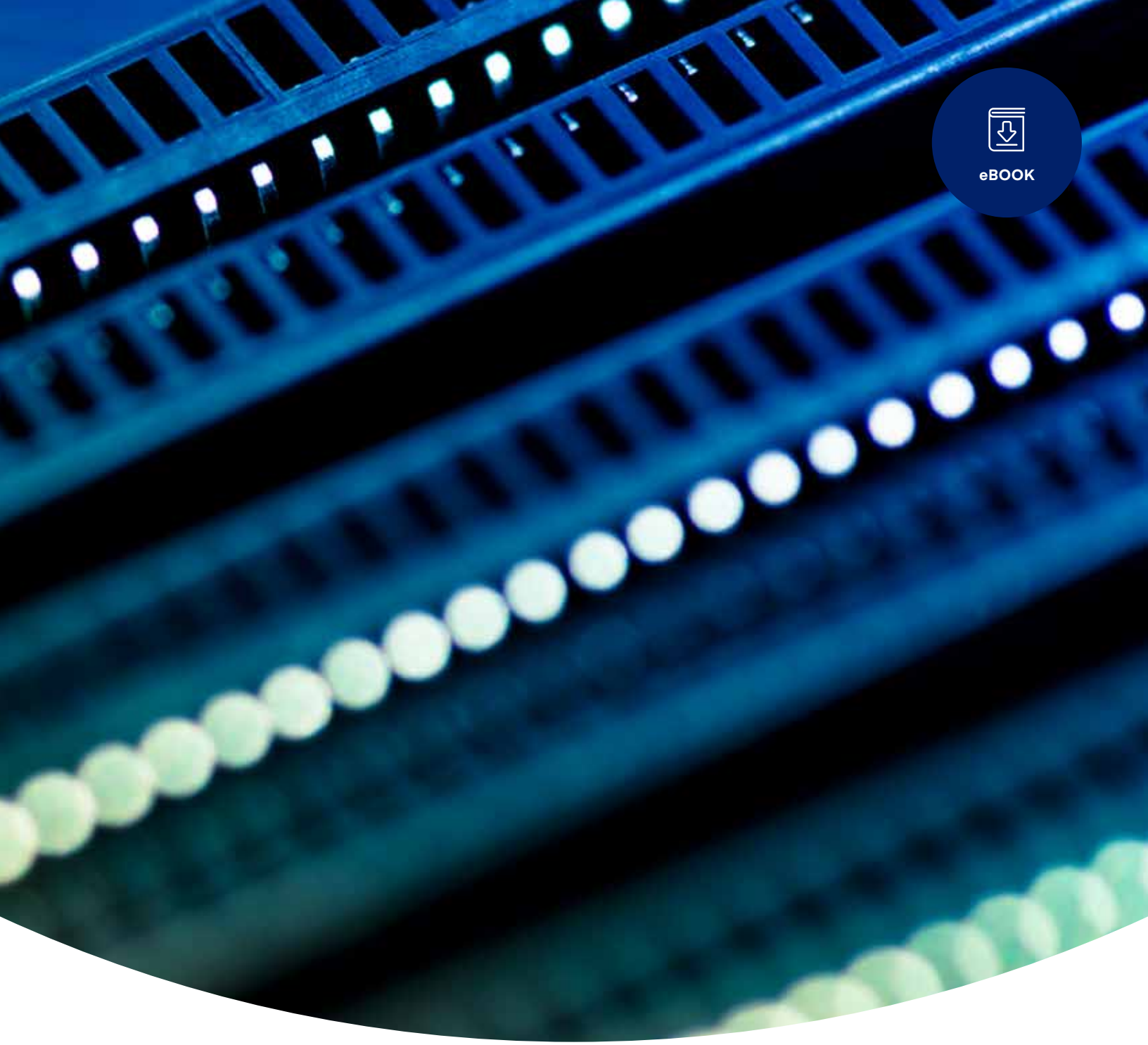

eBOOK

Get Your Organization **Compliant with GDPR**

SailPoint

Enterprises want to keep their data safe for a number of reasons: competitive advantage, customer retention and satisfaction, legal requirements and audit mandates. EU lawmakers have taken a new step in data security requirements, looking at the security of organization's data from another perspective: consumers. From this, the General Data Protection Regulation (GDPR) law was passed in the European Union to give citizens in the EU better control over when their personal information is collected and how it will be used. The EU has passed consumer data protection laws before, but GDPR – for the first time – includes significant financial penalties if companies fail to protect that collected data.

This regulation, which went into effect May 2018, impacts any organization that does business within the European Union (EU) and collects Personally Identifiable Information (PII) from EU citizens (regardless of where its headquarters may be located). The law also comes with steep consequences if you are found to be non-compliant: penalties can be up to 4% of the corporation's global annual revenue or €20 million (whichever is greater).

If your organization has been diligent on addressing existing regulations including PCI DSS, HIPAA or SOX (if in the United States), or one of the many EU country-specific data protection laws, you may already have a good foundation. Even so, you may have more to consider with the ramifications of GDPR especially considering GDPR supersedes existing regulations including the European Union Data Protection Directive. Complicating matters is that GDPR is not a one-size fits all type of regulation. In fact, it is unique as it increases an organization's obligation as the opportunity for risk grows. For example, organizations with greater than 250 employees will need to adhere to more stringent rules than those with fewer than 250 employees.

GDPR also requires material changes in how and where organizations store customer data, and more importantly how they grant access to that data to employees, contractors and business partners. Additionally, it mandates that organizations report any data breach involving customer data in fewer than 72 hours. This requires existing security models to evolve from focusing on preventing data breaches at the network layer to detecting and remediating events in real-time.

For many years, enterprises have been focused on securing the network perimeter as a means to protect their applications and data that resides within it. However, with a growing number of data breaches occurring due to compromised credentials, malicious insider behavior, and the proliferation of sensitive data being saved in unsanctioned locations, organizations are realizing the way to mitigate these risks is to implement tight governance of the identities – employees, contractors, partners, etc. – within their organization and controlling the data, applications, and systems they are allowed to access. As organizations adopt these stronger governance controls, they will find themselves better positioned to address GDPR requirements.

Get Your Identity House in Order

Organizations should focus on a few key identity governance priorities: locating sensitive data, understanding who has access to it and maintaining proper access controls on that data.

1

Identify Your Sensitive Data

First, develop a complete picture of where customer data that is required to be protected under GDPR exists within your organization. It may be in structured systems such as applications or databases, or it may reside as unstructured data (such as an Excel spreadsheet or PDF report exported from an application or database) located on file systems, collaboration portals (such as SharePoint) or even in cloud storage systems (such as Box or Google Drive).

2

Determine Who Has Access

Second, understand who should have access to customer data and reconcile it with who does. This should be an ongoing process, not a one-time event. Make sure to include all applications and file storage platforms (both those running on-premises and in the cloud) where you are actively storing customer data.

3

Create Preventive & Detective Controls

Users should have access to only the minimum resources they need ("least privilege") and access to sensitive data should be highly restricted. You need to build a governance model that aligns access to applications and data based on business need. This is where a comprehensive identity governance program can help make sure users are not able to attain improper access; then, automate review and monitoring processes for user access.

Incorporate a Holistic Identity Governance Strategy

With a comprehensive identity governance solution that spans applications and data stored in files, your organization can gain full visibility into "who has access to what" in addition to how they are using that access. This will help you make the right decisions in the event of a data breach, in addition to during access re-certifications and other security events.

At first, you may feel overwhelmed by the requirements of GDPR, especially considering the financial ramifications of non-compliance. However, leveraging identity governance at the core of your security strategy to protect access to customer data in your organization can go a long way toward mitigating the risk of a data breach and the resulting penalties that may incur.

EB1031-1902