EUROPEAN UNION

NIS2 DIRECTIVE

(Directive EU 2022/2555)

Measures for a High Common Level of Cybersecurity across the Union

English Summary for CISOs and Compliance Leads

Document Reference

Field	Value
Official Name	Directive (EU) 2022/2555
Adoption Date	14 December 2022
Publication Date	27 December 2022 (OJ L 333/80)
Entry into Force	16 January 2023
National Transposition Deadline	17 October 2024
Repealed Instrument	Directive (EU) 2016/1148 (NIS1)

> This document is an unofficial summary of the EU NIS2 Directive of 14 December 2022; it is not an authoritative translation. For binding interpretation, consult the official text at OJ L 333/80, 27.12.2022.

Table of Contents

1. Executive Summary

The **NIS2 Directive** (Directive EU 2022/2555), adopted by the European Parliament and Council on 14 December 2022, is the EU's general cybersecurity baseline directive. It repeals and replaces the earlier NIS1 Directive 2016/1148 with effect from 18 October 2024.

Reviews concluded that while NIS1 contributed to raising the level of cyber resilience across the Union, it proved insufficient to address today's and tomorrow's cybersecurity threats. NIS2 substantially expands scope, introduces uniform criteria, strengthens risk management and incident reporting obligations, and provides for more deterrent enforcement provisions.

The Five Pillars of the Directive

1. **Expanded scope**: more sectors and companies brought under regulation.
2. **Tightened risk management**: 10 minimum technical and organisational measures made mandatory under Article 21.
3. **Rapid and phased incident reporting**: 24-hour early warning, 72-hour incident notification, 1-month final report.
4. **Management body responsibility**: senior management can be held personally liable.
5. **Deterrent penalties**: administrative fines up to 2% of annual global turnover or EUR 10 million.

2. Purpose and Legal Basis

The legal basis of the directive is **Article 114 of the Treaty on the Functioning of the European Union (TFEU)**, which permits measures for the approximation of national rules in order to establish and ensure the functioning of the internal market.

The directive's principal objectives are:

- Eliminate large divergences among Member States and establish common minimum cybersecurity rules;
- Establish effective mechanisms for cross-border cooperation and information sharing;
- Update the list of sectors and activities subject to cybersecurity obligations to reflect today's threat landscape;
- Provide enforcement and remedy mechanisms ensuring effective implementation of obligations;
- Strengthen the cyber resilience capacities of critical infrastructure operators and digital service providers.

The directive applies without prejudice to and in compliance with EU law on the protection of personal data (GDPR, Regulation EU 2016/679) and electronic communications privacy (Directive 2002/58/EC).

3. From NIS1 to NIS2: Why a New Regulation?

NIS1, which entered into force in 2016, was the EU's first horizontal cybersecurity regulation. The review process revealed serious differences in implementation among Member States, with scope determination largely left to Member State discretion, fragmenting the internal market in the process.

Identified Shortcomings of NIS1

Issue Area	NIS1 Situation	NIS2 Solution
Scope determination	Left to Member State discretion; significant variation in practice.	Uniform 'size cap' rule across the EU (medium and large enterprises).
Sector list	Limited number of sectors; significant portion of digital economy excluded.	Much wider sectoral coverage; digital infrastructure, public administration, space etc. included.
Incident reporting	Single-stage; deadlines and content varied between Member States.	Multi-phase reporting: 24h early warning + 72h notification + 1-month final report.
Risk management	General language; specific minimum measures unclear.	Article 21 lists 10 mandatory minimum measure categories.
Penalties	Implemented at very different levels across Member States.	EU-wide harmonised maximum fines (EUR 10M / 2% of turnover).
Senior management responsibility	Not clear.	Management body personally liable for compliance; mandatory training.

NIS2 is not an update to NIS1; it is a replacement designed to produce a **single harmonised and enforceable cybersecurity framework** across the Union.

4. Scope and Excluded Areas

The directive primarily covers entities operating in **Annex I (high-criticality)** or **Annex II (other critical)** sectors within the EU and meeting the definition of at least medium-sized enterprise. Per Article 2 of the Annex to Commission Recommendation 2003/361/EC, a medium-sized enterprise is one with fewer than 250 employees and annual turnover not exceeding EUR 50 million (or balance-sheet total not exceeding EUR 43 million). NIS2 catches entities at or above the medium-sized threshold: the practical floor for in-scope entities is 50 employees or EUR 10 million turnover (the upper limit of "small enterprise" under the same Recommendation).

Entities Covered Regardless of Size

- Public electronic communications network providers and publicly available electronic communications service providers;
- Trust service providers (under eIDAS Regulation EU 910/2014);
- Top-level domain (TLD) name registries and DNS service providers;
- Entities that are the sole provider of a service in a Member State or where service disruption could significantly impact public security, health, or safety;
- All central public administration entities (defined nationally by Member States).

Areas Excluded from Scope

Public entities whose activities are predominantly carried out in the areas of **national security, public security, defence or law enforcement** (prevention, investigation, detection and prosecution of criminal offences) are excluded from the scope of the directive. Member States' diplomatic and consular representations in third countries and trust services used in closed systems are also excluded.

5. Key Definitions

Some basic concepts must be clearly understood for proper interpretation of the directive.

Term	Definition
Network and information system	Electronic communications networks, any device or group of devices that processes digital data, and all digital data processed for the operation, use, protection and maintenance thereof.
Cybersecurity	All activities necessary to protect network and information systems, users and other persons from cyber threats.
Incident	An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems.
Significant incident	An incident that has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.
Cyber threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems.
Significant cyber threat	A cyber threat that, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity, on its users, or on other persons by causing considerable material or non-material damage.
Vulnerability	A weakness, susceptibility or flaw of ICT products or services that can be exploited by a cyber threat.
Near miss	An event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising.
CSIRT	Computer Security Incident Response Team, the technical team responsible for incident handling.
ENISA	European Union Agency for Cybersecurity, plays a central advisory and support role in the implementation of the directive.

6. Entity Categories: Essential and Important Entities

The directive divides all in-scope entities into two main categories. This distinction determines how obligations and the supervision/enforcement regime apply.

Criterion	Essential Entities	Important Entities
Sector	Annex I, High-criticality sectors	Annex II, Other critical sectors (and medium-sized in Annex I)
Size	Large enterprises (250+ employees or 50+ million EUR turnover)	Medium-sized enterprises (50 to 249 employees)
Supervision regime	Both ex-ante and ex-post supervision	Only ex-post on evidence or complaint
Maximum administrative fine	EUR 10 million or 2% of global annual turnover (whichever is higher)	EUR 7 million or 1.4% of global annual turnover (whichever is higher)
Senior management sanctions	Temporary management ban may be applied	Temporary management ban does not apply

Important note: If an entity was identified as an 'operator of essential services' under NIS1, the Member State may decide that this entity is directly an essential entity under NIS2. Additionally, all entities identified as 'critical entities' under Directive 2022/2557 (CER) are automatically considered essential entities under NIS2.

7. Sectors in Scope (Annex I and Annex II)

Annex I, High-criticality Sectors

Large enterprises in these sectors are essential entities; medium-sized are important entities.

Sector	Sub-sector / Entity Type
Energy	Electricity (generation, transmission, distribution, supply); District heating/cooling; Oil (pipeline, production, storage, transmission); Natural gas; Hydrogen production, storage and transmission
Transport	Air (airlines, airports, ATC); Rail (infrastructure managers, rail operators); Water (maritime/inland water operators); Road (intelligent transport systems, road operators)
Banking	Credit institutions under Regulation (EU) 575/2013
Financial market infrastructures	Trading venues (exchanges) and central counterparties (CCP)
Health	Healthcare providers; EU reference laboratories; Entities conducting R&D of medicinal products; Pharmaceutical manufacturers; Manufacturers of medical devices considered critical during public health emergencies (per Regulation (EU) 2022/123)
Drinking water	Suppliers and distributors of water for human consumption
Wastewater	Entities collecting, disposing of, or treating urban wastewater, domestic wastewater, or industrial wastewater
Digital infrastructure	Internet exchange points (IXP); DNS service providers (excluding root DNS); TLD name registries; Cloud computing service providers; Data centre service providers; Content delivery network (CDN) providers; Trust service providers; Public electronic communications network/service providers
ICT service management (B2B)	Managed service providers (MSP); Managed security service providers (MSSP)
Public administration	Central and regional government entities as defined by Member States
Space	Operators of ground-based infrastructure operated by Member State or private sector

Annex II, Other Critical Sectors

Sector	Sub-sector / Entity Type
Postal and courier	Postal service providers (including courier services)
Waste management	Entities providing waste collection, recycling and disposal services
Chemicals	Entities engaged in production, processing and distribution of chemicals
Food	Large enterprises engaged in production, processing, and wholesale distribution of food
Manufacturing	Medical devices/in-vitro medical devices; Computer, electronic and optical products; Electrical equipment; Machinery and equipment n.e.c.; Motor vehicles, trailers and semi-trailers; Other transport equipment manufacturing
Digital providers	Online marketplaces; Online search engines; Social networking services platforms
Research	Research organisations conducting research with commercial intent

8. Member State Obligations

The directive places obligations on Member States as well as on private-sector entities. Each Member State must take the following steps:

National cybersecurity strategy. Adopt a national cybersecurity strategy with clear strategic objectives, priorities, and a governance framework. The strategy addresses topics such as supply chain security, ransomware, SME support, open source, and active cyber defence.

Competent authority(ies). Designate or establish one or more competent authorities to ensure implementation and supervision of the directive.

Single Point of Contact (SPOC). Designate a single point of contact responsible for cross-border coordination at EU level.

CSIRT. Establish or designate one or more CSIRTs responsible for incident handling, proactive monitoring, coordinated vulnerability disclosure, and national/international cooperation.

Entity list. Maintain, regularly update, and transmit to the Commission a list of essential and important entities and entities providing domain name registration services.

Coordinated vulnerability disclosure. Designate a CSIRT as coordinator; promote legal clarity for vulnerability researchers.

Mutual assistance. Provide mutual assistance to other Member States in cross-border supervision and enforcement.

SME support. Provide guidance, free tools, and a national/regional point of contact for small and micro enterprises.

9. Cybersecurity Risk Management Measures (Article 21)

The most important technical provision of the directive is Article 21. It lists the minimum technical, operational, and organisational measures that essential and important entities must implement. The approach is based on an **'all-hazards' perspective**; not only cyber attacks but also threats such as physical damage, natural disasters, equipment failure, and human error are covered.

Article 21, Ten Minimum Measures

#	Measure	Description
1	Risk analysis and information system security policies	Analysis of all risks and written preparation of general information security policies.
2	Incident handling	Processes for prevention, detection, response, and recovery of incidents.
3	Business continuity	Backup management, disaster recovery, and crisis management.
4	Supply chain security	Including suppliers' security practices; cybersecurity provisions in contracts with direct suppliers.
5	Security in network and information system acquisition, development and maintenance	Security throughout the lifecycle, including vulnerability handling and disclosure.
6	Assessment of effectiveness of measures	Regular assessment of the effectiveness of risk management measures.
7	Basic cyber hygiene practices and security training	Cyber hygiene practices and awareness training for staff.
8	Cryptography and encryption	Policies on the use of encryption; end-to-end encryption where appropriate.
9	Human resources security, access control, and asset management	Personnel security checks, authorisation, and asset inventory.
10	Multi-factor authentication and secure communications	MFA where appropriate, continuous authentication, secure voice/video/text communications, and secure communications systems in emergencies.

These measures are applied based on the **principle of proportionality**, taking into account the entity's risk exposure, size, sectoral importance, and potential impact of incidents.

10. Incident Reporting Obligations (Article 23)

The most critical operational innovation of the directive is the multi-stage incident reporting regime. Essential or important entities must report **significant incidents**, defined as those causing severe operational disruption, financial loss, or substantial impact on other persons, to the CSIRT or competent authority within the following timeframes.

Stage	Deadline	Content
Early warning	Within 24 hours of becoming aware of the incident	Suspicion that the incident is caused by unlawful/malicious action; possibility of cross-border impact; basic information enabling CSIRT awareness.
Incident notification	Within 72 hours of becoming aware of the incident	Update to the early warning; severity, impact, and where available indicators of compromise (IoCs).
Intermediate/final report	No later than 1 month after the incident notification	Detailed description of the incident, its severity and impact; type of threat exploited; mitigation measures taken and planned; cross-border impact if any.
Progress report	If the incident is still ongoing when the final report is due	Progress report on the current status of the incident; final report 1 month after the completion of the handling of the incident.

Notification to service recipients: When a significant cyber threat is likely to occur, entities must without undue delay and free of charge notify their service recipients of possible mitigation measures and, where appropriate, the threat itself in clear and understandable language.

Near Misses and Voluntary Reporting

In addition to incidents, entities **may voluntarily report near misses and significant cyber threats** to the CSIRT or competent authority. Entities not in scope of the directive may also voluntarily report. Voluntary reporting does not impose additional obligations on the reporter.

> **Practical impact:** The 24-hour early warning forces entities to have a cyber incident response plan and communication flow ready to be activated immediately upon incident detection. Meeting this deadline through manual and fragmented processes is extremely difficult.

11. Supply Chain Security

Most major cyber attacks in recent years reached their target organisations through suppliers and software providers, not through direct attack on the organisation itself. The directive therefore puts supply chain risk at the centre of risk-management obligations.

- Entities must assess the **quality, security practices, and secure development processes** of their suppliers' and service providers' products/services.
- **Cybersecurity requirements must be included in contracts** with direct suppliers.
- Special diligence must be exercised when selecting **managed security service providers (MSSP)**; these providers are high-value targets for attackers.
- The Cooperation Group, together with the Commission and ENISA, conducts **coordinated security risk assessments** for critical supply chains (as was done for 5G networks).
- **Non-technical risk factors** are also within scope of assessment, including the potential undue influence of third countries over suppliers, hidden vulnerabilities/backdoors, and provider dependency.

12. Management Body Responsibility

The directive ensures that cybersecurity moves out of being a topic confined to technical departments and into the **direct responsibility area of senior management**. Per Article 20, the management bodies of essential and important entities:

- Are responsible for **approving the risk management measures** under Article 21 and overseeing their implementation;
- Can be **held personally liable** for breaches of these obligations;
- Must regularly receive cybersecurity training to gain sufficient knowledge and skills;
- Should encourage similar training for their staff.

> **Important:** In essential entities, the competent authority may request that **temporary management bans** be applied to senior management (those at CEO or legal representative level). This is a measure of last resort, applicable only after all other enforcement options have been exhausted.

13. EU-level Cooperation Structures

The directive regulates or strengthens various structures that ensure effective cooperation among Member States:

Structure	Function
Cooperation Group	Supports cooperation at strategic level; prepares biennial work programmes; publishes guidance documents; conducts coordinated risk assessments for critical supply chains.
CSIRTs Network	Operational-level cooperation; incident information sharing; mutual assistance; joint response.
EU-CyCLONe	European cyber crisis liaison organisation network; bridges technical and political levels in large-scale incidents and crises; prepares impact analyses.
ENISA	Establishes and maintains the European vulnerability database; provides technical support; develops guidance; monitors Member State cyber hygiene policies.
IPCR Arrangements	EU Integrated Political Crisis Response arrangements (Council Implementing Decision 2018/1993), Union-level crisis management for large-scale crises.
EU-CSIRTs CVD Coordinator	A CSIRT in each Member State is designated coordinator to manage cross-border coordinated vulnerability disclosure.

Cooperation with third countries: The EU may conclude international agreements with third countries or international organisations under TFEU Article 218. Such agreements may, while safeguarding the Union's interests and data protection, allow such parties to participate in activities of the Cooperation Group, the CSIRTs Network, or EU-CyCLONe.

14. Supervision and Enforcement

The directive provides different supervision regimes for the two entity categories. **Essential entities** are subject to both ex-ante and ex-post supervision, while **important entities** are supervised only ex-post, on evidence or complaint.

Supervisory Powers of Competent Authorities

- Carry out on-site inspections and remote supervision;
- Request targeted security audits (with the entity potentially bearing costs);
- Order security scans;
- Request documentation of compliance with risk management measures;
- Request information about acts suspected of breaching the directive;
- Request information requiring access to personal data and traffic data where necessary.

Applicable Enforcement Measures

- Issue warnings and binding instructions;
- Order specific measures or remediation of vulnerabilities to be implemented within a specified period;
- Order an independent audit to verify risk management measures;
- Order entities to inform service recipients about the nature of the breach;
- Make public statements (disclosing the entity's name and the nature of the breach);
- For essential entities (last resort): Temporary suspension of certifications or authorisations and temporary management bans on senior management;
- Impose or seek the imposition of administrative fines.

15. Administrative Fines

The directive sets **EU-wide harmonised maximum thresholds** for administrative fines applied by Member States. These thresholds are pegged to the entity's global turnover, similar to GDPR.

Entity Type	Maximum Amount (whichever is higher applies)
Essential entities	EUR 10,000,000 or 2% of global annual turnover
Important entities	EUR 7,000,000 or 1.4% of global annual turnover

Factors in Determining Fines

- Nature, gravity, and duration of the infringement;
- Material or non-material damage caused;
- Whether the infringement was intentional or negligent;
- Measures taken to prevent or mitigate damage;
- Degree of responsibility and previous infringements;
- Degree of cooperation with the competent authority;
- Other aggravating or mitigating factors.

Fines must be **proportionate**, and fundamental rights such as the right of defence, presumption of innocence, and right to effective remedy must be observed in their application. Member States may also provide for criminal sanctions for infringements of national law; however, no person may be punished twice for the same act in violation of the **ne bis in idem** principle.

16. Implementation Timeline and Transition

Date	Event
14 December 2022	Adoption of the directive by the European Parliament and Council
27 December 2022	Publication in the Official Journal of the EU (OJ L 333/80)
16 January 2023	Entry into force of the directive (20 days after publication)
17 October 2024	Deadline for Member States to transpose the directive into national law
18 October 2024	Application of the directive begins
18 October 2024	Repeal of Directive (EU) 2016/1148 (NIS1)
17 April 2025	Deadline for Member States to transmit the list of essential and important entities to the Commission
17 October 2027 onwards	Periodic review of the implementation of the directive by the Commission (every 36 months)

Important: NIS2 is a directive; it does not apply directly. Each Member State must transpose the directive into its own national law. Therefore, the precise obligations and penalties applicable to an entity depend on the national transposition act adopted by the Member State in which it operates.

17. Implications for Non-EU Businesses

Although NIS2 is an EU directive, it has substantial implications for non-EU businesses, particularly those serving the EU market or supplying EU-based critical entities:

Directly Affected Non-EU Businesses

- Non-EU **DNS providers, cloud service providers, data centre operators, CDN providers, managed service and managed security service providers, online marketplaces, search engines, and social networking platforms** offering services in the EU must appoint an EU representative and comply with directive obligations;
- Non-EU companies with EU subsidiaries or branches may be subject to the directive through these units;
- Non-EU suppliers providing products/services to EU essential or important entities will be subject to **supply chain security contractual requirements** imposed by their customers (Article 21(2)(d));
- Non-EU MSPs/MSSPs serving EU digital infrastructure or financial entities may fall directly within scope.

Indirect Effects

- Supply chain risk assessments by EU customers force non-EU suppliers to raise their cybersecurity standards;
- Standards introduced by the directive (ISO/IEC 27001, ENISA guidance, etc.) are becoming **de facto reference points** in the global market;
- Non-EU jurisdictions are increasingly using NIS2 as a reference when developing their own cybersecurity legislation.

18. Practical Compliance Roadmap (10 Steps)

The following 10-step roadmap serves as a practical guide for both businesses operating within the EU and those wishing to voluntarily align with NIS2 standards.

Step	Activity
1. Scope determination	Determine whether the company falls within Annex I or Annex II sectors, meets the size criteria, and identify its category (essential/important).
2. Gap analysis	Evaluate the existing information security management system against the 10 measure categories of Article 21; map gaps.
3. Governance structure	Establish responsibilities, reporting lines, and approval processes at board / senior management level; set up regular training programme.
4. Policy and documentation	Prepare or update information security policy, risk management policy, incident response policy, acceptable use policy, and other documents.
5. Risk assessment	Conduct asset inventory, threat analysis, and risk assessment with all-hazards approach; establish risk acceptance criteria.
6. Implementation of technical controls	Implement MFA, encryption, network segmentation, zero-trust architecture, log management, SIEM, EDR/XDR, backup, and disaster recovery solutions.
7. Incident response capability	Document incident response plan; assign roles/responsibilities; establish 24-hour early warning communication flow; conduct tabletop exercises.
8. Supply chain management	Inventory suppliers; classify them by risk level; add cybersecurity provisions to contract templates; conduct periodic audits.
9. Training and awareness	Run annual cyber hygiene training for all staff; provide specialised training for the management body; conduct phishing simulations.
10. Continuous improvement	Conduct internal and external audits; track KPIs; learn from each incident; update the risk assessment annually; pursue certification (ISO/IEC 27001, EU cybersecurity certification).

19. Conclusion and Assessment

The NIS2 Directive substantially raises the European Union's cybersecurity baseline. It does not just impose technical requirements; it also makes cybersecurity an **integral part of companies' governance structure and business operations**.

Strengths of the Directive

- **Wide reach**: approximately 18 sectors and over 100,000 entities in scope across the EU-27;
- **Harmonisation**: Level playing field in the internal market through uniform criteria and enforcement regime across the EU;
- **Governance focus**: By making senior management accountable, ensures cybersecurity permeates all layers of the company;
- **Supply chain emphasis**: Responds to the reality that the majority of modern attacks come through the supply chain;
- **Cooperation structures**: Multi-layered EU-level coordination through the Cooperation Group, CSIRTs Network, and EU-CyCLONe.

Criticisms and Challenges

- Delays and divergences in Member State transposition; in practice, uniform implementation across the EU-27 is patchy;
- Particularly for medium-sized enterprises, compliance cost and closing the technical capability gap pose a serious challenge;
- Implementation of the 24-hour early warning deadline before sufficient maturity is achieved may lead to shallow or erroneous reporting flows;
- Overlap areas with sectoral regulations (DORA, finance; eIDAS, trust services; sectoral aviation regulations etc.) may create complexity for entities.

Overall Assessment

NIS2 reframes cybersecurity from a technical concern into a matter of **business continuity, corporate governance, and customer trust**. For entities operating in or interacting with the EU, compliance is both a legal obligation and a means to strengthen operational resilience.

For non-EU businesses, NIS2 is establishing a new **de facto standard** for access to the EU market and raising cybersecurity expectations globally. Early compliance facilitates meeting contractual obligations and improves overall cyber resilience.

> **Final note:** This document summarises the directive's main provisions for English-speaking readers. For compliance requirements specific to your organisation, review the official text (OJ L 333/80, 27.12.2022), the national transposition act of your Member State, and sector-specific regulations; engage legal and cybersecurity counsel where appropriate.

Sources

- Directive (EU) 2022/2555, EUR-Lex CELEX number 32022L2555
- Official Journal of the EU L 333/80, 27 December 2022
- ENISA, European Union Agency for Cybersecurity (www.enisa.europa.eu)
- European Commission Digital Strategy portal (digital-strategy.ec.europa.eu)

More on NIS2 from Rediacc

This summary maps the directive's structure and obligations. The companion guides on rediacc.com translate those obligations into concrete operational and procurement decisions.

Three companion guides

- **Article 21(2)(d) and self-hosting.** Why the third-party-ICT register shrinks when the data plane never leaves your tenancy. For CISOs and procurement leads renegotiating DPAs in 2026.
- **Continuous effectiveness without theatre.** Article 21(2)(e), (f), and 23 read together. The constant-time fork that makes weekly drills realistic, and the Article 23 reporting timeline you cannot meet without forensic-grade artefacts. For SRE and ops leads.
- **The structural cost of NIS2 compliance.** The five-tool stack mid-market essential entities are quietly assembling, what a self-hosted control plane collapses, and the line items that stay yours either way. For CFOs and buyers heading into a renewal cycle.

Where to find them

All three guides, together with this summary as a downloadable PDF, are at:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ is an Estonian-registered self-hosted infrastructure platform (Registry code 17363830, VAT EE102920091). The product is not a substitute for a security programme; it is a tooling layer that removes the data-plane vendor risk traditional backup, DR, and test-data tools cannot remove. Free Community tier and paid tiers from $349/month.

> This document and its companion guides are educational material. Compliance decisions specific to your organisation require legal counsel and reference to the national transposition act in your jurisdiction.