IS CONSULTING

NAVIGATING EU CYBERSECURITY LAWS A COMPREHENSIVE GUIDE FOR SMEs

1. Executive Summary

Small and medium-sized enterprises (SMEs) across Europe are increasingly impacted by new cybersecurity regulations. In plain terms, these EU laws aim to strengthen digital security and protect data – and they now affect businesses of all sizes, not just big tech firms or critical infrastructure. Why should SMEs care? Because cyber threats can hit anyone, and the EU is raising the bar for cybersecurity practices. Failing to meet basic security or data protection standards can lead to severe fines or being cut off from valuable markets. On the positive side, complying with these rules will help SMEs build customer trust, avoid downtime, and even compete for new business (many larger clients demand strong security from their suppliers).

As of 2025, the European Union has a patchwork of cybersecurity laws and initiatives that SMEs need to know about. Some apply broadly (like the GDPR data protection law and new *"NIS2"* cybersecurity rules), while others target specific sectors (like finance, energy, health, or automotive). New regulations such as the Cyber Resilience Act will soon require secure-by-design products – meaning manufacturers (including SME innovators) must ensure their hardware and software are cyber-safe. The key message is that SMEs cannot afford to ignore cybersecurity compliance. Regulators now expect even smaller businesses to assess their cyber risks, implement basic protections, train their staff, and report serious incidents. This guide breaks down the complex EU cybersecurity landscape into practical terms: what each law covers, how SME obligations are calibrated, and what steps to take in the next 12 months to stay compliant and secure. It provides a roadmap, checklists, and resources to help SME managers turn legal requirements into actionable security improvements. In short, cybersecurity regulation is no longer "someone else's problem" – it's part of doing business in the digital economy, and this guide will help you navigate it confidently.

2. Timeline of Key EU Cybersecurity Milestones (2016–2028)

To comprehend how the regulatory environment has evolved – and to keep an eye on upcoming dates – here's a chronological timeline of major events and deadlines in the EU cybersecurity ecosystem:

- **2016:** EU adopts two cornerstone laws – the original Network and Information Security Directive (NIS1, Directive 2016/1148) and the General Data Protection Regulation (GDPR, Regulation 2016/679). These set the stage for EU-wide cybersecurity and data protection obligations.
- **2018:** GDPR and NIS1 both become fully applicable (May 2018). Companies across Europe scramble to meet GDPR's deadline – leading to widespread updates of privacy policies and security practices. NIS1 transposition also due; national laws on critical services' cybersecurity kick in.
- **2019:** The EU Cybersecurity Act (Regulation 2019/881) enters into force in June. ENISA is strengthened and work begins on European cybersecurity certification schemes. Also in 2019, the EU's "5G Security Toolbox" is developed (published January 2020) as Member States coordinate on securing next-gen telecom networks.
- **2020:** The European Commission releases the EU Security Union Strategy (2020), signaling upcoming initiatives like NIS2, CER, and the Cyber Resilience Act. The COVID-19 pandemic accelerates digital transformation (and cyber risks) for SMEs.
- **2021:** New sectoral rules take effect: IMO's maritime cyber mandate (January 2021) for shipping and UNECE's automotive cybersecurity regulation (UN R155) (July 2021 for new vehicle types) – pushing transport industries to adopt cyber controls. The Commission proposes the AI Act (April 2021) and Digital Identity (eIDAS2) (June 2021), heralding future compliance needs for AI providers and eID schemes.
- **2022:** A landmark year for EU cyber legislation – three major laws are adopted in December: NIS2 Directive (Directive (EU) 2022/2555), CER Directive (EU 2022/2557), and DORA (Regulation (EU) 2022/2554). Additionally, the Digital Operational Resilience Act for finance is published on 27 Dec 2022, and the Council adopts NIS2 and CER on 14 Dec 2022. Also in 2022, the Radio Equipment Directive Delegated Act (EU 2022/30) is adopted to impose IoT security from 2025.
- **2023:** Implementation phase. NIS2 and CER are in force (Jan 2023) and Member States work on transposition (due by Oct 17, 2024). The European Commission

opens infringement cases in late 2024 against states slow to transpose. DORA enters into force (Jan 2023) and regulators draft technical standards throughout 2023–24. Meanwhile, the Cyber Resilience Act (CRA) is negotiated: the European Parliament approves it in plenary (Mar 2024) the Council adopts it on 10 Oct 2024.

- **2024:** Big developments: AI Act is finalized – Regulation (EU) 2024/1689 is published OJ 12 July 2024, entering force 1 Aug 2024The amended eIDAS2 Regulation (EU 2024/1183) enters force May 2024, kicking off the rollout of European Digital Identity Wallets. NIS2 & CER transposition deadline hits in Oct 2024 – effectively replacing NIS1 and expanding critical infrastructure resilience requirements. The Network Code on Cybersecurity for Electricity is adopted as Delegated Reg 2024/1366 (May 2024). EU Cybersecurity Skills Academy is launched (2023–24) to tackle the skills gap for implementing these laws.
- **2025:** DORA becomes fully applicable on 17 Jan 2025 – financial entities must now comply (many will have spent 2023–24 preparing). Enforcement of NIS2 begins across Member States (most designation of essential/important entities by April 2025). The RED IoT cybersecurity requirements go live on 1 Aug 2025, meaning all wireless products launched after must be secure by design. The AI Act's first obligations kick in Feb 2025 (prohibited AI practices banned). 2025 is also when aviation cybersecurity (Part-IS) requirements start applying (Oct 2025) for airlines/airports.
- **2026:** AI Act main application date – 2 Aug 2026. Providers of high-risk AI must by now comply with the new rules (documentation, conformity assessments, etc.), and the European AI Office begins oversight. Also, eIDAS2 24-month deadline: by late 2026, every EU Member State will offer an EU Digital ID Wallet to citizens, and private services (including SMEs) may start integrating these for login/verification. In aviation, Part-IS cybersecurity fully applies by Feb 2026 for remaining orgs.
- **2027:** Cyber Resilience Act compliance deadline – 11 Dec 2027: all in-scope products (from IoT toys to enterprise software) being sold must meet CRA requirements and have the CE marking for cybersecurity. Expect 2027 to see a rush of conformity assessments and certifications for "critical" products under CRA. Also, AI Act gives an extended deadline until Aug 2027 for high-risk AI that is safety components of products (e.g. AI in medical devices or cars) – those become enforceable by this date (aligned with product recertification cycles).
- **2028:** Review and refinement. By 2028, the EU will likely review NIS2's effectiveness (such directives often have a review clause ~3-4 years after

application, i.e. possibly 2027/28). GDPR might see its first major amendments after a decade in force. New areas like quantum cybersecurity or 6G network security could spawn initiatives. Importantly, SMEs that embraced compliance early will be well-positioned, whereas laggards may face enforcement as regulators by this time have fully ramped up their capacity to monitor also smaller entities.

(Note: Dates above are current as of May 2025.)

3. SME-Specific Angle: Proportional Rules and Exemptions

Not all SMEs are treated equally under these laws – many regulations build in thresholds or lighter duties for smaller businesses. Understanding these proportionality clauses is crucial so you know when you're *in* or *out* of scope:

- **Company Size Thresholds:** A common rule is that micro and small enterprises (fewer than 50 employees and <€10 million turnover) are exempt from certain regulations *unless* they operate in high-impact areas. For example, the NIS2 Directive explicitly excludes micro and small firms from its scope unless an exception applies. That means if you run a small business *not* in a critical sector, NIS2 obligations likely won't apply to you. However, exceptions can pull even a small company in scope if it's the sole provider of an essential service or if it's a special case like a DNS registry, Internet exchange point, or trust service provider (these are critical regardless of size). GDPR, on the other hand, has no blanket small business exemption – it applies based on data handling, not headcount. Even a tiny startup must comply with data protection law if processing personal data, though *some* obligations (like need for a Data Protection Officer) kick in only if certain criteria are met.
- **"Essential" vs "Important" Entities (NIS2):** NIS2 divides covered organizations into two tiers. Essential entities (typically larger companies in vital sectors like energy, transport, banking, health, digital infrastructure) face more stringent oversight – continuous supervision, regular audits, and higher fines for non-compliance. Important entities (often medium-sized firms or large firms in slightly less critical sectors) have the *same security duties* but are subject to lighter oversight – mainly reactive (ex-post) checks if something goes wrong. For SMEs, this means if you are just over the medium-size threshold (50+ employees) in a NIS2 sector, you might be an "important" entity: you must implement all required cyber measures, but you might not be audited until an incident happens. The security requirements themselves do not dilute for smaller entities – important and essential entities must both meet NIS2's baseline controls (like incident response planning, access controls, encryption,

etc.). The difference is mainly in how the law is enforced and the maximum fine levels.

- **Finance Sector Proportionality:** DORA covers even small financial entities, but it acknowledges that one-size-fits-all is inappropriate. Regulators will consider an institution's size and risk profile when assessing DORA compliance. For example, a small community bank or a medium fintech startup must implement ICT risk management, but the depth and formality can be scaled down versus a global bank. *Certain very small pension funds* (IORPs with <15 members) are fully exempt from DORA, and those up to 100 members have simplified requirements. Apart from such specific carve-outs, most SMEs in finance need to comply, but they can expect their supervisors to apply the rules proportionately (e.g. fewer required penetration tests for a small firm, perhaps).
- **Other SME Considerations:** Many regulations include recitals or articles emphasizing *proportional implementation*. For instance, the Cyber Resilience Act was debated to ensure it doesn't overburden small device makers – the final text includes support measures and possibly longer transition periods for smaller manufacturers. The AI Act also has provisions to support SME innovation, like regulatory sandboxes and reduced fees, acknowledging limited resources. However, if an SME's product or service falls under high-risk use, it still must comply fully – but authorities might give guidance to help.
- **Typical Exemptions:** Some laws exempt organizations that *already comply with an equivalent standard*. Under NIS2, if you're an SME that is already regulated under sector-specific cyber rules (for example, a small electricity distribution operator covered by the energy Network Code), you might not have duplicate NIS2 duties. Similarly, firms under DORA may be exempt from NIS2 if there's overlap, to avoid double regulation. Always check if a domain-specific rule overrides a general one for your case.

In summary, SMEs benefit from a risk-based approach in EU laws: if your business is low-risk and small-scale, you're often left out of the most burdensome regimes. But as soon as an SME provides something critical to society (be it internet infrastructure, financial services, healthcare devices, etc.), the law tends to apply regardless of size – because the potential impact of a cyber incident is big. Policymakers have tried to reduce red tape for the smallest players, but core principles like data protection and basic cyber hygiene apply to everyone. It's wise for SMEs to voluntarily adopt good security practices even if not explicitly mandated – not only to prepare for growth (you might cross the threshold soon)

but also to meet contractual expectations from clients and to genuinely protect your business.

Common Pitfall: Assuming "We're too small to matter." In reality, threat actors often target SMEs precisely because they may have weaker defenses, and many EU laws (like GDPR or product safety rules) apply even to micro-businesses. Don't wait until you grow or until an incident happens – basic compliance and security should start early.

Quick Win: Even if you're below a size threshold, implement the spirit of the regulations proactively. For example, conduct a simple risk assessment, draft an incident response plan, and train your staff on cybersecurity awareness. These low-cost steps go a long way toward both compliance and cyber resilience.

4. 12-Month Compliance Roadmap for an SME

Achieving cybersecurity compliance (and better security overall) is a journey – here's a month-by-month plan to guide a typical SME over the next year. This roadmap assumes you're starting from minimal security measures and builds up to a solid compliance posture by month 12. Each month focuses on achievable milestones:

1. **Month 1 – Initiation & Responsibility:** Secure top management support and designate a Cybersecurity Lead (even if not a formal CISO, someone must coordinate). Communicate to all staff that cybersecurity and data protection are now organizational priorities. If GDPR applies, identify a Data Protection Officer or privacy point-person. Begin logging all IT assets and any personal data stores.

2. **Month 2 – Risk Assessment:** Perform a basic cyber risk assessment. Identify your critical information and systems (e.g. customer data, e-commerce platform, payment system) and the main threats (hackers, malware, human error). Rank your top risks. Also review which EU laws apply – e.g. do you handle personal data (GDPR), provide essential services (NIS2), or build digital products (CRA)? Use the decision-tree later in this guide for this step.

3. **Month 3 – Policies & Procedures:** Draft or update simple security policies. Key ones include: an Acceptable Use Policy for staff (how to handle passwords, devices, etc.), an Incident Response Plan (steps to take if something goes wrong), and a Data Protection Policy (covering GDPR basics on data handling). Keep them short and tailored to your risks. Have management approve these and circulate to all employees.

4. **Month 4 – Quick Technical Wins:** Implement "cyber hygiene" measures. Ensure all computers and devices have updated antivirus/anti-malware

protection and firewalls configured. Enable automatic software updates on all systems to patch vulnerabilities promptly. If not already in place, set up data backups (and test restoring from backup). Enforce strong passwords (consider a password manager) and wherever possible turn on multi-factor authentication (especially for email, VPN, banking, cloud services).

5. **Month 5 – Staff Training & Awareness:** Conduct an all-hands security awareness training. Teach employees how to spot phishing emails and social engineering, the importance of using strong passwords and safeguarding data, and the procedure for reporting incidents. Even a short interactive session or an online module can significantly reduce human-related risks. Make this training mandatory for new hires too. Reinforce a culture where people feel responsible for cybersecurity (e.g. no one writes passwords on sticky notes, everyone double-checks unusual payment requests).

6. **Month 6 – Incident Response Drill:** Using your Incident Response Plan, run a tabletop exercise or simple drill. For instance, simulate a ransomware attack or data breach on a Friday afternoon – walk through who does what, how to isolate systems, whom to call (law enforcement, IT support, customers?), and how to recover. This will reveal gaps in your plan and build confidence that you can handle real incidents. Update the plan based on lessons learned.

7. **Month 7 – Secure the Supply Chain:** Review your critical suppliers and service providers. Do you rely on a cloud hosting company, an IT support contractor, or a software vendor? Ensure they meet basic security standards too. This might mean sending a brief security questionnaire to key vendors or checking if they have certifications (like ISO 27001) or adherence to codes of conduct. Also, update contracts to include data protection and security clauses – GDPR requires that your processors (e.g. an email marketing platform handling your customer data) sign Data Processing Agreements. If you are subject to NIS2 or DORA, start engaging with suppliers about incident reporting and risk measures (these laws demand oversight of third-party risk).

8. **Month 8 – Compliance Checkpoint:** By now, you have many controls in place – it's time to check against the specific regulations. Perform a gap analysis: For GDPR, do you have required documentation (records of processing activities, privacy notices, consent forms if needed)? For NIS2, are you implementing the "basic cyber measures" listed in the directive (asset management, access control, encryption, etc.)? For CRA (if you produce software/devices), are you working on securing product design and drawing up compliance docs (e.g. vulnerability disclosure policy)? Make a list of gaps for each applicable law and

plan how to close them. This might be a good time to seek external advice or a consultant for a one-off compliance audit if budget allows.

9. **Month 9 – Improve & Formalize:** Address the gaps identified. This could include: writing a simple Business Continuity Plan (how to keep operating during IT outages – often required under CER or NIS2 for critical entities); tightening user access rights (principle of least privilege); implementing logging and monitoring for your network (even basic logging of admin activities and periodic log review); and updating configurations to meet best practices (e.g. disable old protocols, ensure encryption is used for remote access). If you handle sensitive personal data, consider a vulnerability scan or penetration test on your website/app (some regulations and good practice recommend regular testing).

10. **Month 10 – Documentation & Certification:** Compile all your policies, procedures, training records, and technical measures into a Cybersecurity Handbook (even if informal). Regulators often ask for documentation during inspections – you'll be ready to show your efforts. At this stage, you might also consider certifications or standards for external validation. Achieving ISO/IEC 27001 (Information Security Management) certification or aligning with CIS Controls can demonstrate compliance with NIS2's risk-management requirements, for example. If full certification is too heavy, you could adopt Cyber Essentials (a basic security badge in some countries) or other industry-specific security marks. Month 10 is also a good point to ensure you have completed any registrations or filings (for instance, if under NIS2, have you notified your national authority that you're in scope? If under GDPR, is your privacy notice filed or DPO registered if required?).

11. **Month 11 – Testing & Audit:** Conduct an internal audit or management review of your cybersecurity. Go through each policy and control: is it implemented and effective? For example, test whether backups actually restore data, or whether employees are following password rules. If resources permit, have an external expert do a penetration test or security assessment of your critical systems; fix any high-risk findings. Also review incident logs – were there any near-misses that went unreported? Use this audit to update your risk assessment from Month 2 with current information.

12. **Month 12 – Ongoing Governance:** By now, you should feel much more on top of cyber risks. Establish a routine for the future: set up quarterly security meetings or reports to management, plan to refresh training annually, schedule periodic scans and drills. Also, keep an eye on updates – laws evolve

(e.g. new guidance under NIS2, or upcoming AI Act obligations by 2026). Mark your calendar for key future dates (like the 2027 CRA product compliance deadline) to ensure continued compliance. Celebrate your progress with your team – cybersecurity is now part of your company's DNA, which is a competitive and operational strength.

Following this roadmap, in one year an SME can significantly raise its cybersecurity maturity and meet core compliance requirements. The key is steady, incremental improvement – tackling a few focused actions each month – rather than leaving everything until a deadline or, worse, until after a security incident or regulator notice. By embedding these practices, you're not only avoiding penalties but actively protecting your business's continuity and reputation.

5. Quick-Check Compliance Checklist

For busy managers, here's a practical checklist of essential actions to confirm your SME is on the right track. Use this table as a quick internal audit – if you can tick all the boxes, you're likely covering the major bases of EU cybersecurity laws:

Compliance Item	Status
1. Data Protection (GDPR): Do we know what personal data we hold, where it's stored, and have we informed individuals (privacy notice)? Do we have a lawful basis for processing and, if required, consent recorded?	✔ / ✘
2. Appointed Roles: Have we assigned responsibility for cybersecurity (e.g. a security lead) and data protection (DPO or contact person if needed)? Are these roles aware of their duties?	✔ / ✘
3. Risk Assessment: Have we performed a cybersecurity risk assessment and identified our critical assets and threats? (And for any high-risk personal data or AI system, conducted the necessary impact assessment.)	✔ / ✘
4. Security Measures in Place: Do we have up-to-date antivirus/anti-malware on all systems and networks protected by firewalls? Are all software and devices patched with the latest security updates?	✔ / ✘
5. Access Control: Are user accounts managed with least privilege? (E.g. employees only access what they need.) Do we use strong passwords and 2FA/MFA for important systems (email, finance, remote access)?	✔ / ✘

6. Backup and Recovery: Are we backing up important data regularly, and is the backup stored securely offsite/offline? Have we tested that we can restore data from backups successfully?	✔ / ✘
7. Incident Response: Do we have an incident response plan or procedure and is it known to the team? (Who to call, how to isolate an issue, initial steps.) Have we practiced an incident drill in the last year?	✔ / ✘
8. Incident Reporting Ready: Do we know our obligations to report incidents? (E.g. Personal data breaches to the DPA within 72 hours; NIS2 significant incidents to CSIRT; etc.) Is a draft incident report template prepared?	✔ / ✘
9. Vendor Management: Have we checked that key suppliers handling our data or systems have adequate security? Do we have contracts/DPA in place requiring them to protect our data and inform us of incidents?	✔ / ✘
10. Training & Awareness: Have all employees (incl. non-IT staff) received basic cybersecurity awareness training in the past year? Do we regularly remind staff about phishing risks and safe computing practices?	✔ / ✘
11. Policies & Documentation: Do we have written policies for IT security and data protection (even short ones)? Are they communicated and acknowledged by staff?	✔ / ✘
12. Compliance Records: Can we produce evidence of compliance if asked – e.g. logs of software updates, training attendance, risk assessment report, inventory of personal data, etc.? (Having these ready is important for audits.)	✔ / ✘
13. Sector-Specific Checks: (If applicable) If we are in a regulated sector (finance, health, energy, etc.), have we addressed those specific requirements? E.g. DORA ICT continuity plan, MDR technical file includes cybersecurity, etc.	✔ / ✘
14. Upcoming Regulations: Are we aware of near-future laws that might affect us (e.g. Cyber Resilience Act by 2027 for product makers, AI Act by 2025–2026 for AI use)? Have we mapped out a plan to comply with any that apply?	✔ / ✘
15. Continuous Improvement: Is there a process for regular review (annual or quarterly) of our cybersecurity posture by management? (Compliance is not one-and-done – ensure ongoing oversight.)	✔ / ✘

If you answered "No" or "Not sure" (❌) to any of the above, that's a flag to take action. Prioritize closing those gaps as part of your next steps. This checklist covers the fundamental expectations of EU regulators and good practice frameworks; it can be adapted to your specific business context.

6. Best-Practice Toolbox for SMEs

Beyond strict legal requirements, SMEs can tap into a wealth of frameworks and resources to uplift their cybersecurity. These best practices align with EU regulations and can often streamline compliance. Here's a toolbox of standards and guidance:

- **ENISA Guidance for SMEs:** The European Union Agency for Cybersecurity (ENISA) produces practical resources to help SMEs. For example, ENISA's "12 Steps to Securing Your Business" guide provides non-technical actions SMEs should take (from developing a security culture to securing backups). ENISA also offers free tools on risk assessment, incident response, cloud security for small businesses, etc.. Regularly check ENISA's website for updated reports – e.g. threat landscape summaries or sector-specific advice – all written with a focus on being actionable for smaller organizations.
- **International Standards (ISO/IEC 27001 & 27701):** ISO/IEC 27001 is the globally recognized standard for Information Security Management Systems (ISMS). Implementing it helps you systematically address security across people, processes, and IT systems. Many elements of ISO 27001 overlap with NIS2 and DORA requirements (risk assessments, access control, continuous improvement). Certification to 27001 is not mandated by law, but it provides assurance to regulators and clients that you follow "state of the art" security practices. ISO/IEC 27701 is a related standard that extends 27001 to cover Privacy Information Management – very useful for GDPR compliance, as it guides how to manage personal data securely and lawfully.
- **CIS Controls v8:** The Center for Internet Security's Controls (version 8) are a prioritized set of basic cyber hygiene practices. There are 18 controls, starting from inventorying hardware/software, to malware defense, to incident response. For an SME, CIS Controls serve as an excellent checklist of technical measures to implement. In fact, many regulatory expectations align with these controls. CIS also provides an "Implementation Group 1" which is a subset of controls tailored for small businesses – essentially the essential cyber defenses every SME should have. Following CIS Controls can help demonstrate compliance with the security objectives of laws like NIS2, as they map to required safeguards.

- **OWASP SAMM (Software Assurance Maturity Model):** If your SME is involved in software development (e.g. you create a web application or mobile app), OWASP's SAMM is a framework to improve your software security practices. It covers areas like secure design, threat modeling, secure coding, testing, and maintenance. SAMM is useful under the Cyber Resilience Act and AI Act contexts, where secure development lifecycle and addressing vulnerabilities are key. By using SAMM, you can gradually enhance how your development team incorporates security – which will be needed to meet CRA's requirement of designing products to minimize vulnerabilities. Even outside formal compliance, it reduces costly security fixes later on.
- **EU Funding and Training Programs:** The EU and national governments offer support to help SMEs improve cybersecurity. Under the Digital Europe Programme (2021–2027), significant funding is allocated to cybersecurity initiatives. SMEs can benefit indirectly through projects that offer free training, tools, or services (for instance, some EU-funded programs provide free or subsidized security assessments or innovation vouchers for SMEs). Check your local Digital Innovation Hub or cybersecurity competence center – many have SME-focused programs. Horizon Europe (the EU research and innovation program) also funds cybersecurity R&D; if you're an innovative SME with a new security solution, there are grants and consortium opportunities. Additionally, the new European Cybersecurity Competence Centre (ECCC) in Bucharest coordinates funding to build cyber capacity – keep an eye on its calls which often include SME beneficiaries. On the skills side, the Cybersecurity Skills Academy launched by the EU in 2023 aims to train more professionals – SMEs can tap into these training opportunities to upskill their staff (e.g. through online courses, workshops, or partnering with universities).
- **European and National Guides:** Beyond ENISA, bodies like Europol/EC3, national cybersecurity agencies (like ANSSI in France, BSI in Germany, NCSC in the Netherlands, etc.) publish SME guidebooks and checklists. Many are available in local languages and tailored to specific regional threats. Often, they include case studies of breaches at SMEs, common pitfalls, and "quick win" recommendations. Using these free resources can complement this guide and provide more hands-on advice (for example, how to configure a firewall or how to respond to a ransomware attack in detail).

By leveraging this toolbox – standards to benchmark your practices, controls checklists to ensure coverage, and external support to bolster your efforts – an SME can build a robust cybersecurity program that not only meets legal requirements but genuinely protects the business. Remember, compliance is the floor, not the

ceiling: aim for security best practice, and you will inherently be in good shape for compliance.

7. Glossary of Key Terms and Acronyms

To navigate legal texts and security discussions, it helps to know the lingo. Here's a glossary of 20 common terms in EU cybersecurity compliance:

- **SME:** Small and Medium-sized Enterprise. In EU definition, a company with fewer than 250 employees and ≤€50 million turnover (further split: micro <10, small <50, medium <250). Many laws use this sizing to determine exemptions or support measures.
- **CSIRT:** Computer Security Incident Response Team. A team (often national or internal to an organization) that handles cybersecurity incidents and coordinates response. NIS2 requires Member States to have CSIRTs and companies to report incidents to them.
- **ENISA:** European Union Agency for Cybersecurity (formerly "European Network and Information Security Agency"). The EU's centre of expertise for cybersecurity, based in Greece. It develops guidelines, runs exercises, and helps harmonize policies across the EU.
- **Certification Scheme:** In context of the Cybersecurity Act, a framework defining how products/services can be certified for cybersecurity. Examples: *EUCC* (Common Criteria based scheme for IT products) or upcoming cloud security scheme. Certifications can be basic, substantial, or high assurance.
- **CE Marking:** A conformity mark indicating a product meets EU requirements. Under CRA, a CE mark will also signify compliance with cybersecurity requirements. Already used in radio equipment, medical devices, toys, etc.
- **Personal Data:** Any information relating to an identified or identifiable person (data subject). Core concept in GDPR. Examples: names, emails, IP addresses, HR records, etc. Must be protected and lawfully processed.
- **Data Breach:** A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. GDPR compels notification of certain breaches to authorities and affected individuals.
- **Essential/Important Entity:** Categories under NIS2. Essential entities are generally large companies in high-criticality sectors (e.g. big energy utility); Important entities are medium-sized in those sectors or large/medium in other critical sectors. Determines oversight intensity.

- **Incident Reporting:** Legal obligation to notify authorities about significant cybersecurity incidents within a set time. Under NIS2, within 24 hours an early alert is needed; under GDPR, personal data breaches to be reported within 72 hours; DORA mandates financial firms report within hours/days depending on incident severity.
- **Risk Assessment:** A systematic process to identify threats, vulnerabilities, and potential impacts to your business assets, and to prioritize mitigation. EU laws like NIS2, DORA, and CRA explicitly require regular risk assessments.
- **Proportionality:** A regulatory principle meaning measures or penalties should be scaled to the size/capacity of an entity and the risk involved. For SMEs, this often means simplified obligations or expectations that controls are commensurate with their risk profile.
- **High-Risk AI System:** Defined by the AI Act as AI used in sensitive areas (e.g. in recruitment, credit, law enforcement, critical infrastructure) or as safety components, which faces strict oversight. These systems must comply with extensive requirements before deployment.
- **Vulnerability Disclosure:** The practice/policy of accepting reports about security flaws in your products or systems and fixing them. The CRA will require manufacturers to implement Coordinated Vulnerability Disclosure (CVD) processes, and many companies set up a contact point (or bug bounty program) to manage this.

8. Regulatory Landscape Map

Regulations in force

The EU's cybersecurity framework consists of several horizontal laws (which apply across sectors) and sector-specific regulations. The table below maps out the key instruments – from general cybersecurity directives to data protection and product-specific rules – highlighting their scope, main obligations, who oversees compliance, penalties for violations, and when they take effect.

Regulation	Scope & Coverage	Key Obligations for Entities	Supervisory Authority	Penalties
NIS Directive (2016) *Directive*	Critical services (energy, transport, banking, health, etc.) – "operators of essential services" and some digital service providers in EU. Mainly medium/large firms; transposed into national law.	Implement network and information security measures; incident detection and reporting to authorities.	National NIS competent authority (e.g. cybersecurity agency) in each Member State.	Fines set by each country (varies). NIS1 lacked a uniform EU-wide fine, but non-compliance could lead to orders and national penalties.
NIS2 Directive (2022) *Directive*	Broader range of essential and important entities across critical and other sectors. Covers medium and large organizations in sectors like energy, transport, health, finance, ICT, water, food, chemicals, digital providers, etc. (Micro and small enterprises (<50 staff, <€10M turnover) are generally exempt unless critical exceptions apply.)	Cybersecurity risk management (technical and organizational measures), incident reporting within tight timelines (e.g. 24-hour early warning, supply chain security, and board-level accountability/training. Management must approve and oversee cyber measures.	National cybersecurity authorities (sectoral regulators coordinate). Enhanced supervision for "essential" entities (proactive audits) vs. ex-post oversight for "important" entities.	Up to €10 million or 2% of global turnover (whichever higher) for essential entities; up to €7M or 1.4% turnover for important entities. Managers of essential entities can face personal liability or suspension.
GDPR – General Data Protection Regulation	Any business (of any size) processing personal data of individuals in the EU. This includes virtually all sectors if they handle customer or employee personal data. No	Protect personal data by design, obtain lawful basis for processing, be transparent with individuals, secure the data (technical and org. measures), notify data breaches	National Data Protection Authorities (independent regulators in each country). They can	Fines up to €20 million or 4% of annual global turnover (whichever is higher) for serious

(2016) *Regulation*	blanket SME exemption (though some obligations are lighter for small-scale processing).	within 72 hours, honor individuals' rights (access, deletion, etc). Appoint Data Protection Officer (DPO) if criteria met.	conduct investigations or respond to complaints across all business sectors.	infringements. Lower tier fines up to €10M or 2%. Possible orders to stop processing data.
EU Cybersecurity Act (2019) *Regulation*	Horizontal law – applies EU-wide, focusing on cybersecurity certification of ICT products/services and empowering the EU Cybersecurity Agency (ENISA). Does not impose direct requirements on all companies except if they choose to certify products or if future laws make a certification scheme mandatory.	Established voluntary EU-wide cybersecurity certification schemes for ICT products, services and processes. Reinforced ENISA's role (permanent mandate) to develop these schemes and help Member States. No general "must certify" obligation yet, but frameworks like EU Common Criteria (EUCC) and cloud security schemes exist.	European Commission and ENISA design schemes; national certification bodies issue certificates. Oversight by national market surveillance for certified products.	No direct fines on SMEs in general. Non-compliance would mainly mean loss of certification or market actions if a product falsely claims certification. (However, proposed 2024 amendments may allow mandatory certification for certain services.)
Cyber Resilience Act (2024) *Regulation*	All "products with digital elements" (hardware or software) placed on the EU market – from smart toys and IoT devices to business software. *Exemptions:* Products already regulated for cybersecurity under other EU laws (e.g. medical devices, automobiles, aviation) are largely excluded. Applies to manufacturers, importers, distributors – including SMEs producing tech products.	Mandatory cybersecurity requirements by design: Manufacturers must ensure products are built securely, provide security updates and support for a defined period, handle vulnerabilities (report and remediate), and include clear user info and instructions. Certain "critical" products require third-party conformity assessment (independent certification) before CE marking. Overall, shifts responsibility to producers to maintain product security throughout its lifecycle.	Market surveillance authorities in each Member State (similar to product safety enforcement). ENISA will coordinate a European vulnerability database.	Penalties up to €15 million or 2.5% of global turnover (whichever higher) for serious breaches (per draft texts) – final law sets tiered fines. Non-compliant products can be pulled from the market (losing CE marking).
eIDAS Regulation	Trust service providers (e.g. issuers of digital certificates, e-signatures, website authentication services) and electronic	Must meet strict security and integrity requirements for trust services (e.g. secure signature creation devices, qualified	National supervisory bodies for trust services (usually telecom or digital	Penalties determined by Member States' laws (administrative sanctions

(2014) *Regulation*	identification schemes notified by Member States. Affects providers of e-signature tools, company e-seals, time-stamping, etc., some of which are SMEs. Also sets standards for EU-wide e-ID interoperability.	certificates). Providers of "qualified" trust services must undergo audits and get supervisory body approval. eID schemes must be notified and meet assurance levels.	authorities) ensure providers comply (certification, audits). The European Commission maintains trusted lists of qualified providers.	for trust service violations). Significant incident reporting required. Withdrawal of qualified status if non-compliant.
EU Digital Identity (eIDAS2) Regulation (2024) *Regulation*	EU-wide framework for a European Digital Identity Wallet available to all EU citizens and businesses. Member States must offer a trusted digital ID app/wallet. Trust service rules from 2014 are amended and continue. Businesses that integrate or rely on these wallets (e.g. for customer logins, age verification) are indirectly impacted.	Member States must issue EU Digital Identity Wallets meeting common security standards. Private online service providers will be required to accept the EU ID for login where high-assurance identity is needed (e.g. opening a bank account, SIM registration) – meaning SMEs offering such services must accommodate the European e-ID. The regulation also updates security and certification requirements for trust services (remote identity proofing, new trust services like electronic ledgers, etc.).	National authorities for digital identity (e.g. government eID issuers) and trust service supervisors. The European Commission oversees interoperability and sets technical standards (via implementing acts.	To be set by Member States; likely administrative fines for providers refusing the EU Digital ID or failing security. (The regulation itself doesn't list specific fines, but non-compliance could result in loss of qualified status or other penalties under national provisions.)
CER Directive (2022) *Directive*	Operators of essential services in 10 critical sectors (energy, transport, banking, healthcare, drinking water, wastewater, digital infrastructure, public administration, space, food – focusing on physical and overall resilience (all hazards). Applies to medium/large entities identified as "critical" by Member States. Often the same types of organizations as NIS2 essential entities, but covering their operational continuity against any	Perform risk assessments against all relevant hazards (including cyber, but also physical threats, natural disasters, etc.); implement resilience measures (contingency plans, facility security, backup systems); notify disruptive incidents. Develop culture of resilience and designate a liaison officer. Cybersecurity is one aspect, complementing NIS2's specific cyber measures.	National competent authorities for critical infrastructure (could be civil protection, interior ministry, etc.) coordinate oversight. A European Critical Entities Resilience Group facilitates cooperation.	Penalties are set by each Member State's law (CER mandated that countries impose "effective, proportionate and dissuasive" sanctions). No uniform EU fine; can include fines or orders. Non-compliance could lead to being delisted as an

	disruptions (natural, technical, or malevolent).			operator or other national enforcement.
DORA – Digital Operational Resilience Act (2022) *Regulation*	Financial sector: banks, insurance companies, payment providers, investment firms, stock exchanges, digital finance startups, and ICT service providers critical to finance. In short, nearly all regulated financial entities in the EU, irrespective of size (with some proportional provisions for smaller entities like small pension funds). Third-party ICT providers (e.g. cloud or software firms) that service these financial entities can also fall in scope if designated as critical.	ICT risk management: firms must have robust internal controls over cyber risk (Governance, incident response, backup, encryption, etc.); Incident reporting: report major ICT incidents to regulators within tight timelines; Resilience testing: regular testing of systems (larger institutions must do advanced threat-led penetration tests every 3 years); Third-party risk: strict oversight of ICT outsourcing, with mandatory contract clauses and monitoring of critical suppliers. Senior management is accountable for approving risk frameworks.	Financial regulators (national prudential supervisors like central banks or market authorities) supervise compliance. EU-level bodies (ESMA, EBA, EIOPA) coordinate and can oversee critical third-party providers (with new powers to audit cloud providers, etc.).	Administrative fines (set by national law) for breaches – expected to be hefty, akin to other financial sanctions. DORA itself mandated that penalties be "effective, proportionate and dissuasive". Some Member States can even impose criminal penalties for severe negligence. Additionally, regulators can issue orders, require remediation, or restrict activities until issues are fixed.
Energy Network Code on Cybersecurity (2024) *Delegated Regulation*	Electricity sector operators involved in cross-border power flows – e.g. Transmission System Operators (TSOs), large Distribution System Operators, EU-wide networks (ENTSO-E, etc.). Targets entities critical to EU electricity grid stability (mostly large operators; small local utilities not directly unless they impact cross-border flows).	Sets common minimum cybersecurity requirements for the electricity sector, such as network segmentation, access controls, incident response plans; requires regular sector-specific risk assessments to identify critical digital systems and risks to cross-border power flows. Operators must implement cybersecurity plans, monitor and report incidents, and participate in coordinated emergency response.	National energy regulators or designated authorities (each Member State had to appoint one by Dec 2024) oversee compliance. Cooperation via ACER (EU Agency for Cooperation of Energy Regulators) and ENTSO-E.	Treated similarly to grid code compliance – non-compliance can lead to regulatory action by energy regulators, fines per national energy laws, or ultimately disconnection orders in extreme cases. (The Delegated Regulation calls for penalties under

		Establishes governance for updating security methodologies as threats evolve.		national regimes, similar to NIS2 style enforcement.)
Radio Equipment (RED) Delegated Act – IoT Security (2022) *Delegated Regulation*	Wireless and IoT devices sold in the EU that connect to network or communicate (e.g. smartphones, Wi-Fi toys, baby monitors, wireless alarms). All manufacturers of radio-enabled products (regardless of size) are in scope. This act updates the Radio Equipment Directive's essential requirements to include cybersecurity for these devices.	Manufacturers must design wireless products to: protect networks (no harmful interference or abuse of network resources); safeguard user data and privacy; and prevent fraud (e.g. mitigate risks of device impersonation). In practice, this means IoT gadgets need built-in security features (secure authentication, data protection, etc.) and must be tested/assessed for cyber compliance before CE marking.	National radio/telecom market surveillance authorities (often the spectrum regulators or consumer protection agencies) will enforce at product compliance checks. EU-wide coordination by the Commission.	Products failing to meet the new requirements cannot be CE marked for EU sale (legal market ban). Enforcement may include fines or mandatory recalls under national product compliance laws.
Medical Devices & IVD Regulations (2017) *Regulations*	Medical devices and in-vitro diagnostic devices placed on the EU market (ranging from pacemakers and infusion pumps to medical software and laboratory analyzers). Manufacturers (including many innovative SMEs in MedTech) and their suppliers are affected.	These regulations (MDR 2017/745 and IVDR 2017/746) include cybersecurity as part of product safety and performance. Manufacturers must manage IT security risks as part of design and risk assessment, ensuring devices are secure from unauthorized access and data breaches. Technical documentation must address cyber risks; devices should have measures to ensure confidentiality, integrity, and availability of data (esp. for software as a medical device). Post-market surveillance requires monitoring for vulnerabilities and security updates to devices in the field.	National medical device regulators / competent authorities (and Notified Bodies for higher-risk devices during conformity assessment) check that manufacturers comply. ENISA and the MDCG have issued guidance on medtech cybersecurity.	Non-compliant devices cannot be CE marked or may be pulled from market. Regulators can impose corrective actions or administrative fines under national law. Serious breaches (like failing to report incidents) can trigger large fines or even criminal liability in some states.
Automotive Cybersecurity	Vehicle manufacturers (passenger cars, trucks, buses) seeking EU type-approval for	Must implement a certified Cybersecurity Management System (CSMS) covering the	National Vehicle Type-Approval Authorities (e.g.	If a manufacturer fails to comply, type approval is

(UN R155/R156) *(2021) Regulation via Type-Approval*	new models. Also relevant to automotive suppliers providing electronic control units or software. SMEs making vehicle components or custom vehicles are indirectly involved via supply chain.	vehicle lifecycle. New car models must meet UN Regulation 155 requirements: risk assessment of cyber threats, security by design in vehicle networks, and procedures to detect and respond to cyber incidents. UN R156 mandates a Software Update Management System to ensure safe over-the-air updates. Manufacturers need to monitor for vulnerabilities and report incidents. Vehicles are tested against these cyber standards before approval.	KBA in Germany, RDW in Netherlands, etc.) enforce it by requiring proof of compliance (audit certificates) before granting type approval. The EU law (Reg 2018/858 as amended) makes UN R155/R156 compliance compulsory.	denied – meaning they cannot sell the vehicle in the EU. In-service, if cybersecurity issues emerge, regulators can demand recalls. There are also penalty provisions in Member States for non-compliance with type approval regulations (fines, loss of approval).
Aviation Cybersecurity (EU 2023/203) *Implementing Regulation*	Civil aviation organizations: airlines, airport operators, air navigation service providers, aircraft manufacturers and maintenance organizations – basically any entity required to hold an aviation safety certificate under EASA rules. (SME airlines or maintenance firms are included, with proportional implementation.)	Requires an Information Security Management System (ISMS) as part of safety management. Aviation companies must assess information security risks that could affect aviation safety (e.g. hacking of airport systems, interference with aircraft IT) and implement controls. Includes incident reporting to aviation authorities and ensuring supply chain security in operations (e.g. vetting IT service providers). Maintenance organizations (Part-145) must protect the integrity of aircraft maintenance data/systems. Essentially, cybersecurity is integrated into existing safety oversight processes.	The European Union Aviation Safety Agency (EASA) sets the rules; national aviation authorities enforce them as part of their certification and oversight of airlines, airports, etc. Compliance is checked via audits (similar to safety audits).	Enforcement via aviation safety regulation: authorities can issue findings and require corrective actions; in severe cases, they can suspend or revoke aviation certificates. Non-compliance could ground an airline or shut an airport until issues are fixed. Financial penalties depend on national laws for aviation infractions.
Maritime Cyber Rules (IMO &	Maritime sector: Ship operators (commercial shipping companies), port facility operators, and maritime authorities. Rather than an EU law, the key driver is the	Since 1 Jan 2021, maritime companies must incorporate cyber risk management into their Safety Management Systems (per IMO MSC.428(98)). This means identifying	Flag State administrations (maritime safety authorities in each country) verify that	Failure to address cyber risks can lead to ships being detained or not certified under the ISM

EU) *(2021 onward)*	International Maritime Organization (IMO) resolution which EU countries enforce on their flagged vessels. NIS2 and CER also cover ports and shipping services as critical entities.	cyber threats to ships, training crew, and having response plans as part of the ISM Code compliance. EU port operators are covered under NIS2 (cybersecurity measures, incident reporting) and CER (resilience plans) just like other critical entities. Additionally, new industry standards (IACS Unified Requirements E26/E27 effective July 2024) mandate cybersecurity in ship design for newbuild vessels – ensuring shipyards and suppliers build in cyber protections for navigation, propulsion, and control systems.	shipping companies comply with the ISM Code (including cyber risk management) during audits. Port facility security is overseen by national authorities under EU port security directives and NIS2 regulators for cyber. Classification societies implement the new IACS cyber rules for vessel certification.	Code. Under NIS2, port operators could face fines (like other essential entities) up to €7M or 1.4% turnover for important entities. Non-compliance with IACS rules means a new ship won't get class certification (so it cannot sail).
5G Security Toolbox (2020) *Policy Recommendation*	Telecom operators and 5G network suppliers in the EU. (Indirectly relevant to any enterprise using 5G for critical operations.) This is not a binding law, but a set of measures EU countries agreed on to secure 5G networks, particularly against high-risk vendors or state-sponsored threats.	Recommended measures include: conducting risk profiles of telecom suppliers, diversifying supply chains to avoid high-risk dependency, strict access controls in 5G core networks, and using certified equipment. Telecom regulators, in turn, were advised to impose these through national rules (e.g. restricting high-risk 5G vendors). For SMEs, the toolbox ensures the mobile networks they use are more secure; if an SME is a niche telecom provider, it's expected to follow these best practices.	Primarily implemented by Member States' governments and telecom authorities. The European Commission monitors progress but toolbox actions are voluntary cooperation.	No direct fines (non-legislative). However, many countries translated parts of the toolbox into regulations (e.g. requiring mobile operators to notify use of certain vendors, or giving authorities power to ban equipment). Those national measures carry penalties if violated.
AI Act (2024) *Regulation*	Providers and users of AI systems, especially those deemed *high-risk*. This landmark EU law governs AI across all sectors: from manufacturing to HR tools to	Risk-based obligations: *Prohibited AI* (like social scoring or real-time biometric ID for law enforcement) is banned outright. *High-risk AI* systems (as listed in Annex III of the	National market surveillance authorities (to be designated for AI, likely existing product safety or	Fines are tiered: up to €30 million or 6% of global turnover for the most serious violations (e.g.

	customer-facing AI services. SMEs developing or deploying AI need to check if their systems fall under risk categories. High-risk AI (e.g. AI for credit scoring, recruitment, medical devices, infrastructure control) is heavily regulated. Low-risk AI has minimal obligations.	Act) must be registered in an EU database and comply with strict requirements: robust risk assessments and mitigation, ensuring high data quality to avoid bias, transparency to users, human oversight, cybersecurity safeguards, and conformity assessment before market launch. Some AI must have built-in transparency (e.g. bots must declare they're AI, deepfakes must be labelled). Providers must monitor AI performance and report serious incidents or malfunctions.	digital authorities) will enforce, with coordination by a new European AI Office. They can order corrective actions, recall AI systems, or impose fines.	unlawful use of prohibited AI). Other breaches (e.g. not complying with transparency or data requirements) can attract fines up to 4% or 2% of turnover. These penalties even exceed GDPR in some cases, underlining the high stakes.

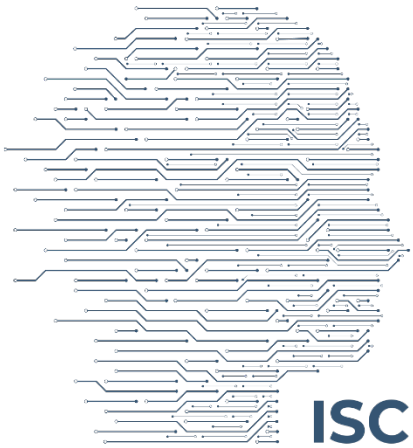
Table: Key EU cybersecurity-related laws and initiatives, with scope, SME-relevant obligations, enforcement, penalties, and timelines (as of May 2025).

Regulations in Development

In addition to the laws already in force or in application, the EU is actively shaping new legislative proposals to address emerging threats and technological developments. These upcoming instruments – such as the Cybersecurity Solidarity Act, Digital Networks Act, and EU Space Act – aim to enhance cross-border cyber crisis coordination, modernize digital infrastructure rules, and secure space-based assets and services.

Regulation	Scope & Coverage	Key Obligations for Entities	Supervisory Authority	Penalties
Cybersecurity Solidarity Act *(proposed 2023)*	EU-wide mechanisms for detecting and responding to cross-border cyber crises. Focuses on preparedness, common cyber shield infrastructure, and joint response mechanisms. Applies mainly to Member States, CSIRTs, and trusted providers.	Establishes EU Cybersecurity Reserve (trusted service providers ready to assist in emergencies); creates Cybersecurity Emergency Mechanism and promotes shared situational awareness platforms like Cyber Shield.	European Commission, ENISA, CSIRT Network	Penalties not focused on SMEs; law targets Member State coordination. Funding conditional on participation in preparedness.
Digital Networks Act *(proposal)*	Updates rules for electronic communications networks and services, including new provisions for security of 5G/6G, resilience, and potentially infrastructure sharing. Applies to telecom providers, possibly cloud and platform services.	Enhances security-by-design, reporting of outages and incidents, and could impose new obligations on Over-The-Top (OTT) providers (e.g. messaging apps). Focus on network resilience and innovation funding.	National telecom regulators, BEREC coordination	TBD – expected to include standardized penalties similar to GDPR/NIS2 structure.
EU Space Law / EU Space Act *(proposed 2024)*	Framework for space infrastructure and cybersecurity – including Galileo, Copernicus, and private space operators under EU contracts. Targets resilience, security, procurement, and governance.	Requires operators of EU-funded space assets to comply with cybersecurity standards, incident reporting, secure supply chains. May mandate cooperation with EU Space Information Sharing Centre (ISAC).	European Union Agency for the Space Programme (EUSPA), European Commission	To be determined by regulation; critical infrastructure penalties may apply.

Table: Key EU cybersecurity-related laws and initiatives, in development as per May 2025



IS Consulting

www.isconsulting.pl

contact@isconsulting.pl

ul. Żelazna 51/53

00-843 Warszawa