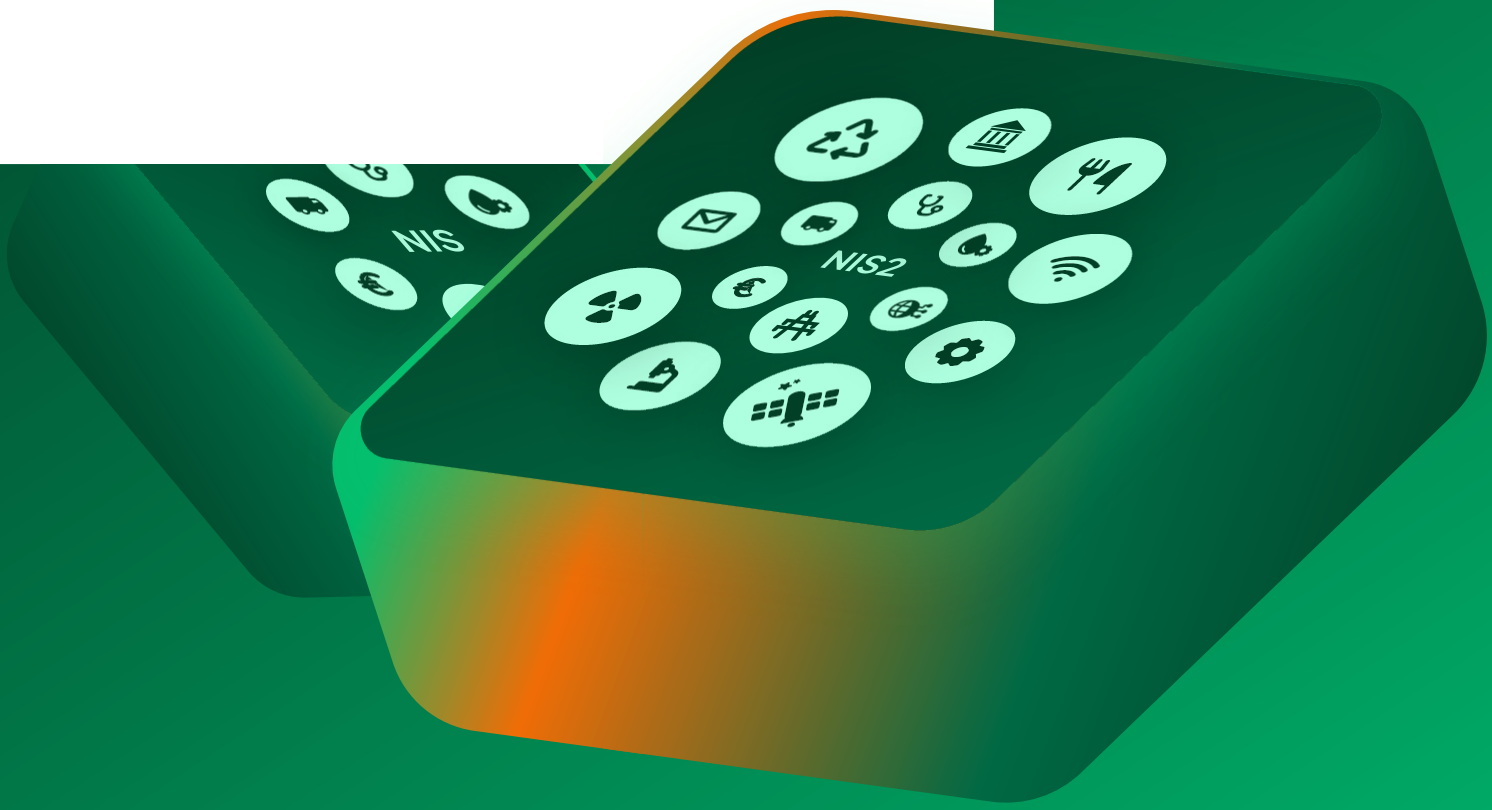
keepit

NIS2 Directive

What you can do now to prepare for compliance

Beginning October 17, 2024, the Network and Information Security Directive (NIS2) will set a new standard for cybersecurity risk management measures and reporting obligations. Organizations must take measures to minimize cyber risks and ensure business continuity to ensure compliance with NIS2.



keepit®

*** Business continuity:** Refers to the high level of readiness an organization maintains in order to confidently execute critical functions during or after an emergency or disruption.

What to do now:

Get your business ready with best practices

What you should do now is run a risk analysis to establish which of your data is business-critical to back up, create a strong disaster recovery plan, and test to know if it works. You can use the following Map-Prioritize-Test framework to help guide you through the process:

1. Map critical systems

Assess and analyze critical infrastructure across on-premises, native cloud, and public cloud environments. Identify and prioritize crucial data, ensuring *business continuity**. Don't overlook SaaS applications like Entra ID; safeguarding identities and credentials is vital. Neglecting identity and access data can impact business continuity even if other data is fully restored. Microsoft recognizes identity systems as more critical than human life support systems: Read more about this.

2. Prioritize: What is critical to maintain access to?

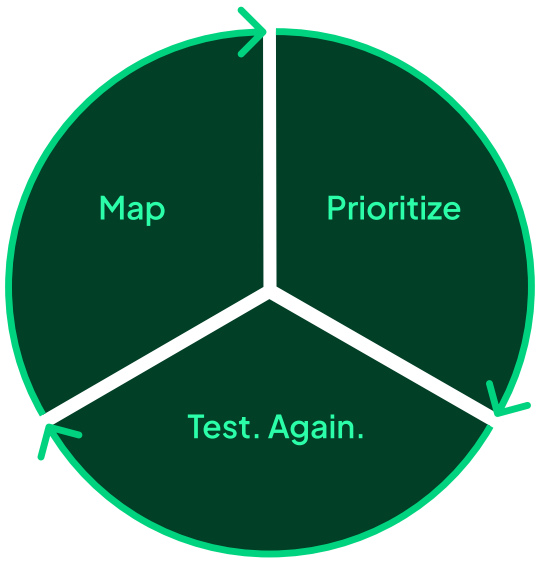
What kind of data do you have? How do you protect it? What is the most critical data to regain access to in the event of an attack? Are your CEO's emails critical to your business continuity? Or maybe your logistics data, customer data, intelligence dashboards, or code? Find out what you need to recover first.

3. Test that your backup works

Testing is a key element of continuity.

Ensure data recovery:

- Validate restoration capability promptly.
- Determine acceptable downtime.
- Regularly test backups for confidence in your dynamic disaster recovery plan and supporting software.



keepit®

Choosing a backup and disaster recovery partner

After implementing the above framework, your next task is to explore solutions tailored to your requirements. When selecting a vendor, adhere to industry best practices for data protection. Consider the following:

Data sovereignty and privacy:

To align with EU regulations like GDPR, ensure your data is stored in a specific geographic location adhering to regional laws. Implement access controls to safeguard against unauthorized access, and process data in compliance with privacy laws. Choose a vendor experienced in data residency and privacy regulations and one that offers a no-transmission guarantee to confidently manage data location and access.

Recovery time:

Recognize the impossibility of recovering petabytes of data within seconds. Prioritize solutions that enable the swift recovery of identified critical data. Business continuity depends on both uninterrupted data availability and minimizing downtime through rapid recovery. Opt for a solution supporting granular, instant, and prioritized recovery of essential data.

Encryption and immutability:

As natural targets for cybercriminals, backups need robust data protection measures, both at rest and during transfer. Vitally important is ensuring data encryption and immutability to keep hackers from altering or deleting your data — even if they were to gain access.

Vendor independence:

Choose a cloud backup provider that ensures separation from your SaaS vendor's public cloud. Employ air-gapping measures and secure data on distinct logical and physical infrastructures. This safeguards against data loss during public cloud unavailability and prevents ransomware attacks from compromising your backups.

keepit®

Who do you trust to keep your data safe? Here at Keepit, we:

- Are European born and built,
- Own and operate our infrastructure and data center regions across the globe — including two EU locations (Denmark and Germany) and one in the UK,
- Ensure full data sovereignty with a no-transmission guarantee, regardless of privacy shield status,
- Deploy leading security measures, such as air gapping, immutability, and encryption both in transfer and at rest,
- Guarantee full compliance with current and future EU regulations, such as NIS2 and GDPR.

NIS2 at a glance

What is the purpose of NIS2?

The purpose of NIS2 is to strengthen EU-wide cybersecurity resilience which includes a requirement for business continuity via backup management and disaster recovery. As such, organizations must maintain a high level of readiness to execute critical functions during a disruption (e.g., a cyberattack) or an emergency. There is a clear priority on protecting critical business SaaS data.

NIS2 requires backup and disaster recovery

In Article 21 of NIS2, it lists several cybersecurity risk-management measures businesses need to adhere to for business continuity, specifically "backup management and disaster recovery."
Learn about Article 21.

Who does NIS2 apply to?

The directive applies to sectors and entities that are classified as "essential" and" important" critical infrastructure like energy, transportation, health, and digital infrastructure. As with GDPR, which protects personal data, NIS2 applies to the organizations on the frontlines and also their contractors.

Start a conversation today

If you'd like to receive advice on your compliance journey and discuss which steps your business needs to take now to comply with the NIS2 directive, let's have a conversation.

Book a meeting

www.keepit.com