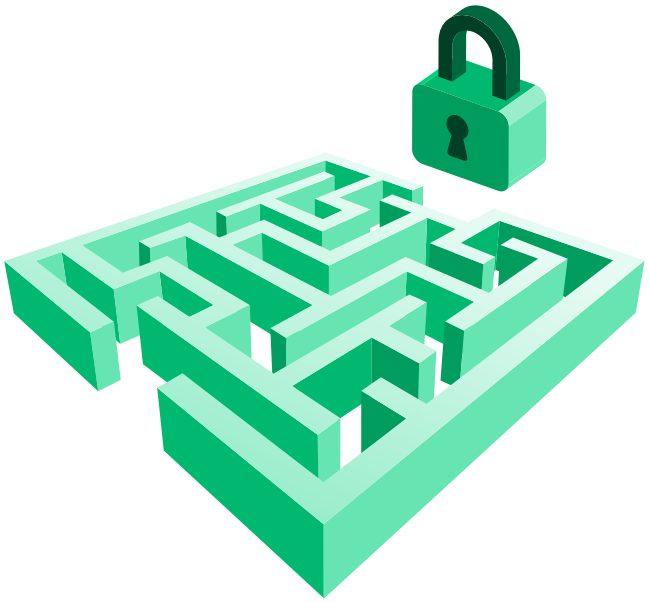
The compliance labyrinth: Navigating global cybersecurity regulations

Cybersecurity regulations are evolving rapidly to address the growing threat of cybercrime, yet the global regulatory landscape remains fragmented and complex. This was a key focus of discussion during a recent Keepit webinar, where Kim Larsen, CISO at Keepit, and a panel of industry experts explored the challenges and opportunities presented by global cybersecurity regulations.

The panel highlighted how regulations differ between the U.S. and European markets, as well as the added complexity brought by industry-specific requirements. Importantly, the experts underscored the need for clearer regulatory goals and alignment with widely adopted frameworks such as NIST and ISO. By doing so, regulators can help organizations better allocate resources, streamline compliance efforts, and ultimately, improve their security posture in this rapidly changing environment.



Overview of cybersecurity standards and frameworks

Topic	US Approach	European Approach
Frameworks and standards	Emphasis on frameworks like NIST, with sector-specific compliance regulations such as HIPAA and PCI.	Focus on ISO 27001 standards and the adoption of new regulations like NIS2.
Regulation vs. directive	Predominantly compliance-based regulations specific to certain industries.	NIS2 is a directive framework, allowing each EU member state to adapt it to local needs.
Certification	Compliance with standards may vary by sector; certification isn't universal across frameworks.	ISO 27001 is certifiable; however, NIS2 currently lacks a certification path, though future certification requirements may emerge.

Commonalities across cybersecurity frameworks

Framework	Overview
Resilience and recovery	Shift from separate disaster recovery and cyber controls to integrated resilience approaches. Regulations now stress the ability to protect, detect, respond, and recover in a unified model.
Zero Trust principles	The need for "least privilege" access, consistent verification, and breach assumption. Zero Trust architecture is emerging as a common expectation across frameworks.
Continuous monitoring and testing	Regular assessments, testing, and monitoring are essential for meeting and maintaining compliance standards over time.

The role of risk assessment and data classification

Effective risk assessment is vital for achieving compliance and safeguarding critical assets. By identifying high-risk areas and ensuring operational resilience, organizations can align with regulatory standards while protecting business continuity. Effective data classification and governance are foundational steps in this process. Technology managers need to implement the following practices to build a secure and adaptable security framework:

Data classification and governance

- Identify critical assets and data categories.
- Focus resources on high-risk areas.

Operational resilience

- Map critical systems and assess risks.
- Develop and rehearse an incident response plan.

Next steps for building a resilient cybersecurity and compliance framework

Achieving compliance and building a robust cybersecurity framework require a unified strategy that assesses risks, involves key stakeholders, and adapts to new challenges. The following checklist offers practical steps for organizations to strengthen their security posture and ensure regulatory alignment:

1. Prioritize based on risk:
Identify and protect critical assets and business processes to maintain continuity during disruptions.

2. Involve all stakeholders:
Engage C-level, IT teams, and business units to align security goals across the organization.

3. Collaborative risk mapping:
Foster teamwork across departments to create a comprehensive view of potential risks.

4. Exercise and test response plans:
Regularly test your incident response strategy through tabletop exercises to ensure readiness.

5. Regular audits and updates:
Treat cybersecurity as an ongoing program by conducting regular reviews and staying ahead of threats.

6. Focus on training and awareness:
Keep employees informed and engaged with regular cybersecurity training and clear policies.

7. Utilize external audits:
Leverage independent assessments to validate your efforts and identify improvement areas.

8. Invest in continuous improvement:
Stay agile by reassessing strategies and adapting to regulatory and business changes.

> “A common trend in cybersecurity regulations is that all of them are changing. All of them are being updated because the environment we operate in today looks vastly different than only a couple of years ago. That’s because we have a much bigger attack surface, and we introduced more advanced technology to support all our organizations.”
>
> Jimmy Nilson, Global VP at Kyndryl Security Consulting

Here at Keepit we:

Support thousands of organizations as they navigate their compliance journey. We have been recognized by Forrester for our significant experience with data privacy and compliance needs.

Specialize in SaaS data protection

We support a wide range of business-critical SaaS platforms, such as Microsoft 365, Entra ID, Salesforce, and more. Our solution is purpose-built and specifically designed for protecting cloud SaaS data.

Are committed to compliance

Keepit holds end-to-end compliance certifications and is certified by both ISO/ IEC 27001:2013 and the ISAE 3402–II, ensuring the highest standards of data protection and security.

Run independent cloud operations

We maintain our own cloud infrastructure and our own data centers across the world without relying on any data sub-processors. Vendor independence means you’ll always have access to your data.

Deploy leading security measures

We deploy leading security measures, keeping your data safe in a fully air gapped, logically segregated environment with immutability by default and encryption both in transfer and at rest.

Continue the conversation

Watch the on-demand webinar

Watch it now

Keepit provides next-level SaaS data protection purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin