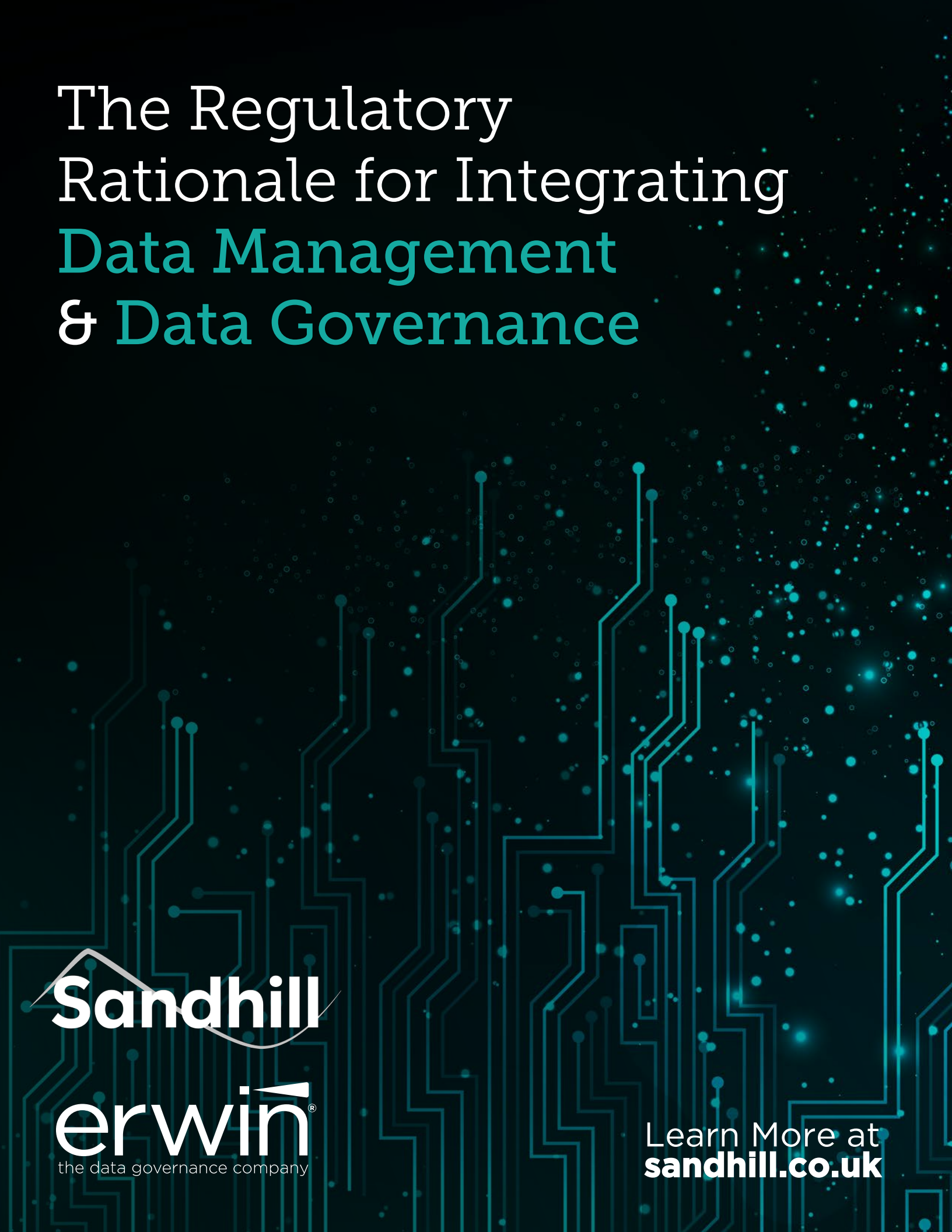
The Regulatory Rationale for Integrating Data Management & Data Governance



Sandhill

erwin®
the data governance company

Learn More at
sandhill.co.uk

Introduction

The European Union's (EU) General Data Protection Regulation (GDPR) took effect in May 2018, with no industry exempt from its reach.

Any company that does business with EU citizens must comply with GDPR or face its potential wrath in terms of fines and public opinion.

GDPR fines for violations are steep: up to 20 million euros ($23 million) or four percent of global annual turnover of the preceding fiscal year, whichever is greater. Companies like British Airways, Facebook and Google all are looking at potential fines, with Facebook facing up to a $1.6 billion penalty as a result of its data breach that allowed hackers to access the information of nearly 50 million users, three million of whom are based in Europe.

While the GDPR is an EU law, it may in fact become the de facto global privacy standard. Companies worldwide can still be affected by the GDPR if they have EU customers or audiences. And in a striking change of position, executives from the world's biggest technology companies asked a United States Senate committee to impose a national privacy law.

However, GDPR isn't the only regulation organizations need to comply with. From the Health Insurance Portability and Accountability Act (HIPAA) in healthcare to the Basel Committee on Banking Supervision (BCBS) in financial services to the California Consumer Privacy Act (CCPA) taking effect January 1, 2020, regulatory compliance is part of running — and staying in business.

Knowing what data you have and where it's stored is the first step in establishing and sustaining a solid compliance program. Additionally, it's important to understand where data comes from (data lineage) and how it has been integrated and/or transformed within your systems. So how do you ensure your organization is ready for whatever regulations come your way?

The GDPR Golden Rule

GDPR has been proclaimed as the most comprehensive data privacy law in the world, essentially making it the standard golden rule of privacy regulations.

The demands it places on organizations are all-encompassing. Protecting what traditionally has been considered personally identifiable information (PII) — people's names, addresses, government identification numbers and so forth — that a business collects and hosts is just the beginning of GDPR mandates.

First, personal data now means anything collected or stored that can be linked to an individual (right down to IP addresses), and the term doesn't only apply to individual pieces of information but also to how they may be combined in revealing relationships. And second, it isn't just about protecting the data your business gathers, processes and stores but also any data it may leverage from third-party sources.

OTHER HIGHLIGHTS:

- Companies must obtain active consent to their data from individuals; be transparent about how they process it and what they do with it; implement data security measures beyond encryption, such as pseudonymization and frequent testing; and adhere to stricter data breach notification protocols, including directly informing customers of major incidents within 72 hours of discovery.
- Individuals have the right to access, correct, remove and restrict processing of their data, as well as to have it transferred across service providers.
- Companies' new systems must adhere to the principle that specifies "privacy and security by design."
- Companies must be able to document and demonstrate their processes and mechanisms to achieve compliance.

The GDPR Golden Rule

continued

These requirements mean that businesses must expand their data governance expertise, understanding all the systems in which personal data is located and all the interactions that touch it. Knowing not only the original instance of the data but its entire lineage and how it is handled across the complete ecosystem is critical to ensure security is applied at all appropriate levels and to quickly detect any points where an individual's data may have been compromised in the event of a breach. Businesses also must ensure that changes, purges or other customer requests are adhered to in a timely manner. And without mechanisms to apply the right data governance when new systems intersect with PII, companies will totally miss the boat on the GDPR "by design" requirements.

Clearly, the level of proactive maneuvers and ongoing attention to systems and data, in an age when customer information proliferates throughout organizations at a rapid pace, requires data governance to become operational — not just informational.

Data landscape policy, procedures and metrics must flow from a central source of truth, interwoven and activated as a day-to-day part of enterprise operations and seamlessly supporting internal and external GDPR compliance audits. As critical as having a data governance platform to support all this is ensuring that roles are appropriately allocated to governance efforts.

In addition to a data protection officer to take ownership of data management — a function mandated by the regulation for public authorities and some private organizations — entities should put the right tools in the hands of data stewards, administrators, enterprise architects, business process analysts and even information consumers to maximize the quality of the solution. Then each person involved, operating under proper authorization, should have the opportunity to leverage these tools in a collaborative fashion.

Alphabet Soup: GDPR + HIPAA, PCI, BCBS

Entities like financial services institutions (particularly the larger ones) and healthcare organizations have had to grapple with strong data privacy mandates for years.

The prescriptive principles behind the PCI DSS standard followed by financial services organizations that issue credit cards could be expanded beyond the protection of payment card data to the wider range of data encompassed by the GDPR, for example. And in healthcare, HIPAA compliance has seen organizations become adept at categorizing and encrypting information and controlling data sharing, so they may be able to progress directly to implementing additional GDPR privacy mechanics — moving beyond treating people's data appropriately to supporting individuals' rights to know what personal data is held about them, to have it erased or ported over to other providers, and so on.

Other industries are in various states of preparedness. Take retail as an example. Retailers with e-commerce operations and/or physical global footprints clearly have exposure to GDPR risks. But their digital channel backgrounds and/or worldwide market experience likely make them more sensitive to different countries' consumer privacy requirements and cross-border PII data curation from the start, and so better poised to adapt to GDPR demands. However, traditional brick-and-mortar businesses with operations largely outside of Europe probably have less knowledge of their potential liability.

Boutique shops, hotels and restaurants that accept EU travelers' debit or credit card payments, enroll them in loyalty programs, or ship items to their home addresses have equal responsibilities under GDPR as their larger or online peers, but without a firm grasp on the standard's mandates likely are further behind in achieving compliance. They may not have gotten very aggressive about data categorization as a starting point, for example — if they've even thought about the need to do so at all.

Alphabet Soup: GDPR + HIPAA, PCI, BCBS

continued

Additionally, any retailer that gets PII data from third parties, such as payment processors and search engines, are subject to the regulation as well.

In the info-tech sector, U.S. telecom and communications companies may not have any EU customers of their own and so consider themselves in the clear. In those cases, they will be caught off guard to learn that they too must comply with GDPR regulations if their U.S. business customers use their products or services to collect, use or store personal data regarding their own EU customers or potential clients. In contrast, leading cloud providers like Amazon, Google and Microsoft are touting their services' commitment to GDPR compliance, as well as have plans to offer customers other GDPR protection and tracking solutions.

Whatever position a whole industry, or any companies within a sector, now finds itself in regarding compliance, the truth is that every business will be pulled into the GDPR or other regulatory sphere to some degree sooner or later — no matter from where its customers hail, with whom those clients do business, or for whom they process data. The signs are clear that even if GDPR does not become an official worldwide data privacy standard, it will become a de facto one, providing a strong set of guidelines for other governmental regulations to align with in some way.

The Compliance Common Denominator: Discovering & Protecting Sensitive Data

The common denominator in compliance across all industry sectors is protecting sensitive data.

But if organizations are struggling to understand what data they have and where it's located, how do they protect it? Where do they begin?

Data is a critical asset used to operate, manage and grow a business. While sometimes at rest in databases, data lakes and data warehouses; a large percentage is federated and integrated across the enterprise, introducing governance, manageability and risk issues that must be addressed.

Knowing where sensitive data is located and properly governing it with policy rules, impact analysis and lineage views is critical for risk management, data audits and regulatory compliance. However, when key data isn't discovered, harvested, cataloged, defined and standardized as part of integration processes, audits may be flawed and therefore put your organization at risk.

Sensitive data — at rest or in motion — that exists in various forms across multiple systems must be automatically tagged, its lineage automatically documented, and its flows depicted so that it is easily found and its usage across workflows easily traced.

Thankfully, tools are available to help automate the scanning, detection and tagging of sensitive data by:

MONITORING AND CONTROLLING SENSITIVE DATA

Better visibility and control across the enterprise to identify data security threats and reduce associated risks

ENRICHING BUSINESS DATA ELEMENTS FOR SENSITIVE DATA DISCOVERY

Comprehensive mechanism to define business data elements for PII, PHI and PCI across database systems, cloud and Big Data stores to easily identify sensitive data based on a set of algorithms and data patterns

PROVIDING METADATA AND VALUE-BASED ANALYSIS

Discovery and classification of sensitive data based on metadata and data value patterns and algorithms. Organizations can define business data elements and rules to identify and locate sensitive data including PII, PHI, PCI and other sensitive information.

Truly Understanding Your Data

Data management and data governance, together, play a vital role in compliance. Data is easier to protect when you know what it is, where it's stored, and how it needs to be governed.

Truly understanding an organization's data, including the data's value and quality, requires a harmonized approach embedded in business processes and enterprise architecture. Such an integrated enterprise data governance experience helps organizations understand what data they have, where it is, where it came from, its value, its quality and how it's used and accessed by people and applications.

But how is all this possible? Again, it comes back to the right technology for IT and business collaboration that will enable you to:

- **Discover data:** Identify and interrogate metadata from various data management silos
- **Harvest data:** Automate the collection of metadata from various data management silos and consolidate it into a single source
- **Structure data:** Connect physical metadata to specific business terms and definitions and reusable design standards
- **Analyze data:** Understand how data relates to the business and what attributes it has
- **Map data flows:** Identify where to integrate data and track how it moves and transforms
- **Govern data:** Develop a governance model to manage standards and policies and set best practices
- **Socialize data:** Enable all stakeholders to see data in one place in their own context

The erwin EDGE: Your Compliance Solution

The need to comply with regulatory mandates, such as GDPR, is a top driver for data governance initiatives, according to 60 percent of the respondents to an erwin-UBM survey.

Less than one-third of organizations have a fully implemented data governance program, however, with the effort being a work in progress at just over 40 percent of survey-takers.

Moving these initiatives forward in as comprehensive and holistic a manner as possible makes sense not only for achieving regulatory compliance but also for making an organization's employees smarter with data. Data governance is the engine behind raising the bar on customer satisfaction and better decision-making too.

With the **erwin EDGE Platform,** businesses are empowered to understand their data topography and make the most of their information assets while adhering to critical regulations. Its Any[2] approach accounts for any data (relational and unstructured) from anywhere (on premise or in the cloud), making it possible to identify and categorize PII data throughout the organization in a granular way. It gives teams — compliance owners, data stewards, business analysts, enterprise architects and others — the role-based tools and the central source of truth they need to create and convey the processes for operationalizing regulatory requirements as part of normal procedures. That includes providing a proactive way to ensure that new databases storing PII data also are deployed with GDPR rules taken into account via GDPR integration templates.

The **erwin EDGE** is centered around a data governance hub that serves as the foundation for an organization's GDPR compliance effort. The technology platform goes beyond the traditional data asset management role of data governance to transform the way all stakeholders in a business discover, understand, govern and socialize data. It provides an integrated business glossary, data dictionary, data catalog, lineage mapping and policy authoring for data elements, providing all invested parties with a role-based view of data and the ability to collaborate on defining GDPR and non-GDPR data and determining any necessary remediations. Critically, this demystification and operationalization of the data landscape, supporting visibility across domains, takes place as part of standard business activities, with a view to minimizing exceptions and unexpected negative data change impacts.

The erwin EDGE: Your Compliance Solution

continued

The following components build on the data governance core for value-added capabilities based on an organization's current GDPR progress and plans:

erwin Data Modeler:

Move beyond detecting individual PII components to understand and document data elements and how, brought together in various combinations, they could reveal sensitive personal information and create unexpected GDPR risks. Data may be categorized as GDPR or non-GDPR using standard templates before new systems are deployed to assure indicators for taking action on PII components (such as forgetting or correcting them) are associated with existing data entities that will be brought into those databases.

erwin Business Process:

Marry GDPR data with the processes that use it, understanding workflow to provide clear visibility into safe and unsafe regulatory practices — as well as rectify the latter. They can apply great specificity to defining new GDPR processes for purging, porting, reporting and otherwise managing GDPR data, analyzing and codifying them into the business, making staff aware of them, and even presenting them to auditors as evidence, for example, of privacy and security by design.

erwin Enterprise Architecture:

Document the situation as it exists and as it will exist, analyzing GDPR priorities and risks that may include moving additional data to the cloud, for instance. Within a dynamic roadmap, you can view how systems fit together with an overarching picture of data as it moves across them, exploring opportunities to assure, input and demonstrate GDPR compliance.

The erwin EDGE: Your Compliance Solution

continued

erwin Data Catalog:

Have data visibility, lineage and governance throughout the data integration lifecycle. You can automate enterprise data mapping and code generation for faster time-to-value and greater accuracy when it comes to data movement projects, as well as synchronize "data in motion" with your data management and governance efforts. Map data elements to their sources within a single repository to determine data lineage, deploy data warehouses and other Big Data solutions, and harmonize data integration across platforms.

The solution reduces the need for specialized, technical resources with knowledge of ETL and database procedural code, while making it easy for business analysts, data architects, ETL developers, testers and project managers to collaborate for faster decision-making.

The **erwin EDGE** also includes automated harvesting and transformation of operational data from multiple enterprise systems for delivery to the erwin Data Catalog (DC). The ability to integrate this type of information into the data dictionary eliminates data silos, reduces discovery time, and mitigates data-related risks.

Regardless of industry, businesses that take advantage of these capabilities will be well prepared for understanding the data assets they have, aligning them to regulatory requirements, and ensuring they remain in sync as changes take place throughout their enterprises. Even those organizations that have not made significant compliance progress to date will find themselves empowered to more quickly achieve that goal — while also gaining greater data agility to improve their overall business operations.

See how the erwin EDGE can support your organization's efforts to expand its data management and data governance expertise.

Start by requesting a demo of erwin DC

erwin®
the data governance company

Sandhill

About erwin, Inc.

As the data governance company, erwin provides enterprise modeling, data cataloging and data literacy software to help customers discover, understand, govern and socialize their data to mitigate risks and realize results. The erwin EDGE platform facilitates IT and business collaboration in driving actionable insights, agile innovation, risk management and business transformation. We help government agencies, financial institutions, healthcare companies and other enterprises around the world unlock their potential by maximizing the security, quality and value of their data assets.

Connect with us at
sandhill.co.uk