



NIS2 Compliance with Dropsuite

Dropsuite's Backup + Recovery solutions can help businesses comply with the NIS2 Directive and avoid penalties

What is NIS2 and why is it being implemented?

The European Union (EU) has implemented the NIS2 Directive, representing a significant step forward in improving cybersecurity compliance across critical sectors.

NIS2 builds upon the three main pillars of the original Network and Information Systems (NIS) Directive to ensure consistency between Member States and expands to include a total of 15 sectors.

The NIS Directive was introduced in 2016 to increase cyber resilience of EU Member States through enforcing incident reporting and other cybersecurity measures.

Consequences of noncompliance

In addition to increased fines of up to €10 million, NIS2 also holds business leadership accountable for failure to meet cybersecurity requirements or report cyber risks, resulting in potential legal ramifications for failure to comply.

Who needs to comply?

The EU has categorized the affected sectors into two tiers:



Essential Entities (EEs)

Energy, transport, finance, public administration, health, space, water supply, and digital infrastructure. IEs face the most stringent compliance requirements.



Important Entities (IEs)

Postal services, manufacturing, waste management, chemicals, research, foods, and digital providers. IEs have slightly less demanding compliance requirements compared to EEs.

Along with expanding the sectors, NIS2 also introduced a size threshold to clarify businesses required to comply. For Essential Entities, the size threshold is approximately 250 employees and for Important Entities it is approximately 50 employees. This means NIS2 now applies to SMBs.

The deadline to comply is October 2024.

NIS2 at a glance...

Deadline

October 2024

15

Affected Sectors

10

Minimum Mandates

NIS2 requirements and the importance of backup + recovery

The NIS2 Organizational Requirements fall into four main categories: risk management, corporate accountability, reporting obligations, and business continuity.

Among the 10 minimum mandated measures, NIS2 necessitates the implementation of robust backup and recovery mechanisms to safeguard critical data and maintain operational continuity in the face of cyber threats.

Key backup requirements include:

- ✔ **Regular backups:** Organizations must perform regular backups of essential systems and data to ensure they can be restored in the event of a cyber incident.
- ✔ **Secure storage:** Backup copies must be stored securely to prevent unauthorized access or tampering, utilizing encryption and access controls.
- ✔ **Rapid recovery capabilities:** Organizations must possess the capability to recover critical systems and data rapidly to minimize downtime and mitigate the impact of cyber incidents on business operations.
- ✔ **Compliance with data protection regulations:** Backup solutions must adhere to data protection regulations such as the General Data Protection Regulation (GDPR) to ensure the privacy and security of personal data.

How Dropsuite can help you comply

Dropsuite's suite of email backup and archiving solutions is engineered to adhere to GDPR and NIS2 requirements, helping organizations streamline, achieve, and maintain compliance.

- ✔ **Secure Backups:** Dropsuite utilizes industry-standard encryption protocols to safeguard your email data at rest and in transit. This ensures the confidentiality and integrity of your data.
- ✔ **Automated Backups:** Our solution automates email backups, eliminating the risk of human error and ensuring consistent data protection. This simplifies compliance by removing the burden of manual backups and scheduling.
- ✔ **Scalable and Reliable Infrastructure:** Dropsuite leverages a secure and reliable cloud infrastructure to store your backed-up email data. This ensures scalability to accommodate your organization's growing needs and guarantees the availability of your data in case of disruptions at your primary location.
- ✔ **Granular Recovery Options:** Dropsuite enables granular recovery of emails, folders, or entire mailboxes. This allows you to retrieve specific data quickly and efficiently in the event of an incident, minimizing disruption to your operations.

To learn more about how Dropsuite can help you meet NIS2 Directive Requirements contact our EMEA sales team: sales@dropsuite.com



© 2024 Dropsuite Limited. All rights reserved.