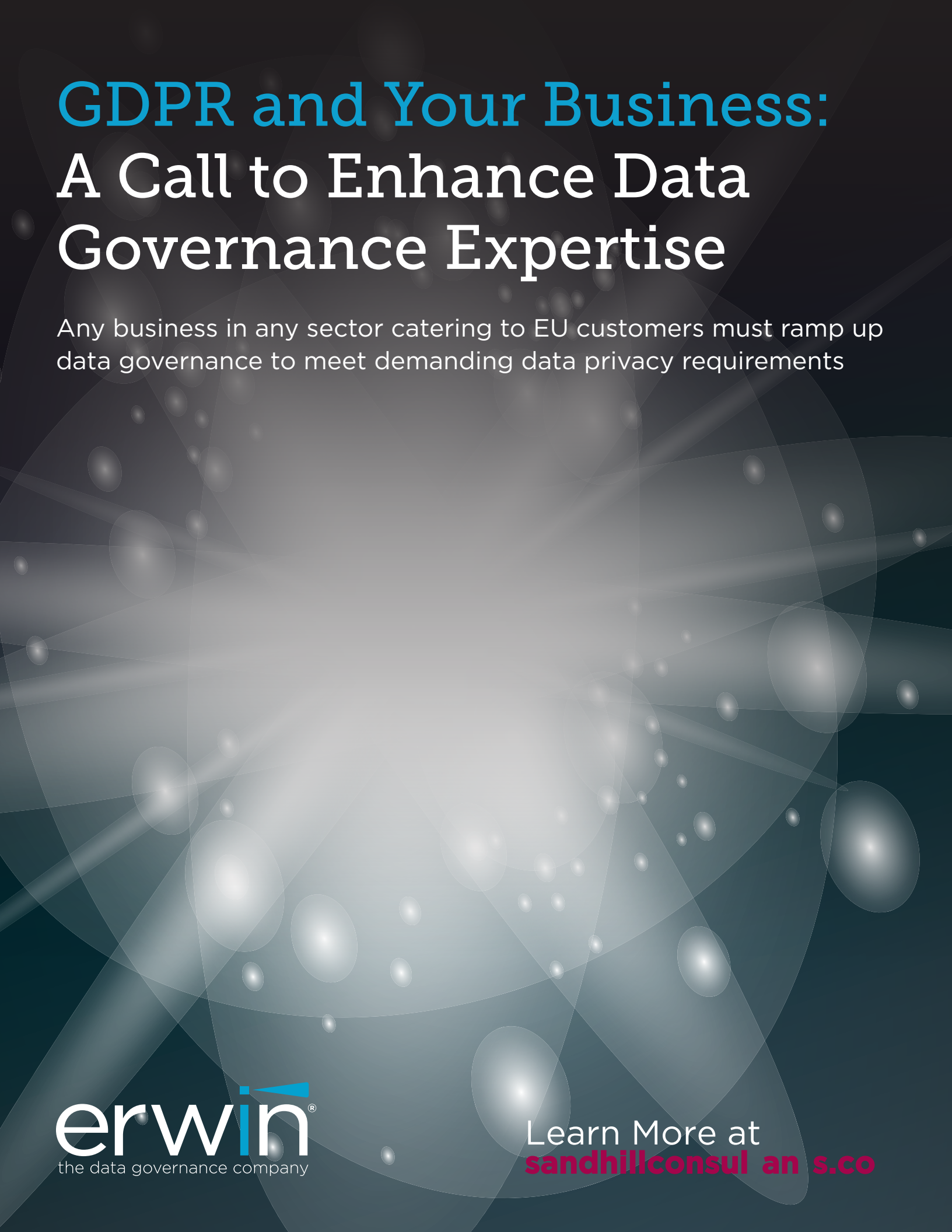
GDPR and Your Business:
A Call to Enhance Data Governance Expertise

Any business in any sector catering to EU customers must ramp up data governance to meet demanding data privacy requirements



erwin®
the data governance company

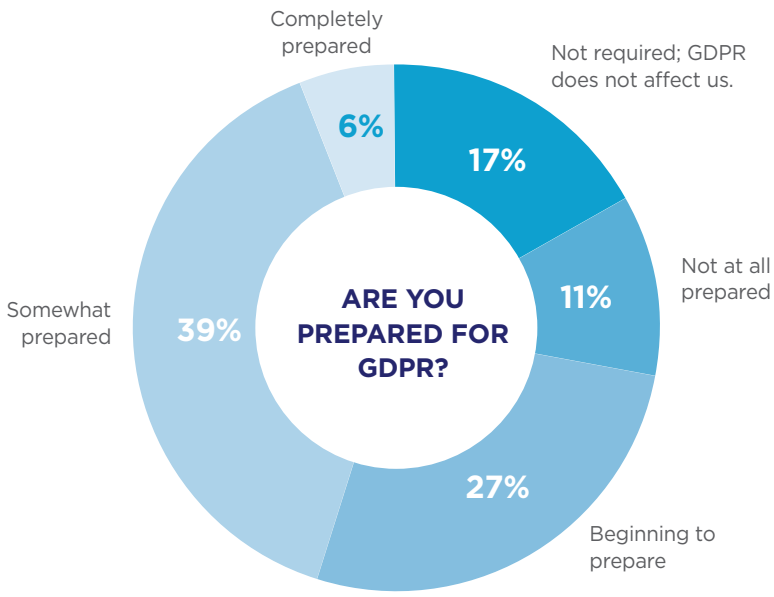
Learn More at
sandhillconsul an s.co

The European Union's Global Data Protection Regulation (GDPR) has a broad wingspan.

No industry is exempt from its reach.

The mandate's requirements apply to any business in any vertical sector—regardless of where the company is based—that counts even one EU citizen among those it services. The Chicago online retailer making a splash with the French couture crowd and the hospital in New York caring for the German ex-pat are as subject to GDPR regulations as the West Coast internet and cloud services giant and the U.S.-headquartered bank with operations across mainland Europe.

Although the effective date for GDPR compliance—May 25, 2018—is fast approaching, many organizations remain unprepared for the standard. That's particularly apparent among those that don't call the European continent home. Just six percent of North American enterprises say they're ready for the upcoming regulation, according to the 2018 State of Data Governance research conducted by erwin and UBM.



Data: *UBM survey of 118 business technology professionals at organizations with 1,000 or more employees, November 2017*

That's cause for concern, though fortunately tempered by the fact that not every company—whether a data controller or processor—will be immediately in GDPR auditors' sites. Additionally, some industries will be able to draw on the experience they've built in implementing tools and processes for other data privacy initiatives to help push their GDPR efforts forward faster. In healthcare, for instance, experts have noted that the similarities that exist between the Health Insurance Portability and Accountability Act's (HIPAA) explanation of protected health information and GDPR's definition of data concerning health could speed data discovery and mapping for the EU regulation.

GDPR's Rigorous Requirements

Still, GDPR has been proclaimed as the most comprehensive data privacy law in the world, and the demands it makes on organizations are suitably 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 expectations. For one thing, 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 apply only to individual pieces of information but also to how they may combine in revealing relationships. For another, this is no longer just about protecting the data your business gathers, processes and stores itself 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.

Such 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 that 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. It also matters to businesses being able to ensure that changes, purges or other customer requests are adhered to in a timely manner. And, unless mechanisms are put in place so that any new systems intersecting with PII are deployed with the right data governance in place, 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.

GDPR becomes effective in an age of rapidly proliferating customer data. For organizations to meet the demands, **data governance** must become operational.

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 it will be to have in place the 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.

Each person involved, operating under proper authorization, should have the opportunity to leverage these tools in a collaborative fashion. With all these parties working together in an effective manner, even if compliance is not fully enabled by day one of the regulation's enforcement, it at least should be possible to compile and supply roadmaps of plans to achieve adherence to the standard to auditors upon request, potentially avoiding immediate fines.

GDPR's Vertical Industry Impact

As GDPR gets into full swing, however, regulators likely won't be averse to making an example of a few non-compliant actors.

For their purposes, imposing penalties on a brand-name company in a big-ticket vertical certainly would get the word out that every organization needs to take the regulation seriously. From that perspective, a financial institution presents as a good target.

Indeed, research carried out by **VansonBourne** shows that 92% of respondents believe that particular industries are more likely to be made an example of if an organization from that sector breaches the EU's GDPR. Slightly more than one-quarter believe that this is most likely to happen to the banking industry.

Which industry do you believe is most likely to be made an example of if an organization from that industry breaches the EU GDPR?

Base: all respondents	Total
Banking	**26%**
IT, technology and telecoms	20%
Financial services (excluding banking and insurance)	8%
Business and professional services	5%
Government	5%
Manufacturing and production	4%
Consumer services	4%
Retail, distribution and transport	3%
Insurance	3%
Media, leisure and entertainment	3%
Public healthcare	3%
Energy, oil/gas and utilities	2%
Construction and property	2%

Base: all respondents	Total
Legal	1%
Public education	1%
Other public sector (please specify)	0%
Other commercial sector (please specify)	0%
I do not think that any industry in particular is more likely to be made an example of should one of their organization's breach GDPR	**8%**
BASE	**500**

Data: *VansonBourne survey of 500 EU IT and risk professionals on GDPR one year from the start date, May 2017*

On the other hand, more regulated entities like financial services institutions (particularly the larger ones) and healthcare organizations have had to grapple with strong data privacy mandates before and may be ahead of the game in some respects. Experts have pointed out that the prescriptive principles behind the PCI DSS standard that is 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.

So many 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 may have made 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. Additionally, any retailer that gets PII data from third parties, such as payment processors and search engines, is subject to the regulation as well.

Different sectors—and even individual companies within them—are all at **different levels of preparedness** when it comes to meeting **GDPR requirements.**

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 be compliant 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 by enforcement date, 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 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.

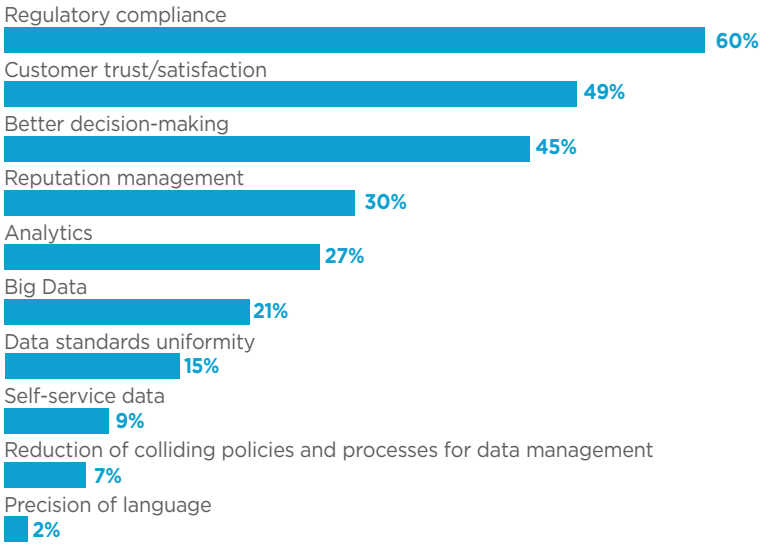
Whether or not **GDPR** becomes an official worldwide standard, it will be a de facto one. **Every business must prepare to support its requirements.**

erwin EDGE: Your GDPR Solution

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

Moving these initiatives forward in as comprehensive and holistic a manner as possible makes sense not only for achieving GDPR 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.

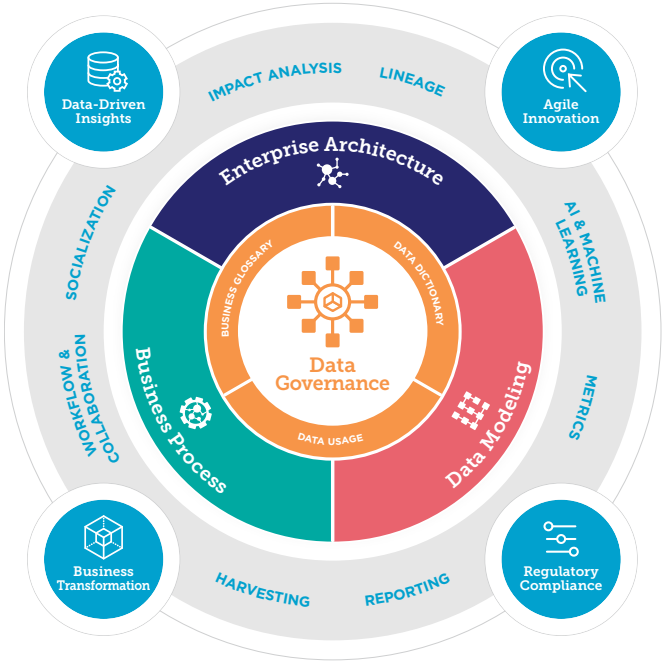
WHAT'S DRIVING YOUR DATA GOVERNANCE INITIATIVE?



Note: *Maximum of three responses allowed.*

Data: *UBM survey of 118 business technology professionals at organizations with 1,000 or more employees, November 2017*

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), 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—GDPR 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 GDPR 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 a persona-based approach and technology platform for creating an* **enterprise data governance experience** *that joins both IT and business functions to ensure organizational objectives around managing risks and maximizing opportunities are met.*

erwin Data Governance serves as the foundation of an organization's GDPR effort. But **erwin DG** 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 following components build on the erwin DG core for value-added capabilities based on an organization's current GDPR progress and plans:

erwin Data Modeler

With this solution, businesses can 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, and integrators applied to assure that 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

With this solution, businesses can 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

With this solution, businesses can document their situation as it exists and as it will exist, analyzing GDPR priorities and risks as they plan futures that may include moving additional data to the cloud, for instance. Within a dynamic roadmap they 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** platform also includes automated harvesting and transformation of operational data from multiple enterprise systems for delivery to **erwin DG**, so the information can be integrated into the company's data dictionary. Data silos are effectively eliminated, reducing GDPR discovery and other 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 GDPR requirements, and ensuring they remain in sync as changes take place throughout their enterprises. Even those organizations that have not made significant GDPR 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.

To learn more about how the **erwin EDGE** can support your business and expand its data governance expertise, **take erwin DG for a free spin** www.sandhillconsultants.com