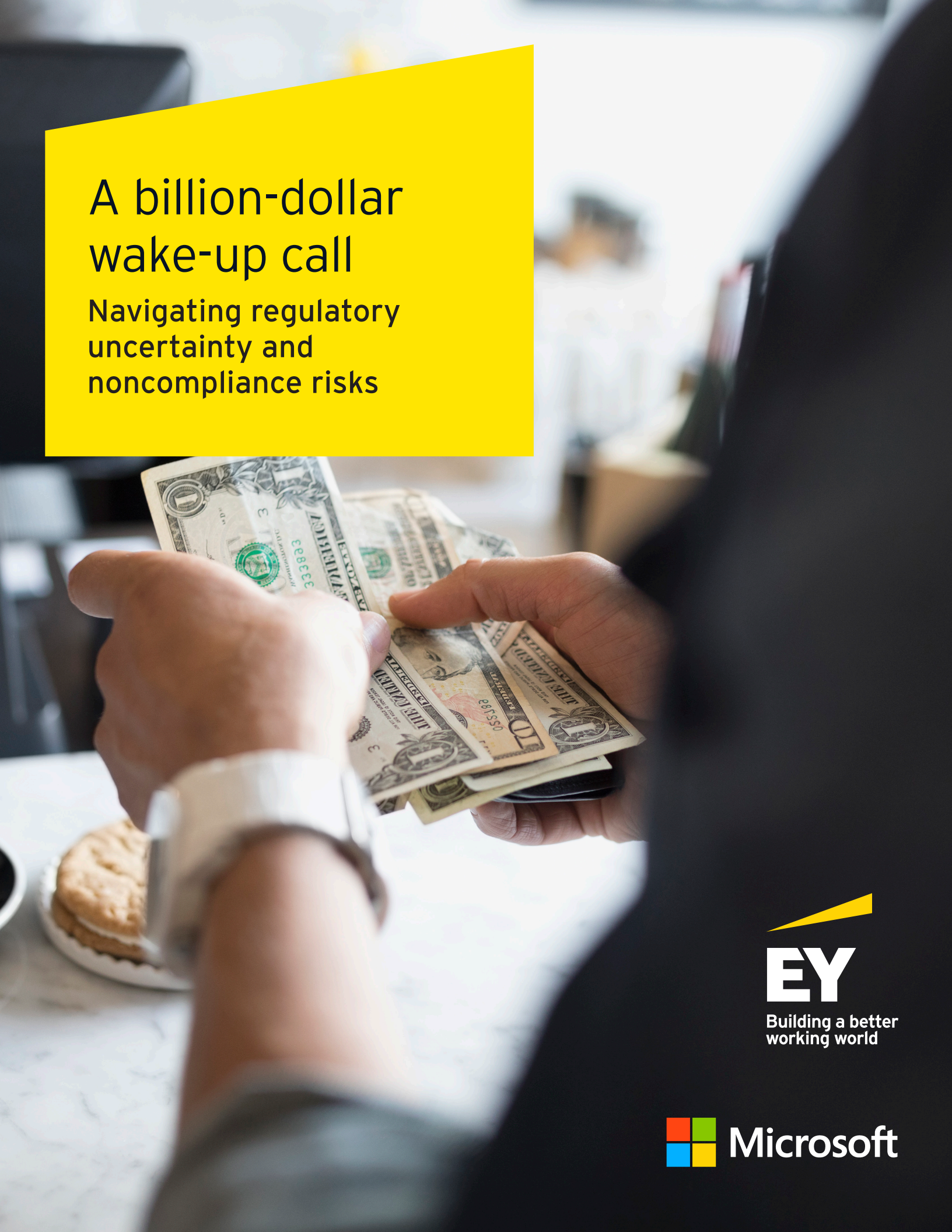
A billion-dollar wake-up call

Navigating regulatory uncertainty and noncompliance risks



EY
Building a better working world

Microsoft

In brief

- Complying with data access and protection regulations has become an important element of the enterprise risk profile.
- Managing the risk of regulatory noncompliance takes an operational mindset, sustainable processes and an integrated platform.
- An integrated cybersecurity platform, such as the Microsoft suite of integrated cybersecurity tools, can be useful in simplifying and strengthening cyber defense while easing the burden of regulatory compliance.

In May 2023, the EU fined Meta a record US$1.3 billion, after ruling that the company broke its General Data Protection[1] Regulation (GDPR) rules by transferring user data from Europe to the US. In response, the Irish Data Protection Commission ordered Meta to suspend all transfers of personal data belonging to users in the EU and the European Economic Area to the US. The fine surpasses the previous US$877 million GDPR ruling against Amazon in 2021.

And while *The New York Times* reported on July 10[2] about "a deal to ensure that data from Meta, Google and scores of other companies can continue flowing between the United States and the European Union," government officials throughout Europe have threatened to derail the agreement[3]. Some European privacy observers say the Data Privacy Framework is "nowhere near as impervious to legal challenges as some of the accord's promoters have suggested."[4]

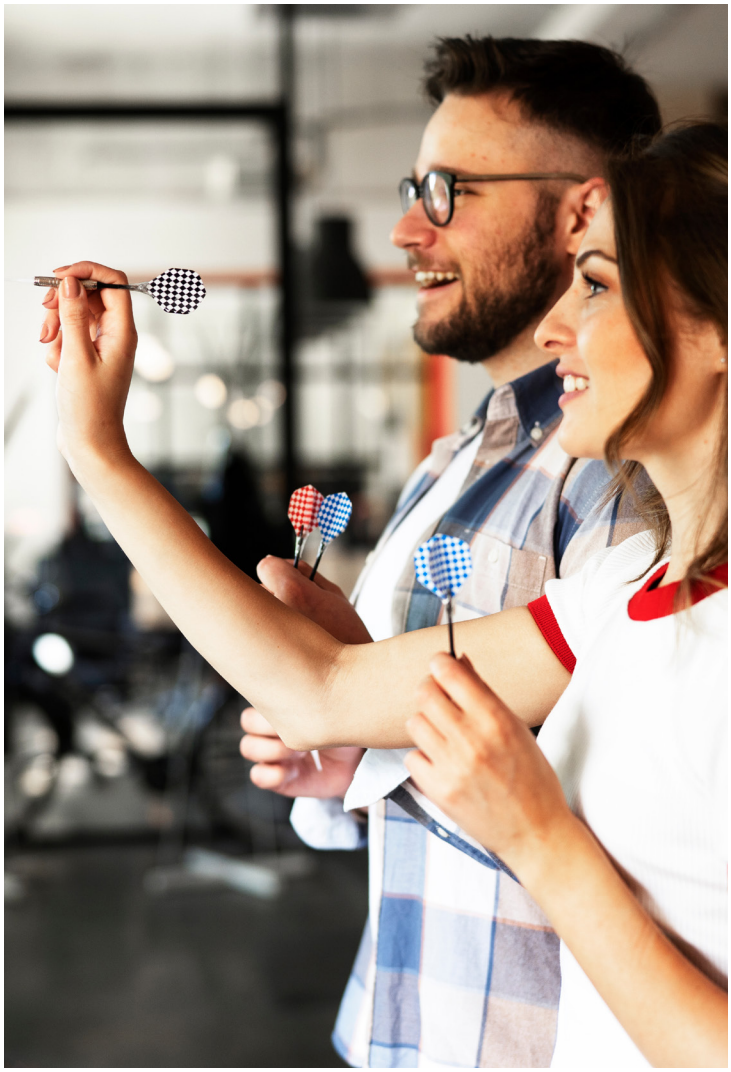
The challenge of regulatory uncertainty: a call to simplify data

This uncertainty underscores both the material impact of noncompliance with data access and protection regulations and the challenge of operating in an environment of regulatory uncertainty. From a management perspective, this should be a call to action to simplify data access and protection, using a modern data protection platform to make the problem smaller and the associated risks more manageable.

The complex landscape of regulatory compliance today is rife with manual processes for responding to data loss incidents, collecting data location information and addressing data subject access requests. EY professionals are working with clients to use innovative technology like artificial intelligence (AI) to simplify their compliance obligations. These complex regulations are tedious to navigate while ensuring proper usage, storage and data-sharing across borders.

Simplifying compliance with innovative technology

Changing regulations drive organizations to make interim changes to their access management, data protection and privacy strategies – a practice that is not sustainable in the long term. Instead of relying on a patchwork of data protection controls (e.g., encryption, tokenization, masking), leading companies are orchestrating enforceable policies, supported by an integrated security platform and implemented with an operational mindset.



Meta fined record $1.3billion and ordered to stop sending European user data to US," Associated Press, https://apnews.com/article/meta-facebook-data-privacy-fine-europe-9aa912200226c3d53aa293dca8968f84, 22 May 2023.

"U.S. and E.U. Complete Long-Awaited Deal on Sharing Data," The New York Times, https://www.nytimes.com/2023/07/10/technology/us-eu-data-privacy-deal.html?searchResultPosition=4, 10 July 2023.

"New EU-US data transfer deal also faces criticism in Germany," Euractiv, https://www.euractiv.com/section/data-protection/news/new-eu-us-data-transfer-deal-also-faces-criticism-in-germany/, 14 September 2023.

"EU-US Data Privacy Framework to face serious legal challenges, experts say," Computerworld, https://www.computerworld.com/article/3702550/eu-us-data-privacy-framework-to-face-serious-legal-challenges-experts-say.html, 12 July 2023.

Navigating changing regulations: the need for sustainability

A new EY white paper, "Proactively adapting to cross-border regulatory needs," provides insights into sustainable compliance and its impacts on organizations, such as how to efficiently comply with multiple data privacy requirements, which is at the heart of the Meta-GDPR dispute:

Data localization regulations are strict and require organizations to use, store or process data in the country of its origin. Countries like Australia, the United Kingdom and China, as well as regions like Europe, have local regulations to not only store and process personal data within borders but also to restrict access to people outside of those individual regions. To apply access restrictions, organizations first identify which country the data is from and who outside of that country has access to the data. In such cases, identification and collection of data location becomes challenging due to manual data gathering processes and incomplete understanding of data.

Organizations can utilize orchestration and innovative ways to view data from multiple countries without changing the location of data storage where it is administered. An orchestration layer can lead to coexistence of conditional access to the legacy and new systems to get the data, where the conditions can be based on policies. Utilization of orchestration will allow IT to adapt to changing business needs without disrupting business itself. It also allows for the central automation of tasks and monitoring over different applications and repositories.

Enabling sustainable, secure data protection and access requires clear cybersecurity policies with concise natural language statements that explain the what, where and why to the business, the board and regulators. For example, identity and access management (IAM) policies should provide a granular view of who has access to what information and a framework for reliably managing that access.

Crafting clear and concise cybersecurity policies: balancing rigidity and adaptability

Businesses need to understand that policies about data breaches, acceptable data use and vendor access are more than mere guidelines or suggestions. There should be a certain flexibility to respond to changing business conditions. A well-structured policy framework should be designed to accommodate differences among regions and regulatory bodies. What works for the GDPR may not satisfy the Cyberspace Administration of China or the US Securities and Exchange Commission (SEC).

An integrated cybersecurity platform should simplify and strengthen cyber defense and resilience and ease regulatory compliance. For example, Microsoft's suite of integrated cybersecurity tools includes Compliance Manager, which features end-to-end capabilities such as onboarding, workflow management, control implementation and evidence cataloging that are fundamental to satisfying regulatory requirements. The tool also offers ready-to-use, customizable and multi-cloud regulatory assessment templates to document compliance.

When protecting personal data is paramount

A multinational technology corporation, operating across multiple data storage platforms, could not afford unauthorized access to sensitive personal user data. The risk of regulatory noncompliance and damage to the company's reputation were too great.

The challenge: stop unauthorized data access and comply with demanding regulations without disrupting operations. By collaborating with EY teams, the client ultimately prevented millions in unauthorized access. Elements of the project included a broad strategy, advanced tooling, data connection analysis, rigorous access permission evaluation and meticulous data categorization.

The company now boasts a robust framework for continual data oversight and categorization, achieving procedural fidelity through regular compliance audits. We helped maintain authorized access and formulated a strategy for proficiently managing access disputes. By fusing technological prowess, simplified processes, and stringent compliance enforcement, EY teams helped the client capture the value of lasting data security and regulatory alignment.

Bridging compliance and business needs

In our experience, adopting an operational mindset, establishing sustainable processes and leveraging an integrated platform are the keys to simplifying regulatory compliance while adding value to the business.

This involves approaching compliance policies as an opportunity to spend smarter, reallocating scarce cybersecurity resources and reducing the complexity and cost of IT operations. More broadly, an operational mindset means solving business-led issues. Successful cybersecurity transformations only occur when the entire organization is actively engaged in the journey and recognizes the benefits.

Conclusion

Data protection is a strategic investment. It may not be possible to predict which regulators will wield their authority next, but the companies that prioritize intelligent investments and spend smarter, not more, on data protection will be best positioned to navigate the evolving landscape of regulatory demands and challenges posed by cybersecurity threats.

Contact

Discover how the EY-Microsoft Alliance simplifies cybersecurity to help your organization transform for trust, compliance and resilience.

Nicole Koopman
Managing Director
Technology Consulting
EY Cyber Alliance Ecosystem Leader
nicole.koopman@ey.com

Authors

Sam Tang
Principal
EY Americas Digital Identity Leader

Varun Sharma
Principal
Technology Consulting
EY Americas Cyber Solutions Leader

EYG no. 010679-23Gbl
2309-4339149
ED None