Mapovanie kontrol KubePlatform na 4 EÚ regulácie

Verzia: 1.0 · **Vydané:** 2026-05-18 · **Pre interné použitie a audítorov / klientov.**

Tento dokument mapuje 58 technických kontrol KubePlatform Compliance Monitoring na konkrétne články 4 EÚ regulácií: **NIS2** (smernica EÚ 2022/2555), **DORA** (nariadenie EÚ 2022/2554), **EU AI Act** (nariadenie EÚ 2024/1689) a **GDPR** (nariadenie EÚ 2016/679). Slúži ako podkladový materiál pre interný compliance review, externý audit alebo regulačnú self-assessment.

> **Legenda:** `NIS2 čl. X` — článok smernice NIS2 · `DORA čl. X` — článok nariadenia DORA · `AI Act čl. X · Annex Y` — článok / príloha AI Actu · `GDPR čl. X` — článok GDPR. Niektoré kontroly pokrývajú viacero regulácií súčasne (cross-cutting).

Rozsah pôsobnosti regulácií (komu sa týkajú)

NIS2 (2022/2555)

Účinné: transpozícia do SR práva do okt 2026.

Komu: prevádzkovatelia kritickej + esenciálnej infraštruktúry (energetika, doprava, voda, zdravotníctvo, IT) + cloudové služby s ≥50 zamestnancami alebo obratom ≥10M€.

Pokuta: až 10M€ alebo 2% celosvetového obratu.

DORA (2022/2554)

Účinné: 17.1.2025.

Komu: finančné inštitúcie + ich ICT third-party providers. Banky, poisťovne, fintech, dodávatelia ICT pre finančný sektor.

Pokuta: až 10M€ alebo 5% obratu (závisí od entity).

AI ACT (2024/1689)

Účinné: 2.8.2026 (čl. 6/Annex III high-risk; možné odklad do dec 2027).

Komu: každý prevádzkovateľ AI systému na EÚ trhu — bez ohľadu na sídlo.

Pokuta: až 35M€ alebo 7% obratu pre PROHIBITED prax, 15M€/3% pre HIGH-RISK.

GDPR (2016/679)

Účinné: od 25.5.2018.

Komu: každý kto spracúva osobné údaje EÚ občanov.

Pokuta: až 20M€ alebo 4% celosvetového obratu.

Mapovanie 58 kontrol → články regulácií

A. TLS / CERTIFIKÁTY (8 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
TLS verzia (1.2/1.3)	TLS	`NIS2 čl. 21(2)(g)` kryptografia · `DORA čl. 9(2)` šifrovanie · `GDPR čl. 32(1)(a)` bezpečnosť
TLS 1.0/1.1 rejection	TLS	`NIS2 čl. 21(2)(g)` · `DORA čl. 9(2)` · BSI TR-02102-2
Certifikát validity ≥ 30d	TLS	`NIS2 čl. 21(2)(c)` incident prevention · `DORA čl. 9(3)`
HSTS preload	TLS	`NIS2 čl. 21(2)(g)` · `GDPR čl. 32(1)`
HSTS rigor (max-age ≥ 1 rok)	TLS	`NIS2 čl. 21(2)(g)` · BSI Grundschutz

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
SSL/TLS handshake	TLS	NIS2 čl. 21(2)(g) · DORA čl. 9(2)
OCSP stapling	TLS	NIS2 čl. 21(2)(c) resilience · ETSI TS 119 612
Kryptografické šifry (cipher suites)	TLS	NIS2 čl. 21(2)(g) · BSI TR-02102-2

B. E-MAIL BEZPEČNOSŤ (12 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
DMARC policy (reject/ quarantine/none)	Email	NIS2 čl. 21(2)(h) phishing prevention · DORA čl. 9(4)(c)
DMARC qualifier strictness	Email	NIS2 čl. 21(2)(h) · RFC 7489
SPF record presence	Email	NIS2 čl. 21(2)(h) · RFC 7208
SPF qualifier (-all vs ~all)	Email	NIS2 čl. 21(2)(h) phishing hardening
DKIM selector validita	Email	NIS2 čl. 21(2)(h) · DORA čl. 9(4)(c) · RFC 6376
MTA-STS policy (mode=enforce)	Email	NIS2 čl. 21(2)(g) · RFC 8461
MTA-STS policy mode	Email	NIS2 čl. 21(2)(g)
TLS-RPT (reporting)	Email	NIS2 čl. 21(2)(c) incident detection · RFC 8460
SMTP STARTTLS	Email	NIS2 čl. 21(2)(g) · GDPR čl. 32(1)(a)
BIMI (brand indicators)	Email	NIS2 čl. 21(2)(h) · ako recommended hygiene
Reverse DNS (PTR)	Email	Recommended hygiene (NIS2 spirit)
SMTP server identifikácia	Email	NIS2 čl. 21(2)(h)

C. DNS / DNSSEC (9 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
DNSSEC chain validity	DNS	NIS2 čl. 21(2)(g) · ENISA DNS hardening guide
DNSSEC algoritmus	DNS	NIS2 čl. 21(2)(g) · BSI TR-02102
CAA records	DNS	NIS2 čl. 21(2)(g) · CA/B Forum BR
MX configuration	DNS	NIS2 čl. 21(2)(c) resilience
NS records	DNS	NIS2 čl. 21(2)(c)
SOA serial format	DNS	Hygiene (RFC 1912)
Reverse DNS	DNS	Hygiene (NIS2 spirit)
DNS resolver redundancy	DNS	NIS2 čl. 21(2)(c) · DORA čl. 12 ICT resilience
DNS TTL hygiene	DNS	Operational hygiene

D. HTTP HLAVIČKY (10 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
	Headers	NIS2 čl. 21(2)(g) · GDPR čl. 32(1)(b) · OWASP

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
Content-Security-Policy (CSP)		
X-Frame-Options	Headers	**NIS2 čl. 21(2)(g)** · OWASP clickjacking
X-Content-Type-Options	Headers	**NIS2 čl. 21(2)(g)** · MIME sniffing protection
Referrer-Policy	Headers	**NIS2 čl. 21(2)(g)** · **GDPR čl. 25** data minimisation
Permissions-Policy	Headers	**NIS2 čl. 21(2)(g)** · **GDPR čl. 25**
Server header (info disclosure)	Headers	**NIS2 čl. 21(2)(g)** · OWASP best practice
Cache-Control	Headers	**GDPR čl. 32(1)** · NIS2 čl. 21(2)(c)
COOP / COEP / CORP	Headers	**NIS2 čl. 21(2)(g)** · cross-origin isolation
CORS policy	Headers	**NIS2 čl. 21(2)(g)**
HTTP version (HTTP/2 / HTTP/3)	Headers	Operational hygiene

E. DNSBL / REPUTÁCIA (8 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
DNSBL Spamhaus	DNSBL	**NIS2 čl. 21(2)(h)** · **DORA čl. 9(4)(c)**
DNSBL Barracuda	DNSBL	**NIS2 čl. 21(2)(h)**
DNSBL SORBS	DNSBL	**NIS2 čl. 21(2)(h)**
Blacklist status (aggregate)	DNSBL	**NIS2 čl. 21(2)(h)**
Reputation score	DNSBL	**NIS2 čl. 21(2)(h)**
Spam-related TXT records	DNSBL	**NIS2 čl. 21(2)(h)**
Domain age (WHOIS)	DNSBL	Hygiene
Dark-web mentions	DNSBL	**NIS2 čl. 21(2)(c)** · **GDPR čl. 33** breach detection

F. WEB OBSAH / COOKIES / AI ACT DISCLOSURE (11 KONTROL)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
Cookie SameSite	Web	**GDPR čl. 7** consent · **NIS2 čl. 21(2)(g)**
Cookie Secure flag	Web	**GDPR čl. 32** · **NIS2 čl. 21(2)(g)**
Cookie HttpOnly flag	Web	**GDPR čl. 32** · OWASP
robots.txt presence	Web	Hygiene (search engine discoverability)
sitemap.xml presence	Web	Hygiene
security.txt (RFC 9116)	Web	**NIS2 čl. 21(2)(c)** · **NIS2 čl. 23** incident notification channel
AI Act Art. 50 disclosure	AI Act	**AI Act čl. 50** transparency obligation (limited-risk + chatbot)
Open Graph / metadata	Web	Hygiene (brand integrity)
Structured Data (JSON-LD)	Web	Hygiene + AI Act Art. 13 (high-risk transparency)

KONTROLA	KATEGÓRIA	POKRYTÉ ČLÁNKY
Mixed content (HTTP on HTTPS)	Web	NIS2 čl. 21(2)(g) · GDPR čl. 32(1)(a)
SRI (Subresource Integrity)	Web	NIS2 čl. 21(2)(g) supply-chain · OWASP

Cross-cutting: AI Act sprievodca

Okrem 58 technických kontrol KubePlatform poskytuje **AI Act sprievodcu**, ktorý za 5 minút (8 otázok) klasifikuje konkrétny AI systém zákazníka do jednej z kategórií AI Actu:

KATEGÓRIA	DEFINÍCIA	POKRYTÉ ČLÁNKY AI ACTU
PROHIBITED	zakázaná prax	AI Act čl. 5 social scoring, manipulácia, real-time biometria
HIGH-RISK	vysoké riziko	AI Act čl. 6 + Annex III §1-§8 · obligations čl. 9-15 (risk mgmt, data quality, transparency, oversight, accuracy, cybersecurity)
LIMITED-RISK	limited	AI Act čl. 50 transparency / disclosure obligations
MINIMAL-RISK	minimal	Bez konkrétnych povinností (best practice)

Cross-cutting: tamper-evident audit log (Merkle hash)

Per-tenant SHA-256 hash chain nad finalizovanými wizard verdiktmi. Customer si môže kedykoľvek stiahnuť celý audit log + spustiť verejne publikovaný verifikačný skript (`scripts/verify_audit_chain.py`) a získať matematický dôkaz, že záznamy neboli upravené po svojom vytvorení.

VLASTNOSŤ	POKRYTÉ ČLÁNKY
Append-only audit log	NIS2 čl. 21(2)(b) incident handling · DORA čl. 9(4)(d) · GDPR čl. 30 records of processing · AI Act čl. 12 logging
Cryptographic verifiability	NIS2 čl. 21(2)(g) integrity · DORA čl. 9(3)
Per-tenant isolation	GDPR čl. 32(1)(b) confidentiality

Cross-cutting: HMAC-podpísaný kvartálny certifikát

Kvartálny PDF dokument asserting stav súladu, podpísaný HMAC-SHA256 nad canonical JSON. Verifikovateľný cez verejnú URL bez interakcie s KubePlatform.

VLASTNOSŤ	POKRYTÉ ČLÁNKY
Quarterly attestation	NIS2 čl. 21(3) regular assessment · DORA čl. 18 reporting framework
Public verify URL	DORA čl. 28 ICT third-party assurance · GDPR čl. 28 processor accountability
SK + EN bilingual	Pre slovenských dohliadacích orgánov (NBÚ, NCKB) + EÚ úroveň

Upozornenie: Tento dokument je *orientačná mapa* technických kontrol KubePlatform na vybrané články EÚ regulácií. Nie je právnym stanoviskom ani formálnou conformity assessment dokumentáciou. Pre formálnu certifikáciu kontaktujte oprávnenú EÚ notifikovanú osobu (ISO/IEC 27001, ISO/IEC 42001) alebo NBÚ (NIS2 audit per zákon 69/2018 Z.z.). Mapovanie odráža stav regulácií k 18.5.2026 — pri zmene článku alebo zavedení vykonávacieho aktu (implementing act) bude aktualizované.

Kontakt pre otázky / opravy: info@likeyou.today · audit.likeyou.today