $148.**

Source: SailPoint Market Pulse Survey 2017

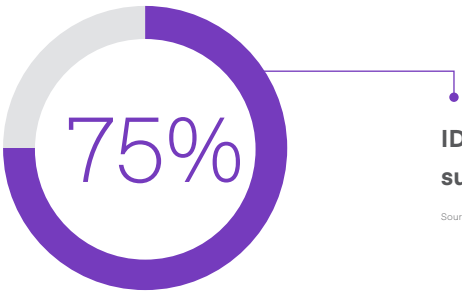
## The New Compliance Calculus

You may argue that the expense of maintaining compliance in the face of increasing regulations is not cost effective and simply accept the risk of financial penalties. The reality is business costs include damage to brand, lost customers and credibility. Regulatory financial penalties will be ongoing and only escalate (and you will still spend to address infractions each and every time). In addition, if non-compliant with one regulation you are likely exposed for others. But it's important to realize that the costliness of most existing compliance processes results from the fact they are manual and inefficient.

Identity governance can address the common core requirement protecting data privacy by ensuring access is well managed at all times. New technologies such as automation and AI/ML applied to an identity governance program can significantly mitigate operating costs – and reduce the risks of financial penalties. Using this foundational approach, you can be compliant now and be ready for the next (inevitable) new regulation.

It turns out that protecting data privacy is what customers and consumers want; it is what you need to do as a business – not just because it is prescribed by regulations.

Digital transformation which involves moving data and workloads to the cloud, deploying more automated processes, and empowering employees and clients with more flexible and productive services – requires scalable, adaptive and more automated identity governance.




**IDC estimates by 2022, 75% of IT operations will be supported by AI or analytics-driven automation.**

Source: IDC Directions 2019

## Check Out SailPoint Predictive Identity™

SailPoint enables you to build a strong identity governance practice for cost effective compliance—and more. Simplify access and accelerate your business while also building a foundation for future compliance.

- Automatically discover where sensitive data resides whether in file storage or cloud platform – AWS, Azure, and GCP.
- See who has access to what and based on policy, continually adjust access so that those who "should" have access do, and those who do not are locked out.
- Implement controls to meet regulatory compliance and automatically enforce proper access, e.g. separation of duties, least privilege, etc.
- Receive alerts when access decisions are not compliant with current policies.
- Identify where compliance gaps exist due to excess permissions and risky user access.
- Maintain a detailed audit trail to demonstrate compliance to auditors and communicate to the board.

The vectors that can compromise an organization's data protection efforts are growing and dynamic. An identity governance approach that is largely dependent on human book-keeping and manual processes is simply no longer practical – nor prudent. A more automated, identity governance solution that employs AI and ML helps do a lot of the bulk, repetitive functions of protecting access. It also more quickly surfaces areas and activity that needs attention – providing a better view of what requires human intervention or remediation.

For more information, visit us at:
**www.sailpoint.com**

**SAILPOINT: RETHINK IDENTITY**

**sailpoint.com**

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.



WP1402-2005