AIRNITE

ZERO DAY

ISSUE 05/2026 · IT SECURITY

NIS2 is in force: what around 29,500 companies in Germany must do now

Germany's NIS2 implementation act has applied since December 2025. The registration deadline at the BSI has passed and reporting duties apply. Who is affected, what management is responsible for and what to do now.

Published: 21 November 2026 Reading time: 7 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

≈ 29,500
entities affected
"particularly important" and "important" entities according to the BSI

6 Dec 2025
obligations apply since
according to the BSI; act published in BGBl. 2025 I No. 301 on 5 Dec 2025

24 h / 72 h
early warning / notification
for significant security incidents (BSI)

3 months
deadline to register
from becoming subject to NIS2; expired for initial cases according to the BSI

Since 6 December 2025, the obligations of the European NIS2 Directive have applied in Germany. The implementation act was promulgated in the Federal Law Gazette on 5 December 2025. According to Germany's Federal Office for Information Security (BSI), this means statutory cyber security obligations for **around 29,500 entities** for the first time. Other EU countries have their own national laws; this article covers the German implementation.

// What happened?

The EU's NIS2 Directive requires member states to make cyber security mandatory in far more sectors and companies than before. Germany implemented it with the "Act implementing the NIS2 Directive", published in the Federal Law Gazette 2025 I No. 301. At its core is a revised BSI Act (BSIG). It distinguishes between "particularly important" and "important" entities.

Affected companies must register with the BSI themselves – according to the BSI **within three months** of first becoming subject to the rules. For companies affected from the start, the BSI says this deadline **has already passed**. The BSI urges latecomers to register immediately.

// How does the obligation work?

Registration takes two steps: first the company needs an organisation account via "Mein Unternehmenskonto" with an ELSTER certificate, then it uses that to register in the BSI portal. According to the BSI, changes must be reported without delay, at the latest after two weeks.

After that, two areas of obligations apply. First, **risk management**: section 30(2) BSIG lists ten areas of measures, from risk analysis and incident handling to supply chain security. Second, the **reporting obligation** for significant security incidents: an early warning **within 24 hours** of becoming aware, a notification **within 72 hours** and a final report **no later than one month** afterwards. According to the BSI, entities that are not yet registered must still report incidents – via a separate form.

// Who is affected?

Whether a company is affected depends mainly on its sector and size. The BSI offers a free **NIS2 applicability check** for this: an anonymous questionnaire that gives an initial assessment. The BSI stresses that it does not replace a company's own assessment. Federal, state and municipal administrations are not covered by the tool.

Responsibility explicitly lies at the top: according to the BSI, responsibility for implementing and supervising the measures lies **with management**. In 2026 the BSI also published material for management training. NIS2 is therefore not just an IT issue but a matter for the boardroom.

// What should you do now?

Anyone who does not yet know whether they are affected should complete the BSI applicability check and have the result confirmed legally. Anyone who is affected and has not yet registered should do so immediately. At the same time, every affected company needs a working reporting process: 24 hours is short if nobody notices until Monday that something happened on Saturday.

Then comes the real work: compare security measures with the requirements, close gaps by risk, involve suppliers and train management. The checklist below sums up the steps.

// How does Airnite help?

In **consulting**, Airnite guides you through the assessment and prepares a gap analysis of your measures under section 30 BSIG. We help set up a reporting process with clear roles and templates. In **training**, we explain clearly to management and staff what NIS2 requires. With **penetration tests**, we check whether your measures hold up in practice. Legal questions are clarified together with your legal advisers.

> Note: general information, not legal advice. We have not checked fine amounts and details of individual sections in the legal text and therefore do not cite them. Research status: 21 November 2026.

Checklist: what to do now

[+] Get an initial assessment with the BSI's free NIS2 applicability check and have the result confirmed legally.

[+] If affected and not yet done: register immediately – organisation account via “Mein Unternehmenskonto” (ELSTER certificate), then in the BSI portal.

[+] Define a reporting process: who recognises a significant incident, who reports within 24 hours, who delivers the 72-hour notification and the final report?

[+] Compare the risk management measures under section 30(2) BSIG with your current state and prioritise gaps.

[+] Involve management: approve measures, supervise implementation, take part in training.

[+] Include suppliers and service providers: add security requirements to contracts and review their access.

How Airnite helps

- Consulting – An outside view of your plans and projects.
- Training – Your team learns our tools and processes.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.

Are you subject to NIS2 – and prepared?

Airnite helps you assess your status, analyse gaps in your security measures and set up a reporting process that meets the 24-hour deadline. For management we offer clear training on duties and risks. Legal questions are clarified together with your legal advisers.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/nis2-obligations-companies-germany/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **BSI · NIS-2-regulierte Unternehmen** · as of November 2026 · PRIMARY SOURCE
   Primary source: two-step registration, notice that the deadline has passed
   https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html
2. **BSI · NIS-2-Pflichten** · as of November 2026 · PRIMARY SOURCE
   Primary source: approx. 29,500 entities, registration within three months, reporting deadlines, management responsibility
   https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Pflichten/nis-2-pflichten_node.html
3. **BSI · NIS-2-Meldepflicht** · as of November 2026 · PRIMARY SOURCE
   Primary source: 24 hours, 72 hours, one month; obligations from 6 Dec 2025
   https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Meldepflicht/NIS-2-Meldepflicht_node.html
4. **BSI · NIS-2-Betroffenheitsprüfung** · PRIMARY SOURCE
   Tool: anonymous, non-binding initial assessment
   https://betroffenheitspruefung-nis-2.bsi.de/
5. **Bundesgesetzblatt · Act implementing the NIS2 Directive (BGBl. 2025 I No. 301)** · 5 Dec 2025 · PRIMARY SOURCE
   Legal text
   https://www.recht.bund.de/bgbl/1/2025/301/VO.html

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de