



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Annex B – Legal Matrix
Release Date	October 2025
Next Review	August 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.2

1. What is the Cross-Reference Matrix?

The Cross-Reference Matrix is your quick-look map between legal obligations in EU cybersecurity laws and the specific controls in the ShieldNet Cybersecurity Standard that fulfill them. It is designed to give you — and any regulator, auditor, or business partner — a clear view of which requirements are covered, where, and how. By linking each article or clause from the relevant legislation directly to the ShieldNet control IDs, the matrix eliminates guesswork and provides a defensible compliance trail.

By maintaining this mapping, you not only make your compliance posture easier to explain — you also simplify internal governance, as every team member knows which controls serve which legal purpose. It also ensures that when laws change, you can quickly identify which controls need updating, without combing through your entire security framework.

2. How to use the Matrix

The Cross-Reference Matrix works best when it is treated as an active compliance tool, not just a static reference table. Its purpose is to help you quickly identify which ShieldNet controls meet specific legal obligations — and just as importantly, where you may have gaps that need addressing.

Start with the Core Matrix to confirm that all 48 mandatory controls in the ShieldNet Core Standard are in place and aligned to their respective legal obligations. This will give you a clear view of your baseline compliance with EU-wide cybersecurity laws such as NIS2, GDPR, the Cyber Resilience Act, and the AI Act. If you are new to the standard, use the Core Matrix as your checklist — tick off controls you have implemented and highlight those needing work.

If your organization operates in a regulated sector or provides high-impact services (e.g., finance, health, energy, AI systems in high-risk categories), review the Extensive Matrix. This will show you any Sector Add-On obligations and their related controls, so you can layer them onto your baseline. Sector obligations are designed to be modular — you only need to apply the add-ons relevant to your sector.

Core Matrix – Covers the baseline obligations from horizontal EU laws such as NIS2, GDPR, the Cyber Resilience Act, and the AI Act, and maps them to the 48 mandatory Core Standard controls. This section applies to all ShieldNet members and represents the minimum compliance footprint required in the community.

Best practice for using the matrix:

- Assign responsibility for maintaining the matrix to your Info-Sec Coordinator or compliance lead.
- Review at least annually or after any regulatory changes to ensure mappings remain accurate.
- Use the matrix alongside Annex A's Legal & Compliance Mapping Table (A-7) to keep both your external (law-to-control) and internal (law-to-policy) mappings consistent.
- During audits or supplier reviews, present the matrix to clearly demonstrate how you meet each legal requirement.

When kept current and used proactively, the Cross-Reference Matrix becomes your compliance compass — showing exactly where you stand, where you're covered, and where action is needed.

3. The Core Matrix

The table below maps key legal obligations to the ShieldNet Core Controls that help fulfill them. This shows how the 48 controls cover the baseline cybersecurity requirements in each EU instrument. (Articles and recitals are paraphrased for brevity.)

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>NIS2 Directive</i>	
NIS2 – Art. 21(2)(a): Cybersecurity policies on risk analysis (implement policies and a risk management framework)	[KP2], [KP4], [KP5] – Compliance matrix, Risk assessments, Security policy
NIS2 – Art. 21(2)(b): Incident handling (establish processes for incident detection & response)	[RR1]–[RR4], [RR8] – Incident response plan, escalation, containment, recovery, documentation
NIS2 – Art. 21(2)(c): Business continuity & disaster recovery (backup management, crisis plans)	[KP6], [RR9] – Continuity plan with backups, Backup workarounds / alternate procedures
NIS2 – Art. 21(2)(d): Supply chain security (address security in supplier relationships)	[KP7], [WP10] – Vet suppliers (contracts & due diligence), Monitor third-party security
NIS2 – Art. 21(2)(e): Security in development & maintenance (incl. vulnerability handling/disclosure)	[SB6], [SB8], [WP3], [WP4], [WP7] – Secure configuration, Secure dev practices, Patch mgmt, Vuln scanning, Vulnerability disclosure channel
NIS2 – Art. 21(2)(f): Measures effectiveness assessment (test and audit cybersecurity measures)	[WP6], [LL2], [LL3], [LL5] – Security testing, Incident drills, Post-incident lessons, Independent audits
NIS2 – Art. 21(2)(g): Basic cyber hygiene and training	[SB4], [LL1] – Endpoint protection (updates, AV), Staff awareness training (incl. phishing tests)
NIS2 – Art. 21(2)(h): Cryptography use (including encryption policies)	[SB7] – Data encryption (in transit and at rest), plus key management procedures

ShieldNet Cybersecurity Standard – Annex B

NIS2 – Art. 21(2)(i): HR security, access control, asset management	[KP3], [SB1], [SB2], [WP8] – Asset inventory, Account control (least privilege), Staff vetting & revocation, Access reviews
NIS2 – Art. 21(2)(j): MFA, secure communications (including emergency comms)	[SB3], [SB7], [RR9] – Multi-factor authentication, Encrypted communications, Backup communication/work methods in crises
NIS2 – Art. 23(1): Incident notification to CSIRT (notify significant incidents without undue delay)	[RR5] – Notify regulators (24h initial notice, 72h report as needed)
NIS2 – Art. 23(2): Threat info to recipients (tell service users of significant cyber threats/remedies)	[RR6], [RR10] – Inform affected users/customers of incidents and guidance, Post-incident updates
<i>GDPR</i>	
GDPR – Art. 5(1)(f): Integrity and confidentiality (ensure appropriate security of personal data)	[SB1]–[SB7], [WP1]–[WP4] (holistic: access control, encryption, network security, etc., all maintain data confidentiality/integrity)
GDPR – Art. 24(1): Accountability for security measures (implement and adjust measures as needed)	[KP2], [LL4], [LL6] – Compliance matrix (covering GDPR), Regular policy updates, Management review of security effectiveness
GDPR – Art. 25(1): Data protection by design (embed privacy/security in design of systems)	[KP8], [SB8], [SB9] – Security by design in projects, Secure development, Data minimization in collection/storage
GDPR – Art. 28(1)&(3): Use of processors (due diligence and contractual security clauses with vendors)	[KP7] – Vet suppliers (GDPR Data Processing Agreement in place, security requirements in contracts)
GDPR – Art. 30: Records of processing activities (inventory of personal data processing)	[KP3] – Asset & data inventory (includes personal data mapping), [KP2] – compliance matrix noting if RoPA needed
GDPR – Art. 32: Security of processing (risk-based measures: pseudonymization, encryption, resilience, regular testing)	[SB7] (encryption), [SB1]–[SB6] (access control, etc.), [KP4] (risk assessment), [KP6] (backups for resilience), [WP6] & [LL2] (regular testing/drills)
GDPR – Art. 33: Personal data breach notification to authority (within 72 hours)	[RR5] – Notify regulators (DPA) of breaches with required info within 72h
GDPR – Art. 34: Personal data breach communication to individuals (if high risk)	[RR6] – Inform affected users (data subjects) without undue delay, including advice to mitigate harm
<i>Cybersecurity Act</i>	
Cybersecurity Act (EU 2019/881) – Cybersecurity certification framework (voluntary use of EU certification schemes)	[LL5] – Seek independent assurance (consider EU cert schemes or equivalent as security improves)
<i>Cyber Resilience Act</i>	
Cyber Resilience Act – Art. 10(2): Analyzing and reducing cyber risks in product design	[KP8], [SB8] – Secure development process (risk analysis for products, secure coding to reduce vulnerabilities)
Cyber Resilience Act – Annex I, Part 1 (“Essential requirements” for products: e.g. protect from unauthorized access, ensure confidentiality, integrity, availability, limit attack surfaces)	[SB1]–[SB7] – Access control, encryption, network security, MFA, etc. (covering unauthorized access, data protection, service continuity)
Cyber Resilience Act – Annex I, Part 2 (Vulnerability handling: processes for receiving	[WP7] – Vulnerability disclosure channel, [WP3] – prompt patching process, [RR5] & [RR6] – notifying ENISA/users if applicable

ShieldNet Cybersecurity Standard – Annex B

reports, issuing updates, notifying users of fixes)	
<i>Cyber Solidarity Act</i>	
Cyber Solidarity Act – Art. 7: European Cybersecurity Alert System (cooperation in sharing early warnings)	[WP5], [LL7] – Subscribe to threat alerts, Participate in information-sharing (national/EU alerts from CSIRTs, Cyber Hubs)
Digital Services Act – Art. 10: Single point of contact (for authorities’ communication)	[KP9] – Online content rules (includes establishing contact info for authorities)
Digital Services Act – Art. 14: Terms and conditions for users (include any content restrictions and policies)	[KP9] – Online content rules (clear terms of service against illegal content)
<i>Digital Services Act</i>	
Digital Services Act – Art. 16: Notice-and-action (mechanism to flag illegal content and act expeditiously)	[KP9] – Online content rules (process to remove/block reported illegal content)
Digital Services Act – Art. 17: Statement of reasons to users (inform users of content removals or service restrictions)	[RR6], [RR10] – Inform affected users (though RR covers mainly incident context, it aligns with transparent user comms)
Data Governance Act – Art. 11: Requirements for data sharing services (secure processing environment, neutrality, transparency, registry notification)	[KP7], [LL7] – Vet providers (ensure they meet security), Info sharing engagement (transparency in data sharing). <i>(If organization itself is a data intermediary, then [KP2] mapping obligations and [KP5] policies would cover implementing DGA’s security measures.)</i>
<i>Data Act</i>	
Data Act – Art. 4: User access to device data (must allow users to easily access data generated by their products)	[KP2] – Map legal requirements (if making IoT/connected products, include building data export functions to comply), [KP8] – Build security & privacy into new products (which includes planning data access features securely)
Data Act – Art. 27: Unlawful data transfer prevention (cloud providers must prevent non-EU gov’t access unless required)	[KP7] – Vet suppliers (choose providers with EU data protections), [SB7] – Encrypt data (so even if disclosed unlawfully, it’s unreadable)
<i>AI Act</i>	
Artificial Intelligence Act – Art. 9: Risk Management (for high-risk AI, implement continuous risk management system)	[KP10] – Manage AI risks (perform AI risk assessment, testing)
Artificial Intelligence Act – Art. 10: Data and data governance (ensure training data quality, etc.)	[KP10] – Manage AI risks (includes dataset checks), [SB9] – Minimize data (only use relevant training data, avoid bias)
Artificial Intelligence Act – Art. 13: Human oversight (design AI so humans can oversee and intervene)	[KP10] – Manage AI risks (ensure human-in-the-loop or other oversight measures for AI systems)
Artificial Intelligence Act – Art. 15: Accuracy, robustness, cybersecurity of AI systems (ensure high-risk AI is resilient to attacks and errors)	[SB8], [WP6] – Secure development/testing (adversarial testing of AI as part of secure dev), [LL5] – Independent audits (possibly include AI systems audit)

4. Add-on Matrix

The tables below mas key legal obligations to the ShieldNet Standard Add-ons that help fulfill them. This shows how the additional controls cover the baseline cybersecurity requirements in each sector. (Articles and recitals are paraphrased for brevity.)

4.1. Healthcare Add on

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>GDPR</i>	
GDPR – Art. 5(1)(f): Integrity and confidentiality of personal data	[KP-H1], [SB-H1–H4], [WP-H1–H3], [RR-H1–H3] – Classifying, encrypting and restricting access to patient data maintain integrity and confidentiality.
GDPR – Arts. 6–9 / Rec. 35: Lawful basis & special-category health data	[KP-H3], [KP-H6], [SB-H12] – Lawful processing of health data with technical and organizational protections.
GDPR – Art. 25: Data protection by design and default	[KP-H2], [SB-H3], [SB-H9–H12] – Risk management and secure-by-design development across systems and devices.
GDPR – Arts. 32–34: Security of processing & breach notification	[SB-H1–H4], [WP-H1–H3], [RR-H1–H3] – Technical controls, monitoring and incident response ensure protection and timely reporting.
<i>NIS2 Directive</i>	
NIS2 Directive – Art. 21(2)(a–c): Risk analysis, incident handling & continuity	[KP-H2], [RR-H1–H3] – Integrated cyber risk management and continuity of care planning.
NIS2 Directive – Art. 21(2)(d): Supply-chain security	[KP-H8], [SB-H14] – Supplier security clauses and audits for healthcare supply chains and product tracking.
NIS2 Directive – Art. 21(2)(e): Vulnerability management & maintenance	[WP-H2], [SB-H9–H11] – Regular patching and secure development cover system and device updates.
NIS2 Directive – Art. 21(2)(f–g): Testing & training	[LL-H1], [LL-H2] – Staff cybersecurity training and audits validate control effectiveness.
NIS2 Directive – Art. 21(2)(h–j): Access control & secure communications	[SB-H1], [SB-H2], [SB-H4], [SB-H5] – Strong authentication, segmentation and encryption protect EHR and device networks.
NIS2 Directive – Arts. 23–24: Incident reporting to authorities	[RR-H1], [RR-H2] – Defined reporting timelines and responsibilities to CSIRTs and regulators.
<i>Regulation (EU) 2017/745 - MDR</i>	
Regulation (EU) 2017/745 – MDR Annex I (17.2), (18.8): Device security & unauthorized access protection	[KP-H6], [SB-H5], [SB-H12] – Cyber-risk management and built-in protections against unauthorized access to medical devices.
Regulation (EU) 2017/745 – Annex II 6.3: Software verification & validation	[SB-H11] – Verification and validation testing before device release ensures safety and security.
<i>Regulation (EU) 2017/746 - IVDR</i>	
Regulation (EU) 2017/746 – IVDR Annex I (16.2), (16.4): Secure software development & network requirements	[SB-H9], [SB-H10], [LL-H4] – Secure SDLC, customer security guidelines and disclosure contacts for health software.
<i>EudraLex</i>	

ShieldNet Cybersecurity Standard – Annex B

EudraLex Vol. 4 Annex 11 §1, §6, §9–13: Computerised system controls & audit trails	[KP-H2], [WP-H3], [LL-H2], [LL-H3] – Risk management, audit-trail review and post-incident learning support GxP integrity.
EudraLex Vol. 4 Annex 11 §2: Training & qualification of personnel	[LL-H1] – Cybersecurity training for IT and clinical staff to perform duties safely.
EudraLex Vol. 4 Annex 11 §3: Third-party agreements & supplier competence	[KP-H8] – Supplier cybersecurity assurance and periodic audits embedded in contracts.
EudraLex Vol. 4 Annex 11 §10–11 & Annex 15 (Intro): Change control & validation of GxP systems	[KP-H7], [WP-H5] – Formal change-control and periodic review maintain validated state of critical systems.
<i>Directive 2011/24/EU</i>	
Directive 2011/24/EU – Art. 14(2)(a): Continuity of care & secure eHealth exchange	[RR-H3–H5], [SB-H6], [SB-H7] – Continuity and secure data exchange/telemedicine maintain trusted care delivery.
Directive 2011/24/EU – Cross-border health information systems (high trust and security)	[SB-H6], [SB-H14] – Secure interoperability and traceability systems for eHealth and medical products

4.2. Education Add on

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>GDPR</i>	
GDPR – Art. 5(1)(c),(f): Data minimization and confidentiality	[KP-E1], [SB-E1–E4], [WP-E1–E3] – Data classification, network segmentation and encryption maintain integrity and confidentiality of student data.
GDPR – Arts. 6–7 / Rec. 38: Lawful basis and parental consent for minors	[KP-E4], [KP-E7], [KP-E8] – Documented consent and clear privacy notices for children and guardians.
GDPR – Arts. 9 & 89: Special-category and research data safeguards	[KP-E6], [KP-E8] – Research data classified by sensitivity with anonymization and ethics approval controls.
GDPR – Arts. 12–15: Transparency and data-subject rights	[LL-E4], [KP-E8] – Parent communication channels and privacy notices support access and rectification rights.
GDPR – Art. 25: Data protection by design and default	[SB-E3], [SB-E8] – Secure configuration of platforms and restricted device policies embed privacy by design.
GDPR – Art. 28: Processor security & Data Processing Agreements	[WP-E3], [KP-E8], [KP-E9] – Vendor contracts with DPAs, EU hosting and tenant segregation requirements.
GDPR – Art. 30: Record of Processing Activities (ROPA)	[KP-E8] – Maintained register of child and daycare data processing activities with update log.
GDPR – Art. 32: Security of processing (risk-based measures)	[SB-E1–E6], [WP-E1–E5], [RR-E1–E3,E6] – Layered technical and organizational controls for availability, integrity and resilience.
GDPR – Arts. 33–34: Breach notification to authority and data subjects	[RR-E4], [RR-E5], [RR-E7] – 72-hour regulator notice and child/parent communication workflow.
GDPR – Art. 35: Data Protection Impact Assessment (DPIA)	[KP-E4], [KP-E8], [KP-E5] – DPIAs for AI use, children’s apps and special-category data.
GDPR – Arts. 37–39: Data Protection Officer / Privacy Lead	[KP-E3] – Appointed DPO or privacy lead with independence and direct reporting to management.
<i>NIS2 Directive</i>	
NIS2 – Art. 21(2)(a): Cybersecurity risk analysis and policy framework	[KP-E2] – Regular cyber risk assessments integrated into institutional risk management.
NIS2 – Art. 21(2)(b),(c): Incident handling and business continuity	[RR-E1–E3] – IR plan, tabletop drills and learning-continuity fallback procedures.

ShieldNet Cybersecurity Standard – Annex B

NIS2 – Art. 21(2)(d): Supply-chain security	[WP-E3], [KP-E9] – Vendor register and contractual security clauses with technical segregation.
NIS2 – Art. 21(2)(e): Vulnerability management and maintenance	[SB-E2], [WP-E2] – Patching and vulnerability scanning with tracked remediation timelines.
NIS2 – Art. 21(2)(f): Testing and effectiveness assessment	[LL-E2] – Annual audits, self-assessments and post-incident reviews.
NIS2 – Art. 21(2)(g): Basic cyber hygiene and training	[LL-E1], [SB-E6] – Staff and student training plus web/email filtering to enforce safe practice.
NIS2 – Art. 21(2)(h–j): Access control and secure communications	[SB-E1], [WP-E4], [SB-E5] – Network segmentation, MFA and secure campus access controls.
NIS2 – Arts. 23–24: Incident reporting to authorities	[RR-E4], [RR-E7] – Defined notification timelines and communication to CSIRTs or clients.
<i>AI Act</i>	
Artificial Intelligence Act – Arts. 9–15: High-risk AI requirements	[KP-E5] – AI inventory, risk management, testing, human oversight and logging for educational AI systems.
<i>Cyber Resilience Act</i>	
Cyber Resilience Act – Art. 10 & Annex I: Secure product design and updates	[SB-E2], [WP-E2], [WP-E3] – Controls ensure secure maintenance and vendor patch management for digital products used in education.
<i>Directive 2011/93/EU</i>	
Directive 2011/93/EU – Arts. 15–17: Child protection and reporting duties	[RR-E5], [SB-E7] – Child-centric IR playbooks and camera/streaming privacy controls support protective action and law-enforcement cooperation.
<i>Digital Services Act</i>	
Digital Services Act – Arts. 14–17: Platform responsibility and minor protection	[KP-E6], [SB-E3], [SB-E6] – Acceptable-Use Policy, secure LMS configuration and content filtering support safe online environments.
<i>PSD2 / PCI DSS</i>	
PSD2 / PCI DSS – Strong customer authentication and cardholder protection	[WP-E6] – Hosted PCI-DSS-compliant payment gateways and SCA reduce financial and data exposure risks.
<i>Copyright Directive 2001/29/EC</i>	
Copyright Directive 2001/29/EC (InfoSoc) – Rights management and lawful use	[SB-E9] – Watermarks, DRM and restricted sharing protect licensed courseware and exam materials.

4.3. Water & Wastewater Add on

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>GDPR</i>	
GDPR – Art. 5(1)(c),(f): Data minimization and confidentiality	[KP-E1], [SB-E1–E4], [WP-E1–E3] – Data classification, network segmentation and encryption maintain integrity and confidentiality of student data.
GDPR – Arts. 6–7 / Rec. 38: Lawful basis and parental consent for minors	[KP-E4], [KP-E7], [KP-E8] – Documented consent and clear privacy notices for children and guardians.
GDPR – Arts. 9 & 89: Special-category and research data safeguards	[KP-E6], [KP-E8] – Research data classified by sensitivity with anonymization and ethics approval controls.

ShieldNet Cybersecurity Standard – Annex B

GDPR – Arts. 12–15: Transparency and data-subject rights	[LL-E4], [KP-E8] – Parent communication channels and privacy notices support access and rectification rights.
GDPR – Art. 25: Data protection by design and default	[SB-E3], [SB-E8] – Secure configuration of platforms and restricted device policies embed privacy by design.
GDPR – Art. 28: Processor security & Data Processing Agreements	[WP-E3], [KP-E8], [KP-E9] – Vendor contracts with DPAs, EU hosting and tenant segregation requirements.
GDPR – Art. 30: Record of Processing Activities (ROPA)	[KP-E8] – Maintained register of child and daycare data processing activities with update log.
GDPR – Art. 32: Security of processing (risk-based measures)	[SB-E1–E6], [WP-E1–E5], [RR-E1–E3,E6] – Layered technical and organizational controls for availability, integrity and resilience.
GDPR – Arts. 33–34: Breach notification to authority and data subjects	[RR-E4], [RR-E5], [RR-E7] – 72-hour regulator notice and child/parent communication workflow.
GDPR – Art. 35: Data Protection Impact Assessment (DPIA)	[KP-E4], [KP-E8], [KP-E5] – DPIAs for AI use, children’s apps and special-category data.
GDPR – Arts. 37–39: Data Protection Officer / Privacy Lead	[KP-E3] – Appointed DPO or privacy lead with independence and direct reporting to management.
<i>NIS2 Directive</i>	
NIS2 – Art. 21(2)(a): Cybersecurity risk analysis and policy framework	[KP-E2] – Regular cyber risk assessments integrated into institutional risk management.
NIS2 – Art. 21(2)(b),(c): Incident handling and business continuity	[RR-E1–E3] – IR plan, tabletop drills and learning-continuity fallback procedures.
NIS2 – Art. 21(2)(d): Supply-chain security	[WP-E3], [KP-E9] – Vendor register and contractual security clauses with technical segregation.
NIS2 – Art. 21(2)(e): Vulnerability management and maintenance	[SB-E2], [WP-E2] – Patching and vulnerability scanning with tracked remediation timelines.
NIS2 – Art. 21(2)(f): Testing and effectiveness assessment	[LL-E2] – Annual audits, self-assessments and post-incident reviews.
NIS2 – Art. 21(2)(g): Basic cyber hygiene and training	[LL-E1], [SB-E6] – Staff and student training plus web/email filtering to enforce safe practice.
NIS2 – Art. 21(2)(h–j): Access control and secure communications	[SB-E1], [WP-E4], [SB-E5] – Network segmentation, MFA and secure campus access controls.
NIS2 – Arts. 23–24: Incident reporting to authorities	[RR-E4], [RR-E7] – Defined notification timelines and communication to CSIRTs or clients.
<i>AI Act</i>	
Artificial Intelligence Act – Arts. 9–15: High-risk AI requirements	[KP-E5] – AI inventory, risk management, testing, human oversight and logging for educational AI systems.
<i>Cyber Resilience Act</i>	
Cyber Resilience Act – Art. 10 & Annex I: Secure product design and updates	[SB-E2], [WP-E2], [WP-E3] – Controls ensure secure maintenance and vendor patch management for digital products used in education.
<i>Directive 2011/93/EU</i>	
Directive 2011/93/EU – Arts. 15–17: Child protection and reporting duties	[RR-E5], [SB-E7] – Child-centric IR playbooks and camera/streaming privacy controls support protective action and law-enforcement cooperation.
<i>Digital Services Act</i>	
Digital Services Act – Arts. 14–17: Platform responsibility and minor protection	[KP-E6], [SB-E3], [SB-E6] – Acceptable-Use Policy, secure LMS configuration and content filtering support safe online environments.
<i>PSD2 / PCI DSS</i>	

ShieldNet Cybersecurity Standard – Annex B

PSD2 / PCI DSS – Strong customer authentication and cardholder protection	[WP-E6] – Hosted PCI-DSS-compliant payment gateways and SCA reduce financial and data exposure risks.
<i>Copyright Directive 2001/29/EC</i>	
Copyright Directive 2001/29/EC (InfoSoc) – Rights management and lawful use	[SB-E9] – Watermarks, DRM and restricted sharing protect licensed courseware and exam materials.

4.4. District Heating & Cooling Add on

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>GDPR</i>	
GDPR – Art. 25(1) Data protection by design	[KP-HC5], [SB-HC7] – Integrations governance and metering data governance implement privacy by design in sector platforms and building automation integrations.
GDPR – Art. 25(2) Data protection by default	[SB-HC9] – Least privilege portals and APIs plus rate limiting and strong authentication support privacy by default for customer access interfaces.
GDPR – Art. 32(1)(b) Security of processing confidentiality integrity	[KP-HC5], [SB-HC7], [WP-HC4], [SB-HC9], [RR-HC6] – Controls address protection of customer and occupant related data and safeguard platform and building automation integrity.
GDPR – Art. 32(1)(c) Security of processing availability and resilience and restore	[SB-HC1], [RR-HC4] – Configuration backups and building automation restore baselines support recoverability and operational resilience.
GDPR – Art. 32(1)(d) Testing assessing evaluating effectiveness	[WP-HC2], [SB-HC7], [LL-HC4] – Centralized logs support detection and evidence while governance and metrics drive ongoing effectiveness review
<i>NIS2 Directive</i>	
NIS2 – Art. 21(2)(a): Cybersecurity risk analysis and policy framework	[KP-HC1], [KP-HC3], [LL-HC1], [KP-HC4], [KP-HC7] – Criticality mapping safety boundaries seasonal reviews and abuse scenarios operationalize risk based planning.
NIS2 – Art. 21(2)(b) Incident handling	[WP-HC1], [WP-HC2], [WP-HC3], [RR-HC2], [RR-HC3], [WP-HC6], [RR-HC6] – Detection and escalation plus platform command monitoring and safe mode strengthen handling and coordination.
NIS2 – Art. 21(2)(c) Business continuity crisis management backup and recovery	[SB-HC1], [RR-HC1], [RR-HC2], [WP-HC3], [RR-HC3], [RR-HC4], [RR-HC6], [LL-HC4] – Backups manual operation playbooks restore baselines and safe mode support continuity and recovery.
NIS2 – Art. 21(2)(d) Supply chain security	[KP-HC2], [SB-HC4] – Remote access path mapping and procurement security requirements reduce third party and supplier driven risk.
NIS2 – Art. 21(2)(e) Secure acquisition development and maintenance vulnerability management	[SB-HC3], [SB-HC4], [SB-HC6], [RR-HC4], [LL-HC3], [KP-HC7] – Segmentation procurement requirements secure commissioning restore planning and product support transparency support secure maintenance.
NIS2 – Art. 21(2)(f) Testing auditing and effectiveness assessment	[WP-HC1], [WP-HC2], [LL-HC1], [SB-HC5], [WP-HC4], [WP-HC6], [LL-HC4] – Monitoring logging anomaly checks seasonal reviews and service metrics support ongoing effectiveness evaluation.

ShieldNet Cybersecurity Standard – Annex B

NIS2 – Art. 21(2)(i) Policies and procedures on access control asset management and related governance	[KP-HC1], [KP-HC2], [KP-HC3], [SB-HC1], [SB-HC2], [SB-HC3], [WP-HC1], [SB-HC5], [KP-HC5] – Controls formalize access pathways segmentation safety boundaries and change governance.
NIS2 – Arts. 23–24: Incident reporting to authorities	[RR-E4], [RR-E7] – Defined notification timelines and communication to CSIRTs or clients.
NIS2 – Art. 21(2)(j) Use of multi factor authentication and secure communications where appropriate	[SB-HC2] – MFA and controlled remote maintenance sessions operationalize strong authentication for OT adjacent access.
<i>CER Directive</i>	
CER – Art. 12(1) Critical entity risk assessment	[KP-HC1] – Service criticality mapping supports structured risk assessment for essential service delivery.
CER – Art. 12(2) Risk assessment considering relevant risks and dependencies	[KP-HC4], [LL-HC2], [KP-HC7], [WP-HC6] – Impact tiering information sharing abuse scenarios and platform command abuse detection reflect broader resilience risk thinking.
CER – Art. 13(1)(a) Resilience measures and identification of relevant assets	[KP-HC4] – Substation and field node impact tiers support prioritized resilience measures.
CER – Art. 13(1)(b) Physical and cyber protection of facilities and systems	[SB-HC3] – Network separation and controlled gateways support protection of operational systems.
CER – Art. 13(1)(c) Measures to prevent incidents and ensure service continuity	[KP-HC3], [RR-HC1], [SB-HC5], [WP-HC3], [RR-HC3] – Safety boundaries manual operation change control anomaly monitoring and dispatch coordination support continuity.
CER – Art. 13(1)(d) Business continuity and crisis management	[RR-HC1] – Manual operation and safe degradation procedures support crisis operation for essential thermal services.
CER – Art. 13(1)(e) Supply chain security and secure access for service providers	[KP-HC2], [SB-HC2] – Remote access path mapping and hardened maintenance sessions address third party access exposure.
CER – Art. 13(1)(f) Staff awareness training exercises and information exchange	[LL-HC2] – Cross entity information sharing and lessons learned improve sector wide resilience.
CER – Art. 13(2) Review and update of resilience measures	[LL-HC1] – Seasonal readiness reviews align resilience measures with peak risk periods and ensure updates.
CER – Art. 15(1) Incident notification where required	[RR-HC2] – Defined escalation and communication paths support timely notification in disruption scenarios.
<i>Cyber Resilience Act</i>	
CRA – Art. 13(1) Product security by design and default	[SB-HC8] – Secure update and recovery mechanisms plus secure defaults for connected devices.
CRA – Art. 13(2) Cyber risk management for products	[KP-HC6], [SB-HC8] – Product risk files and secure update design implement risk based product security.
CRA – Art. 13(3) Support period and security maintenance transparency	[KP-HC6], [LL-HC3] – Risk file maintenance across support life and end of support transparency.
CRA – Art. 13(5) Security requirements in procurement and supply	[SB-HC4] – Procurement controls require support duration update methods and vulnerability handling evidence.
CRA – Art. 13(6) Vulnerability handling process	[WP-HC5] – Vulnerability intake triage and advisory process.
CRA – Art. 13(7) Vulnerability management during lifecycle	[KP-HC6], [WP-HC5] – Ongoing model level tracking triage and remediation decisions.
CRA – Art. 13(8) End of support handling	[LL-HC3] – End of support transparency and secure decommissioning guidance.
CRA – Art. 14(1) Reporting of actively exploited vulnerabilities and incidents	[WP-HC5], [RR-HC5] – Triage escalates into reporting and customer notification for exploited issues.

ShieldNet Cybersecurity Standard – Annex B

CRA – Art. 14(2) Timely notification content and process	[RR-HC5] – Templates and customer guidance support structured notification.
CRA – Art. 14(8) Follow up and communication obligations	[RR-HC5] – Confirmation tracking for high risk cases supports follow up accountability.
<i>Radio Equipment Directive</i>	
RED – Art. 3(3)(d) Network protection requirements for connected radio equipment	[RR-E5], [SB-E7] – Child-centric IR playbooks and camera/streaming privacy controls support protective action and law-enforcement cooperation.
RED – Art. 3(3)(e) Personal data privacy safeguards for connected radio equipment	[SB-HC8] – Secure by default commissioning and secure update mechanisms protect privacy and integrity of connected devices.
<i>Data Act</i>	
Data Act – Art. 4(1) User access to product and related service data	[SB-HC9] – Portal and API controls secure the access and sharing interfaces used for connected product data.
Data Act – Art. 4(5) Protection of trade secrets and security when sharing data	[SB-HC7] – Metering and occupant data governance supports controlled access and secure handling when sharing is required
Data Act – Art. 11(1) Technical protection measures for data access and sharing	[WP-HC4] – Integrity validation of sensors and meters supports trustworthy data before sharing or billing use.

4.5. E-commerce & Retail Add-on

Legal Obligation (EU Regulation / Directive & Article)	Relevant Shield Net Cybersecurity Standard Control ID(s)
<i>GDPR</i>	
GDPR – Art. 25(1) Data protection by design and by default	[KP-EC1], [KP-EC6] – Customer trust journey mapping and omni channel risk analysis support privacy by design decisions and secure defaults across sales and loyalty flows.
GDPR – Art. 28(3) Processor obligations and contractual safeguards	[KP-EC4] – Mapping third party data sharing such as fulfilment delivery returns and payment partners supports processor governance and security clauses.
GDPR – Art. 30(1) Records of processing accountability	[KP-EC1], [KP-EC4] – Documented personal data flows for orders and customer records provide the backbone for records of processing activities and accountability evidence.
GDPR – Art. 32(1): Security of processing	[SB-EC1], [SB-EC2], [SB-EC3], [SB-EC4], [SB-EC6], [RR-EC4], [LL-EC3] – Controls for account takeover prevention, secure checkout architecture, protection of value assets, hardened customer support verification, refund and return abuse controls, and anti-phishing readiness.
GDPR – Arts. 33–34 Breach notification (authority and data subjects)	[RR-EC1], [RR-EC2] – Incident playbooks and customer communication templates support timely notification decisions and consistent outreach
<i>NIS2 Directive</i>	
NIS2 – Art. 21(2)(a) Risk analysis and security policy framework	[KP-EC1], [KP-EC2], [KP-EC6] – Sector specific risk scenarios across key ecommerce journeys such as login, checkout, fulfilment, returns and loyalty operationalize risk analysis and governance
NIS2 – Art. 21(2)(b) Incident handling	[KP-EC2], [WP-EC1], [WP-EC4], [RR-EC1], [RR-EC4], [RR-EC6] – Detection thresholds and response actions for fraud and account

ShieldNet Cybersecurity Standard – Annex B

	takeover, plus containment for checkout and refunds and operational procedures for stores support resilience.
NIS2 – Art. 21(2)(c) Business continuity and crisis management	[RR-EC4], [RR-EC6], [WP-EC6] – Continuity procedures for store operations and point of sale plus controlled restoration reduce downtime and customer harm during disruptions.
NIS2 – Art. 21(2)(d) Supply chain security	[KP-EC4], [RR-EC1] – Supplier dependency mapping for payment, logistics and marketplace tooling and coordinated incident handling with partners support supply chain controls.
NIS2 – Art. 21(2)(e) Vulnerability handling and secure maintenance	[WP-EC4], [SB-EC1], [WP-EC2] – Monitoring abuse patterns and integration manipulation supports identifying exploitable weaknesses and driving remediation across process and technology.
NIS2 – Art. 21(2)(f) Testing and effectiveness assessment	[WP-EC1], [WP-EC2], [LL-EC1], [LL-EC2], [LL-EC5], [LL-EC6] – Metrics driven tuning for fraud and chargebacks, post campaign reviews, improvement backlog and vulnerability management indicators support effectiveness assessment.
NIS2 – Art. 21(2)(g) Basic cyber hygiene and training	[LL-EC3] – Customer support scripts and customer facing guidance reduce phishing, impersonation and secondary fraud after incidents.
NIS2 – Art. 21(2)(i–j) Access control and secure communications	[SB-EC4], [SB-EC1], [SB-EC2] – Strong identity verification for high risk support actions, account takeover prevention and secure checkout architecture strengthen access control and secure operations.
NIS2 – Arts. 23–24 Incident reporting	[RR-EC1], [RR-EC2], [RR-EC6] – Reporting ready workflows and controlled customer communications support notification obligations and coordinated response.
<i>Digital Services Act</i>	
DSA – Art. 9(1) Orders from authorities	[KP-EC3], [RR-EC3], [RR-EC5] – Stop sale and delist playbooks, handling authority orders and evidence retention for marketplace enforcement actions.
DSA – Art. 16(6) Notice and action mechanism requirements	[KP-EC3] – Defined roles and procedures to act on notices and remove or disable illegal offers efficiently, including marketplace contexts.
DSA – Art. 30(1)(2)(5) Trader traceability	[KP-EC5] – Seller identification and verification file, retention controls and operational traceability requirements for marketplaces.
DSA – Art. 23(1) Statements of reasons	[WP-EC5], [RR-EC5] – Documented enforcement actions such as warnings and suspensions and decision traceability support transparency obligations.
<i>General Product Safety Regulation</i>	
GPSR – Art. 22 Platform duties	[KP-EC3], [RR-EC3], [WP-EC3], [SB-EC5] – Monitoring safety alerts, stop sale and delisting, buyer notifications and required safety information in listings.
<i>PSD2 RTS – Delegated Regulation</i>	
PSD2 RTS –Security controls	[KP-EC2], [WP-EC1], [WP-EC2], [WP-EC6], [SB-EC2] – Fraud and anomaly monitoring, secure checkout architecture and iterative tuning based on fraud and chargeback levels.
<i>Cyber Resilience Act</i>	
CRA – Vulnerability handling and communications (products with digital elements where applicable)	[KP-EC7], [WP-EC7], [RR-EC7], [SB-EC7], [LL-EC6], [WP-EC3] – Vulnerability intake, triage and tracking, disclosure contact, secure update handling and user notification for exploited or high impact vulnerabilities.

5. Reference Links

Document	Official link
GDPR Regulation EU 2016/679	https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
NIS2 Directive EU 2022/2555	https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
Cybersecurity Act Regulation EU 2019/881	https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
Cyber Resilience Act Regulation EU 2024/2847	https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
Cyber Solidarity Act Regulation EU 2025/38	https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng
Digital Services Act Regulation EU 2022/2065	https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
Data Governance Act Regulation EU 2022/868	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868
Data Act Regulation EU 2023/2854	https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
Artificial Intelligence Act Regulation EU 2024/1689	https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
General Product Safety Regulation EU 2023/988	https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng
CER Directive EU 2022/2557	https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
Radio Equipment Directive 2014/53/EU	https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng
PSD2 Directive EU 2015/2366	https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
PSD2 RTS Commission Delegated Regulation EU 2018/389	https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/eng
Medical Devices Regulation MDR EU 2017/745	https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng
In Vitro Diagnostic Regulation IVDR EU 2017/746	https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng
Directive 2011/24/EU patients rights in cross-border healthcare	https://eur-lex.europa.eu/eli/dir/2011/24/oj/eng
Directive 2011/93/EU child sexual abuse and exploitation	https://eur-lex.europa.eu/eli/dir/2011/93/oj/eng
Directive 2001/29/EC copyright in the information society	https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
EudraLex Volume 4 EU GMP Guidelines landing page	https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en
PCI DSS Payment Card Industry Data Security Standard	https://www.pcisecuritystandards.org/standards/pci-dss/
PCI SSC Document Library	https://www.pcisecuritystandards.org/document_library/

6. Version History

Version	Change
1.0	Initial document
1.1	Added Healthcare Add-on and Education Add-on matrix
1.2	Added Water & Wastewater Add-on, District Heating & Cooling Add-on and E-commerce & Retail Add-on matrix. Added section 5. Reference Links