EU security laws: which apply to you and what is due when?

Check which of your legal entities fall under NIS2 or DORA and which products under the CRA, since all three require a first report within 24 hours[1,2,3]. Then resolve overlaps by role: DORA replaces NIS2's risk and reporting rules for financial entities[1] and the CRA adds product duties, so one group can face all three.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.2**	**IT, security and compliance leads in EU organizations, especially in Germany**

Latest version
sheets.einblick.dev/eu-security-laws/

If you only do five things

This is guidance, not legal advice.

1. **Decide scope per legal entity and product.** NIS2 and DORA apply to entities[1,4], the CRA to products with digital elements and their manufacturers, importers and distributors[3]. Record the sector and size figures you used.
2. **Run one incident process with several clocks.** NIS2 and the CRA require an early warning within 24 hours[1,3] and DORA an initial notification within 4 hours of classification as major[2]. Name who classifies incidents and who sends each report.
3. **Have management sign off and take training.** Management bodies must approve and oversee the NIS2 risk management measures and take training, and they can be held liable[1]. Put both on the board calendar.
4. **Map your controls to the NIS2 measures.** Article 21 requires measures in at least ten areas, from incident handling and backups to supply chain security and multi-factor authentication[1]. Give each gap an owner and a date.
5. **Put the duties into supplier contracts.** DORA requires a register of information on all ICT service contracts[4] and NIS2 requires supply chain security[1]. Add security update, incident notification and audit clauses at renewal.

Find out which laws apply to you

1. **Do you supply connected products in the EU?**
   If you make, import or distribute hardware or software that connects to a device or network, the CRA applies to those products[3]. Medical devices, motor vehicles and certified aviation products are excluded, as are cloud services that aren't remote data processing for a product[3].
2. **Are you a financial entity under DORA?**
   DORA lists 20 types, including credit institutions, payment and e-money institutions, investment firms, crypto-asset service providers, insurers and fund managers[4]. For them it replaces NIS2's risk management, reporting and supervision[1].
3. **Is your sector in NIS2 Annex I or II?**
   NIS2 covers 18 sectors, among them energy, transport, health, finance, digital infrastructure, digital services, critical product manufacturing, waste, postal services and public administration[5]. If no annex lists your type of entity, NIS2 generally doesn't apply[1].
4. **How big is the entity?**
   An Annex I or II entity is in scope with 50 or more employees, or with turnover and balance sheet both above €10 million. An Annex I entity is essential with 250 or more employees, or with turnover above €50 million and a balance sheet above €43 million[6,1]. Telecom, trust service and DNS providers and TLD registries are in scope at any size[1].

The three laws side by side

NIS2

- **Who.** Medium and large entities in the Annex I and II sectors, plus telecom, trust service and DNS providers and TLD registries at any size[1].
- **Duties.** Management-approved risk management measures in at least ten areas, incident reporting and registration with the national authority[1].
- **Dates.** Member States had to apply it from 18 October 2024[1].
- **Penalties.** Maximum fines of at least €10 million or 2% of worldwide turnover, whichever is higher, for essential entities and €7 million or 1.4% for important ones[1]. Managers of essential entities can be temporarily barred[1].

DORA

- **Who.** 20 types of financial entity[4], plus critical ICT providers: 19 designated in November 2025, including AWS, Microsoft and SAP[7].
- **Duties.** An ICT risk management framework owned by the management body, major incident reporting, resilience testing and a register of information on all ICT service contracts[4]. Threat-led penetration tests at least every 3 years for entities their supervisor selects[4].
- **Dates.** Applies since 17 January 2025[4].
- **Penalties.** Set by Member States, also for management body members[4]. Daily penalties of up to 1% of average daily worldwide turnover for critical ICT providers[4].

CRA

- **Who.** Manufacturers, importers and distributors of connected hardware and software in the EU[3].
- **Duties.** The Annex I security requirements, a software bill of materials, CE marking and vulnerability handling for a support period of at least 5 years, or the expected use time if shorter[3].
- **Dates.** In force since 10 December 2024[8]. Reporting applies from 11 September 2026 and the remaining duties from 11 December 2027[3].
- **Penalties.** Up to €15 million or 2.5% of worldwide turnover for breaches of Annex I or Articles 13 and 14[3].

What you can skip

- **Waiting for the proposed changes.** Neither the reporting rules in the general Digital Omnibus nor the NIS2 amendments are law yet[9,10], and the proposed single entry point would keep today's reporting duties and recipients[11].
- **A separate compliance program for each law.** Keep one risk register for all three and add law-specific steps only where the duties differ.

Mistakes that cost the most

- **Leaving group companies out of the size test.** The EU test adds the figures of linked and partner enterprises[6].
- **Waiting for the full picture to report.** The NIS2 early warning only has to say whether you suspect unlawful or malicious acts or cross-border impact[1].
- **Forgetting products already on the market.** CRA reporting also covers products placed on the market before December 2027[3].

- **Reporting every alert.** NIS2 requires reports only for incidents that cause or could cause severe operational disruption, financial loss or considerable damage to others[1]. Give the on-call team written thresholds.

Reporting clocks

Each clock starts when you become aware, unless noted.

NIS2

Significant incidents, to the CSIRT or competent authority; in Germany, the BSI[13]. The final report is due 1 month after the notification[1].

24 hours	72 hours	1 month
Early warning	Incident notification	Final report

DORA

Major ICT-related incidents, to the competent authority. The 4 hours run from classification, capped at 24 hours after awareness unless you classify later; later clocks run from the previous report[2].

4 hours	72 hours	1 month
Initial notification	Intermediate report	Final report

CRA

Manufacturers, through ENISA's platform[15]. The final report is due 14 days after a fix for actively exploited vulnerabilities and 1 month after the notification for severe incidents[3].

24 hours	72 hours	14 days
Early warning	Notification	Final report

What changed in 2026

- **CRA reporting started.** Since 11 September 2026 manufacturers must report actively exploited vulnerabilities and severe incidents[3].
- **The Commission proposed NIS2 amendments.** Its proposal of 20 January 2026 would clarify the scope to ease compliance for 28,700 companies, add a small mid-cap category and simplify jurisdiction rules[20]. It still awaits a committee decision in Parliament[10].
- **Missing the implementing regulation.** Cloud, data center, managed service and other digital providers must also meet the detailed requirements of Implementing Regulation (EU) 2024/2690[12].

Germany: the NIS2 Implementation Act

- **The law took effect on 6 December 2025.** The act was published in the Bundesgesetzblatt on 5 December 2025, with no general transition period[16,17]. It applies to about 29,500 companies and federal institutions[18].
- **The registration deadline has passed.** Entities must register within 3 months of falling under the law, so the first deadline passed in March 2026[13,19]. If you haven't registered, get an ELSTER organization certificate through Mein Unternehmenskonto, then register in the BSI portal[19], open since 6 January 2026[18]. Report changes within 2 weeks[13].
- **DORA entities must register too.** They are exempt from the BSIG's risk management, reporting and management body duties, and the BSIG rules out reporting the same incident under both laws[17].
- **Energy operators follow the EnWG.** Grid and energy plant operators meet their security and management duties through the Federal Network Agency's IT security catalogs under §§ 5c and 5e EnWG, but still register with and report to the BSI[13,14].
- **Group figures can be left out.** The BSIG excludes linked and partner enterprises from the size test if your IT systems run independently of theirs[13].
- **Management is liable to the entity.** It must implement and oversee the risk management measures and attend regular training, and it is liable for culpable damage under company law[13].
- **The Council wants national reporting entry points.** The general Digital Omnibus, separate from the one on AI, would let you file NIS2, DORA, GDPR and other reports through one ENISA entry point[11]. The Council's position of 21 October 2026 swaps it for one national entry point per Member State and backs a longer GDPR breach deadline; Parliament has not adopted its position yet[9].

Version history

5 Nov 2026, version 1.2	Added that German energy grid and plant operators meet their security and management duties through the Federal Network Agency's IT security catalogs under the EnWG, but still register with and report to the BSI.

Sources

1. Directive (EU) 2022/2555 (NIS2), Articles 2 to 4, 20, 21, 23, 32, 34 and 41 and recital 28. EUR-Lex, 2022. eur-lex.europa.eu
2. Commission Delegated Regulation (EU) 2025/301 (DORA incident reporting standards), Article 5. EUR-Lex, 20 Feb 2025. eur-lex.europa.eu
3. Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 2, 13, 14, 19, 20, 30, 64, 69 and 71, recital 12 and Annex I. EUR-Lex, 2024. eur-lex.europa.eu
4. Regulation (EU) 2022/2554 (DORA), Articles 1, 2, 5, 26, 28, 35, 50 and 64. EUR-Lex, 2022. eur-lex.europa.eu
5. NIS2 Directive: securing network and information systems. European Commission, 2 Jul 2026. digital-strategy.ec.europa.eu
6. Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises, Annex Articles 2 and 6. EUR-Lex, 6 May 2003. eur-lex.europa.eu
7. List of designated critical ICT third-party service providers at Union level. European Supervisory Authorities (EBA, EIOPA, ESMA), 18 Nov 2025. esma.europa.eu
8. Cyber Resilience Act. European Commission, 7 Sep 2026. digital-strategy.ec.europa.eu
9. Digital rulebook: Council agrees position to simplify data protection, privacy and cyber reporting rules. Council of the EU, 21 Oct 2026. consilium.europa.eu
10. 2026/0012(COD): Amending the NIS 2 Directive as regards simplification measures and alignment with the Cybersecurity Act 2. European Parliament Legislative Observatory, checked 2 Nov 2026. oeil.europarl.europa.eu
11. Digital Package. European Commission, 20 Nov 2025. digital-strategy.ec.europa.eu
12. Commission Implementing Regulation (EU) 2024/2690, Article 1. EUR-Lex, 2024. eur-lex.europa.eu
13. BSI-Gesetz (BSIG), §§ 28, 32, 33 and 38. BMJV (Germany), checked 2 Nov 2026. gesetze-im-internet.de
14. Energiewirtschaftsgesetz (EnWG), §§ 5c to 5e. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
15. The CRA Single Reporting Platform is launched. ENISA, 11 Sep 2026. enisa.europa.eu
16. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (BGBl. 2025 I Nr. 301). Bundesgesetzblatt, 5 Dec 2025. recht.bund.de
17. Fragen und Antworten zu NIS-2. BSI, checked 2 Nov 2026. bsi.bund.de
18. Zweiter Schritt zur NIS-2-Registrierung: BSI-Portal ab sofort freigeschaltet. BSI, 6 Jan 2026. bsi.bund.de
19. NIS-2-regulierte Unternehmen. BSI, checked 2 Nov 2026. bsi.bund.de
20. Cybersecurity Package - Questions & Answers. European Commission, 20 Jan 2026. digital-strategy.ec.europa.eu