ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 2:
Zodpovednosť regulovaných subjektov, Časť. 1

JUDr. Michal Rampášek

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

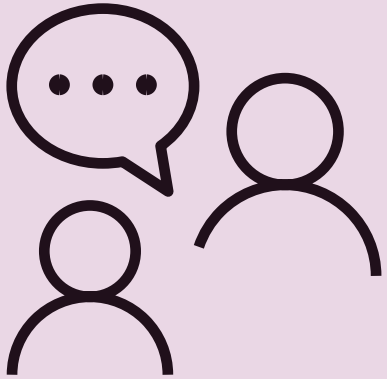
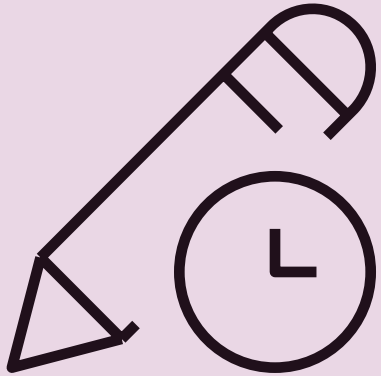
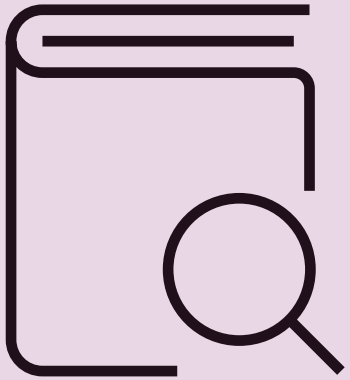
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

- Technická normalizácia kybernetickej bezpečnosti a vzťah k regulácií v EÚ
- Európska certifikácia kybernetickej bezpečnosti
- Aktuálny legislatívny vývoj (CSA2, revízia NIS2, Digital Omnibus, etc.)
- Prehľad regulácií v KB a ich súvislosti
- Zákon o kybernetickej bezpečnosti a povinnosti a zodpovednosť PZS
- Bezpečnostné opatrenia

ÚVOD

TECHNICKÁ NORMALIZÁCIA A REGULÁCIA KYBERENETICKEJ BEZPEČNOSTI

Technická norma

- **dokument vytvorený na základe dohody a schválený uznaným orgánom, ktorý poskytuje na všeobecné a opakované použitie pravidlá, pokyny, charakteristiky alebo výsledky činností**.
- Dokument technickej normy:

➢ je kodifikovanou najlepšou praxou a obsahuje všeobecne uznávané technické riešenia, ktoré sú k dispozícii všetkým zainteresovaným stranám,

➢ je návodom na efektívne ošetrovanie rizík,

➢ je nástrojom konkurencieschopnosti pre výrobcov, predajcov a dovozcov,

➢ prispieva k ochrane spotrebiteľov a

➢ uľahčuje medzinárodný obchod.

Právna úprava technickej normalizácie

- Nariadenie (EÚ) č. 1025/2012 o európskej normalizácii,
- zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu v znení neskorších predpisov,
- zákon č. 55/2018 Z. z. o poskytovaní informácií o technickom predpise a o prekážkach voľného pohybu tovaru v znení neskorších predpisov,
- zákon č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

Organizácie v EÚ

- **CEN/CENELEC**
- **Technická normalizácia v Európskej únii** je zastrešená Európskym výborom pre normalizáciu (CEN „Comité Européen de Normalisation"). V európskej technickej normalizácii normy pripravované, preberané a publikované spoločne s Európskym výborom pre normalizáciu v elektrotechnike (CENELEC „Comité Européen de Normalisation Électrotechnique"). Rovnako ako v ISO/IEC, sa aj CEN/CENELEC opiera o štruktúru technických komisií, z ktorých sú pre oblasť informačnej a kybernetickej bezpečnosti podstatné najmä nasledujúce dve:
- CEN-CLC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov" - horizontálna technická komisia (naprieč rôznymi sektormi)
- CLC/TC 65X „Meranie, riadenie a automatizácia priemyselných procesov" – vertikálna komisia (zameraná špecificky na priemyselné automatizačné systémy (IACS).)
- EN-CENELEC Joint Technical Committee 21 on 'Artificial Intelligence'

Záväznosť technických noriem

- Technická norma je dokument vo všeobecnosti určený na dobrovoľné používanie. Plnenie požiadaviek technických noriem na rozdiel od požiadaviek všeobecne záväzných právnych predpisov (napr. zákonov) nie je povinné.
- § 3 ods. 14 zákona č. 60/2018 Z. z. o technickej normalizácii
- Orgán štátnej správy môže uviesť odkaz na slovenskú technickú normu alebo technickú normalizačnú informáciu v texte návrhu všeobecne záväzného právneho predpisu. Podmienky: predkladateľ návrh zákona nesie výdavky na každé poskytnutie slovenskej technickej normy, vopred musí oboznámiť ÚNMS SR, technická norma je alebo bude prevzatá do sústavy STN

Záväznosť technických noriem

- V zmysle legislatívnych pravidiel vlády SR platí, že ak je to potrebné vzhľadom na technický charakter právneho predpisu alebo ak ide o právny predpis, ktorým sa do právneho poriadku Slovenskej republiky preberá právne záväzný akt Európskej únie, ktorý odkazuje na technické normy, **odkazovať sa na ne možno iba v poznámke pod čiarou**. **Podmienkou takejto citácie medzinárodnej alebo európskej technickej normy je, že norma je prevzatá do sústavy STN**.
- **Záväznosť v rámci zmluvných vzťahov**, napríklad v zmluvách medzi dodávateľom a odberateľom, zmluvách o SW dielo, zmluvách o poskytovaní služieb kybernetickej bezpečnsoti, alebo v dohodách o úrovni služieb (SLA).

Technické normy v KB

- STN EN ISO/IEC 27001 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2022)
- STN EN ISO/IEC 27002:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022),
- STN EN ISO 22301 Ochrana spoločnosti. Systémy manažérstva kontinuity podnikania. Požiadavky (ISO 22301: 2019)
- STN EN ISO/IEC 29147:2020 Informačné technológie. Bezpečnostné metódy. Odhaľovanie zraniteľností (ISO/IEC 29147: 2018)
- ISO/IEC 42001:2023 – Information technology – Artificial intelligence – Management system (Informačné technológie. Umelá inteligencia. Systém manažérstva).

EU harmonizované normy (HN)

- CEN/CENELEC
- Technická komisia CEN-CLC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov" - európske normy (EN) na podporu právnych aktov EÚ (napr. CSA, CRA, DORA, AI Act, NIS2)
- Nariadenie (EÚ) č. 1025/2012 o európskej normalizácii
- Životný cyklus tvorby a prijatia HN sa začína a končí v Komisii
- Len Komisia rozhodne, či v *Úradnom vestníku EÚ* uverejní, neuverejní alebo uverejní s obmedzením odkazy na príslušnú harmonizovanú normu

Spoločné špecifikácie

- Väčšia kontrola nad HN
- Komisia je splnomocnená priamo vypracovať - prostredníctvom vykonávacích aktov - spoločné špecifikácie (technické dokumenty alternatívne k HN)
- Výnimočné núdzové riešenie
  - keď HN buď neexistujú, sú nedostatočné, alebo *primerane neriešia obavy týkajúce sa základných práv* (čl. 41 ods. 1 AI Akt)
  - na uľahčenie povinnosti výrobcu digitálneho produktu dosiahnuť súlad so základnými požiadavkami, keď je normalizačný proces zablokovaný alebo keď pri zavádzaní vhodných HN dochádza k oneskoreniam (čl. 27 ods. 2 CRA)

Žiadosti Komisie na vývoj noriem

- **AI Akt: C(2023)3215 – Standardisation request**
- COMMISSION IMPLEMENTING DECISION of 22.5.2023 on a standardisation request to CEN/CENELEC in support of Union policy on artificial intelligence

https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

- **CRA: C(2025)618**
- COMMISSION IMPLEMENTING DECISION on a standardisation request to CEN/CENELEC/ETSI as regards products with digital elements in support of Regulation (EU) 2024/2847

https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en

Normy a preukazovanie zhody

- Dodržiavanie harmonizovaných noriem síce nie je povinné,
- Pre výrobky, ktoré spĺňajú tieto normy, platí predpoklad zhody so základnými požiadavkami, ktoré sa ich týkajú a sú stanovené príslušnými harmonizačnými právnymi predpismi Únie. Tento právny účinok, ktorý priznáva uvedená právna úprava, predstavuje jednu z podstatných vlastností týchto noriem.
- Harmonizované normy sú teda jedným z hlavných prostriedkov na dosiahnutie zhody a súladu s legislatívnymi požiadavkami. Recitál č. 5 nariadenia č. 1025/2012.

Juridifikácia

- Právny význam HN vzrástol natolko, že predpisy nie je možné plne pochopiť bez príslušných noriem, čím sa HN stávajú *de facto* záväznými (**C-171/11 *Fra.bo***)
- Pojem "juridifikácia" - Schapel, Harm. '*The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law*.' (2013) Maastricht Journal of European and Comparative Law
- HN sú vzhľadom na svoje právne účinky súčasťou práva Únie, keďže práve odkazmi na ustanovenia takejto normy je určené, či domnienka [súladu] uvedená v [uvedenej smernici] platí alebo neplatí pre daný výrobok (**C-613/14 *James Elliott***)
- Ak právna úprava Únie stanovuje, že dodržiavanie harmonizovanej normy zakladá predpoklad zhody so základnými požiadavkami tejto právnej úpravy, znamená to, že každá fyzická alebo právnická osoba, ktorá sa snaží účinne tento predpoklad vyvrátiť vo vzťahu k danému výrobku alebo službe, musí preukázať, že tento výrobok alebo služba nespĺňa túto normu, alebo alternatívne, že uvedená norma je chybná.(**C-588/21 *Public.Resource.Org***)

Prístup k HN

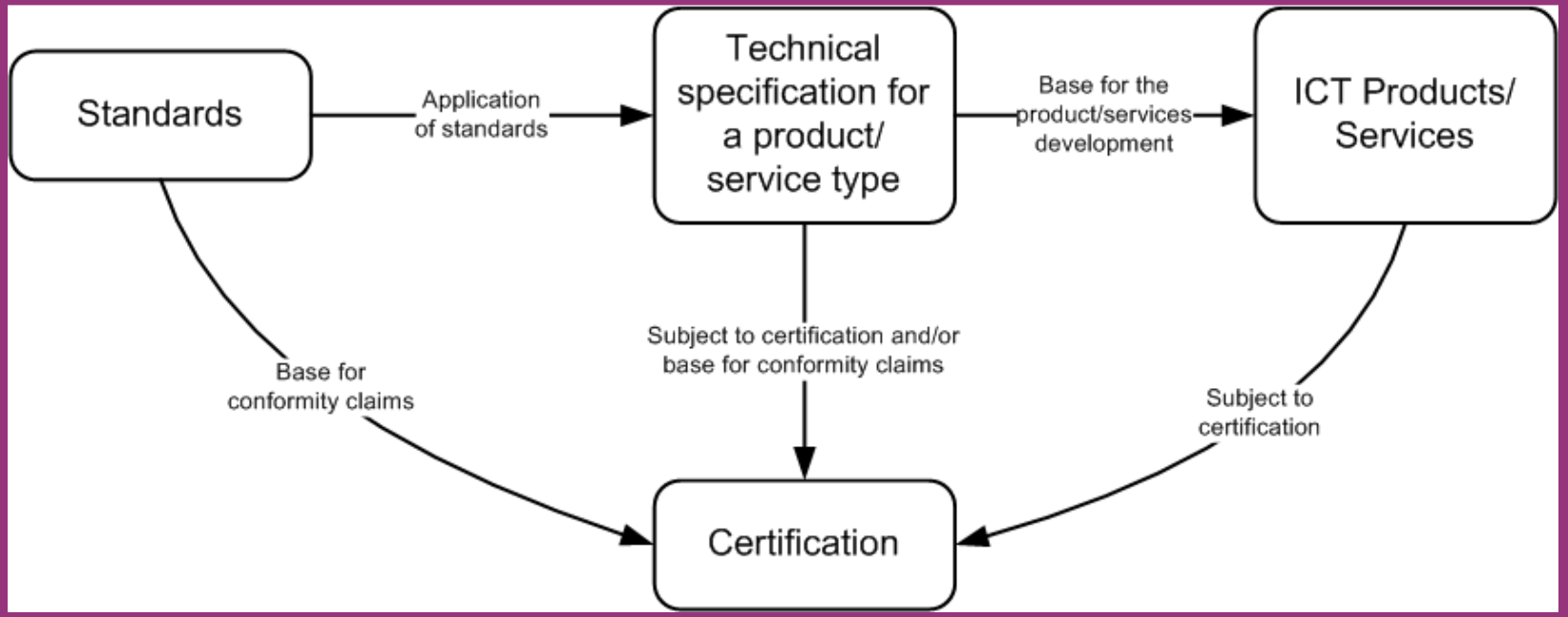
- (**C-588/21 *Public.Resource.Org***) Súdny dvor EÚ zrušil základnú axiómu Európskeho systému normalizácie : platený prístup k harmonizovaným normám. Súdny dvor potvrdil, že harmonizované normy sú neoddeliteľnou súčasťou práva EÚ a musa byť voľne prístupné.
- prístup podliehal obmedzeniam autorských práv , najmä licenčným poplatkom stanoveným normalizačnými orgánmi.
- „ hoci nariadenie č. 1025/2012 stanovuje, že dodržiavanie harmonizovaných noriem nie je povinné, pre výrobky, ktoré spĺňajú tieto normy, platí predpoklad zhody so základnými požiadavkami, ktoré sa ich týkajú a sú stanovené príslušnými harmonizačnými právnymi predpismi Únie. Tento právny účinok, ktorý priznáva uvedená právna úprava, predstavuje jednu z podstatných vlastností týchto noriem a vytvára z nich základný nástroj pre hospodárske subjekty na účely uplatňovania práva na voľný pohyb tovaru alebo služieb na trhu Únie.“
- „ požadované harmonizované normy sú súčasťou práva Únie.“
- „ prevažujúci verejný záujem .. odôvodňuje zverejnenie požadovaných harmonizovaných noriem.“

Certifikácia a Akt o kybernetickej bezpečnosti (CSA)

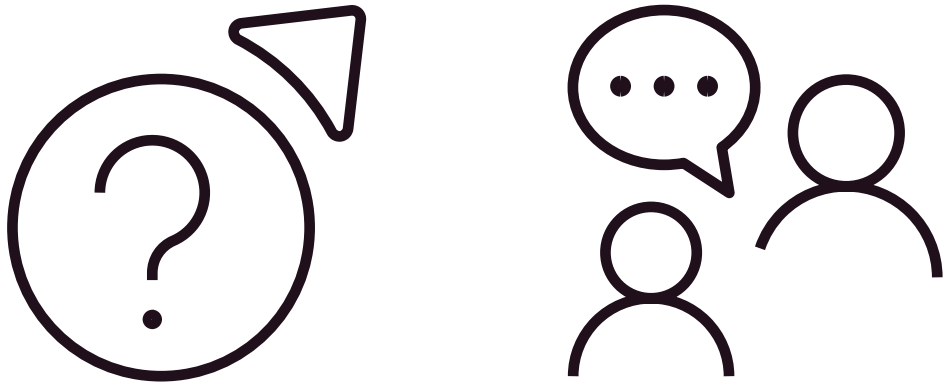
- Akt o kybernetickej bezpečnosti (Nariadenie 2019/881)
- produkty IKT, služby IKT alebo procesy IKT a ***riadené bezpečnostné služby*** v Únii **Novela CSA**: Nariadenie(EÚ) 2025/37 + návrh CSA2 (nový objekt posudzovania „Cyber posture")
- „Riadená bezpečnostná služba" je služba poskytovaná tretej strane pri riadení rizika kybernetickej bezpečnosti alebo poskytovanie pomoci pri týchto činnostiach, ako je **riešenie incidentu, penetračné testovanie, bezpečnostné audity a konzultácie vrátane odborného poradenstva súvisiaceho s technickou podporou**
- Európske systémy certifikácie kybernetickej bezpečnosti by mali byť nediskriminačné a založené na európskych alebo medzinárodných normách.
- Certifikát alebo EÚ vyhlásenie o zhode odkazujú na súvisiace technické špecifikácie, normy a postupy vrátane technických kontrol, ktorých účelom je znížiť riziko kybernetických bezpečnostných incidentov alebo týmto incidentom predísť.

Úloha noriem v procese posudzovania zhody a certifikácie

- ENISA: Standardisation in support of the Cybersecurity Certification. December 2019



Certifikácia



Certifikácia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Certifikácia a Zodpovednosť

- Certifikácia môže pomôcť pri preukázaní súladu, ale vo všeobecnosti **nenahrádza (ani automaticky neznižuje) zodpovednosť subjektu** (prevádzkovateľa základnej služby).

Harmonizácia certifikácie

- Nariadenie CSA je od roku2019 základným kameňom rámca EÚ pre certifikáciu kybernetickej bezpečnosti. Poskytuje EÚ základ pre vývoj schém.
- Zamerané na produkty, procesy a služby IKT. Najnovšia verzia, novelizovaná v roku 2024, zahŕňa možnosť certifikácie riadených bezpečnostných služieb
- Doteraz nebola certifikácia v EÚ harmonizovaná. Národné schémy na uspokojenie Preto bolo pre poskytovateľov riešení IKT, ktorí boli ochotní osloviť rôzne členské štáty, nákladné, pretože si nechali svoje riešenia certifikovať viackrát. Bez schém bolo aj pre spotrebiteľa náročné dôverovať riešeniu
- Jednotný rámec na úrovni EÚ umožňuje výrobcom a poskytovateľom ľahšie osloviť trh v celej EÚ a spotrebiteľom lepšie pochopiť úroveň bezpečnosti riešení, ktoré si kupujú.
- Dodržiavanie procesu a požiadaviek uvedených v certifikačnom rámci v konečnom dôsledku zvyšuje celkovú úroveň kybernetickej bezpečnosti na trhu IKT.

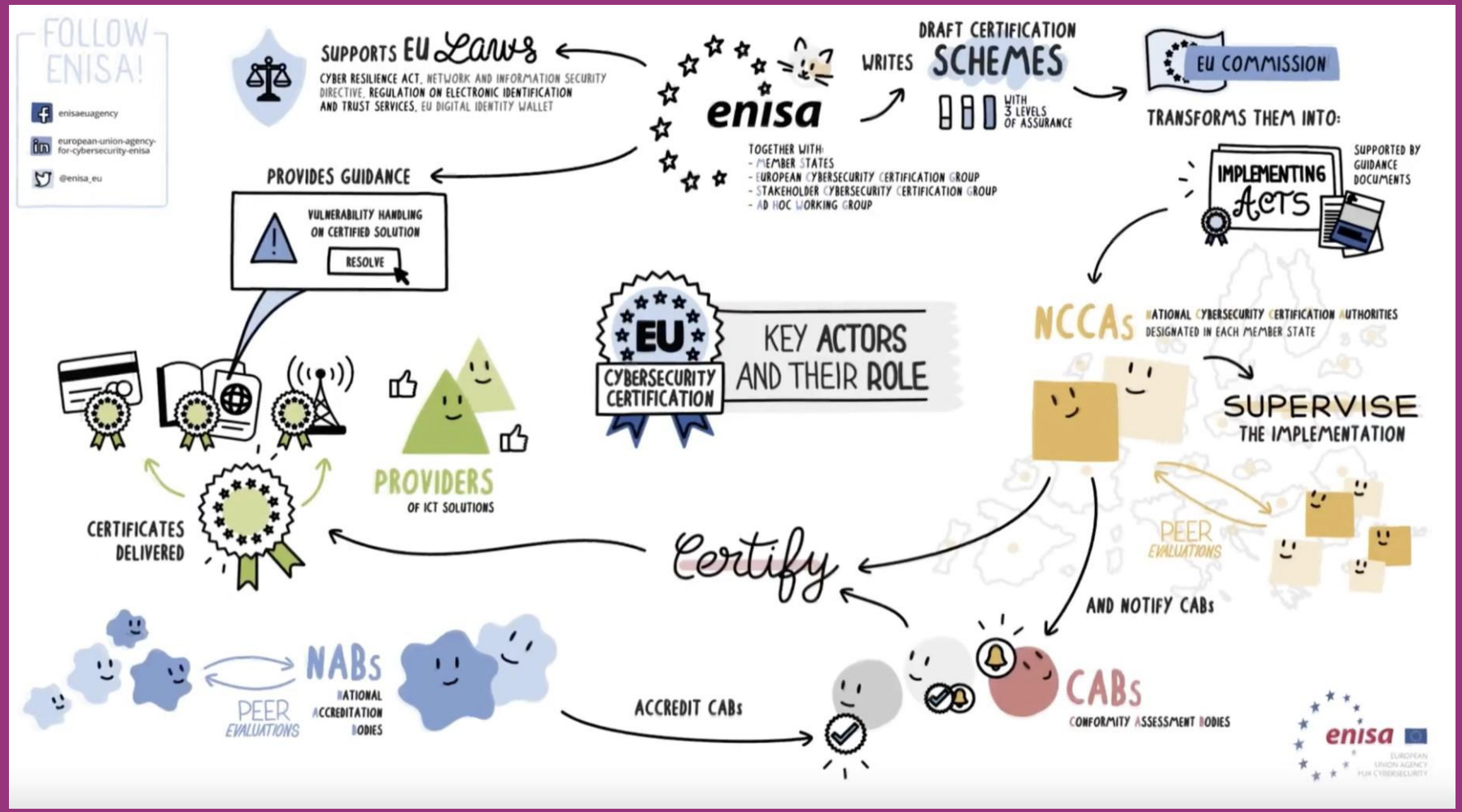
Certifikácia a regulácia

- Hoci je certifikácia dobrovoľná, v niektorých prípadoch môže riešiť aj regulačné požiadavky.
- Akt o kybernetickej solidarite spomína certifikáciu služieb pri definovaní kritérií pre budovanie kybernetickej rezervy EÚ;
- Produkty s digitálnym prvkom s certifikáciou EUCC budú v súlade so Aktom o kybernetickej odolnosti (CRA).
- Komisia je v v čl. 24 smernici NIS2 splnomocnená prijímať akty na doplnenie tejto smernice tým, že bližšie určí, od ktorých kategórií kľúčových a dôležitých subjektov sa má vyžadovať, aby používali určité certifikované produkty IKT, služby IKT a procesy IKT alebo získali certifikát v rámci niektorého európskeho systému kybernetickej bezpečnosti.

Pojmy v systéme certifikácie

- **Systémom certifikácie** kybernetickej bezpečnosti je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti.
- **Schéma certifikácie** kybernetickej bezpečnosti je súbor pravidiel, technických požiadaviek, technických noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT.
- Certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná a vysoká podľa osobitého predpisu vykonáva len akreditovaná osoba.
- **Akreditovanou osobou** pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká môže byť len Národný bezpečnostný úrad

Certifikácia



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Certifikačné schémy EÚ

- Každá EÚ schéma by mala špecifikovať najmä:

1. Kategórie zahrnutých produktov a služieb;
2. Požiadavky na kybernetickú bezpečnosť, ako sú normy alebo technické špecifikácie;
3. Typ hodnotenia, ako napríklad sebahodnotenie alebo hodnotenie treťou stranou;
4. Zamýšľanú úroveň záruky.
5. Úrovne záruky sa používajú na informovanie používateľov o kybernetickom riziku produktu a môžu byť základné, podstatné a/alebo vysoké. Sú úmerné úrovni rizika spojeného so zamýšľaným použitím produktu, služby alebo procesu z hľadiska pravdepodobnosti a dopadu nehody. Vysoká úroveň zabezpečenia by znamenala, že certifikovaný produkt prešiel najvyššími bezpečnostnými testami.

- Výsledný certifikát bude uznávaný vo všetkých členských štátoch EÚ, čo uľahčí podnikom obchodovanie cez hranice a kupujúcim pochopenie bezpečnostných prvkov produktu alebo služby.

EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

- Prvá schéma založená na medzinárodnej norme Common Criteria (ISO/IEC 15408), ktorá sa používa na vydávanie certifikátov už takmer 30 rokov.
- 27. februára 2025. Schéma sa bude uplatňovať v celej EÚ na dobrovoľnom základe a zameriava sa na certifikáciu kybernetickej bezpečnosti produktov IKT v ich životnom cykle vrátane: biometrických systémov, firewallov (hardvérových aj softvérových), detekčných a reakčných platforiem, routerov, switschov, špecializovaného softvéru (ako sú systémy SIEM a IDS/IDP), dátových diód a operačných systémov (vrátane mobilných zariadení).

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Union Rolling Work Programme for European cybersecurity certification (URWP)

- Oblasti pre budúcu európsku certifikáciu kybernetickej bezpečnosti:

1. ID peňaženky
2. Riadené bezpečnostné služby
3. Priemyselné automatizačné a riadiace systémy (IACS)
4. Vývoj životného cyklu zabezpečenia na základe požiadaviek CRA
5. Kryptografické mechanizmy

Revízia EU certifikačného rámca COM(2026) 11 (CSA2)

- Dňa 20. januára 2026 Komisia zverejnila návrh nového Aktu o kybernetickej bezpečnosti, ktorým sa reviduje Európsky rámec certifikácie kybernetickej bezpečnosti (ECCF).
- Nový ECCF má priniesť väčšiu jasnosť a jednoduchšie postupy pre vývoj schém štandardne do 12 mesiacov.
- Objekty certifikácie (čl. 71)

(a) produkty IKT, služby IKT a procesy IKT,

(b) riadené bezpečnostné služby

(c) **stav kybernetickej bezpečnosti subjektu („Cyber posture").**

- Subjekty, najmä tie, ktoré poskytujú viacero druhov služieb vo viacerých členských štátoch, môžu čeliť rôznym povinnostiam v oblasti kybernetickej bezpečnosti a bezpečnosti údajov podľa horizontálnych nástrojov, (napr. GDPR, NIS2), ako aj podľa sektorovo špecifických predpisov. Ide o možnosť preukázať subjektom súlad s požiadavkami na riadenie kybernetických rizík prostredníctvom európskeho certifikátu. Relevantná schéma by mohla prispieť k zefektívneniu požiadaviek na dodržiavanie predpisov vyplývajúcich z rôznych regulačných nástrojov bez toho, aby boli dotknuté ich špecifické požiadavky na certifikáciu.

Nový legislatívny rámec (NLF)

- súbor opatrení zameraných na posilnenie jednotného trhu s tovarom, zvýšenie bezpečnosti výrobkov a zlepšenie kvality posudzovania zhody (napr. označenie CE). Zjednodušuje aplikáciu predpisov a konsoliduje pravidlá pre označovanie a dohľad nad trhom, platný od roku 2010.

- tvoria dva komplementárne nástroje, ktorými sú nariadenie (ES) č. 765/2008 o akreditácii a dohľade nad trhom a rozhodnutie č. 768/2008/ES, ktorým sa zavádza spoločný rámec na uvádzanie výrobkov na trh
- Nariadením NLR sa zaviedli pravidlá o akreditácii (nástroj na hodnotenie odbornej spôsobilosti orgánov posudzovania zhody) a požiadavky na organizáciu a vykonávanie dohľadu nad trhom a kontroly výrobkov z tretích krajín.
- Rozhodnutím NLR sa stanovuje spoločný rámec harmonizačných právnych predpisov EÚ o výrobkoch. Tento rámec tvoria ustanovenia, ktoré sa používajú v právnych predpisoch EÚ o výrobkoch jednotne (napríklad vymedzenia pojmov, záväzky hospodárskych subjektov, notifikované orgány, mechanizmy v súvislosti s ochrannou doložkou atď.).

Označenie CE

- Označovanie – Všeobecné zásady
- Umiestnenie = zodpovednosť za zhodu

1. Označenie CE umiestňuje iba výrobca alebo jeho splnomocnený zástupca.
2. Označenie CE, ako je uvedené v prílohe II, sa umiestňuje len na výrobky, na ktoré je jeho umiestnenie ustanovené osobitnými harmonizačnými právnymi predpismi EÚ, a neumiestňuje sa na žiadny iný výrobok.
3. Umiestnenie označenia CE na výrobok znamená, že výrobca oznamuje, že berie na seba zodpovednosť za to, že výrobok spĺňa platné požiadavky ustanovené v harmonizačných právnych predpisoch Spoločenstva týkajúcich sa umiestnenia tohto označenia.
4. Označenie CE je jediným označením, ktorým sa potvrdzuje zhoda výrobku s platnými požiadavkami harmonizačných právnych predpisov
5. Zakazuje sa umiestňovať na výrobok označenia, znaky a nápisy, ktoré by mohli tretie strany zavádzať, pokiaľ ide o význam alebo podobu označenia CE. Na výrobok sa môže umiestniť akékoľvek iné označenie, ak sa tým nenaruší viditeľnosť, čitateľnosť a význam označenia CE.

Produktová legislatíva NLF

Príklady:

1. Strojové zariadenia – nariadenie (EÚ) 2023/1230 (ktoré nahrádza smernicu 2006/42/ES)
2. Zákon o umelej inteligencii – nariadenie (EÚ) 2024/1689
3. Zákon o kybernetickej odolnosti – nariadenie (EÚ) 2024/2847
4. Rádiové zariadenia – smernica 2014/53/EÚ
5. Zdravotnícke pomôcky – nariadenie (EÚ) 2017/745
6. Diagnostické zdravotnícke pomôcky in vitro – nariadenie (EÚ) 2017/746

Modrá príručka

- Modrá príručka je jedným z hlavných referenčných dokumentov Európskej komisie, ktoré vysvetľujú, ako implementovať legislatívu na základe NLF.
- Publikovaná verzia 2022, na eur lex pod číslom **2022/C 247/01**
- Pomôcka pri výklade aj RED smernice a nariadenia CRA, napríklad:
- Čo je „**sprístupnenie na trhu**"? = Výrobok je sprístupnený na trhu, keď je dodaný na distribúciu, spotrebu alebo používanie na trhu Únie v rámci obchodnej činnosti, či už za odplatu, alebo bezplatne (napr. výzva na nákup, reklamné kampane). Koncepcia sprístupnenia sa vzťahuje na každý jednotlivý výrobok a iba vtedy, ak je výrobok určený na konečné použitie na trhu Únie.

Modrá príručka

- Čo je „**uvedenie na trh**“? = Výrobok je uvedený na trh vtedy, keď je **prvýkrát sprístupnený** na trhu Únie. Podľa harmonizačných právnych predpisov Únie sa každý jednotlivý výrobok môže uviesť na trh Únie len raz. Koncepcia uvedenia na trh sa vzťahuje **na každý jednotlivý výrobok**, nie na typ výrobku, a na to, či bol vyrobený ako samostatná jednotka alebo v sérii. Výrobky sprístupnené na trhu musia byť v čase uvedenia na trh v súlade s príslušnými harmonizačnými právnymi predpismi Únie.

PREHĽAD REGULÁCIE A SÚVISLOSTI

Kontext

EÚ dnes reguluje kybernetickú bezpečnosť ako ekosystém: časť pravidiel ide cez „bezpečnosť organizácií" (governance, riadenie rizík, incidenty), časť cez „bezpečnosť produktov" (hardvér/softvér na trhu) a ďalšia cez „odolnosť a krízové reakcie" (spoločné kapacity, koordinácia, pomoc pri veľkých incidentoch).
Popri horizontálnych pravidlách existujú aj sektorové predpisy, najmä finančný sektor, energetika a letectvo , ktoré idú v detailoch ďalej alebo stanovujú špecifické požiadavky.

1) EÚ právny rámec je vrstvový: organizácie (NIS2), produkty (CRA), certifikácia (CSA), dáta (GDPR) a reakcia (CSoA).

2) Sektorové predpisy sú rozhodujúce v oblasti bezpečnostných opatrení: špecifikujú testovanie, riadenie rizík dodávateľov a reportovanie (napr. DORA, NCCS, Part-IS).

3) Pre právnu prax je potrebné vždy identifikovať rolu subjektu (prevádzkovateľ/poskytovateľ vs výrobca/dovozca vs dodávateľ služby) a potom mapovať povinnosti.

4) Smernice EÚ vs. Nariadenia EÚ, od minimálnej po úplnú harmonizáciu.

Vykonávacie a delegované akty

Vykonávacie akty
Primárnu zodpovednosť za vykonávanie práva EÚ nesú krajiny EÚ. V oblastiach, kde sú potrebné jednotné podmienky vykonávania (dane, poľnohospodárstvo, vnútorný trh, zdravie a bezpečnosť potravín atď.), však Komisia (alebo výnimočne Rada) prijíma vykonávací akt (napr. vykonávacie nariadenie Komisie 2024/2690).

Delegované akty
Komisia ich prijíma na základe delegovania udeleného v texte právneho predpisu EÚ.
Právomoc Komisie prijímať delegované akty má obmedzenia:

a. delegovaný akt nemôže meniť podstatné prvky právneho predpisu
b. legislatívny akt musí vymedziť ciele, obsah, rozsah a trvanie delegovania právomoci
c. Parlament a Rada môžu delegovanie odvolať alebo voči nemu vzniesť námietky

Napr. delegované nariadenia k nariadeniu DORA (2025/301, 2025/532, 2025/420, atď.)

Vývoj

2016
GDPR

2019
CSA

2022
NIS2 / CER / DORA

2023
Chips Act / Part-IS

2024
AI Act / CRA / eIDAS2 / NCCS

2025
Cyber Solidarity Act, EHDS Act, + CSA zmena (MSS)

2026
CSA2, revNIS2, Digital Omnibus, Dital Networks Act

NIS2 (2022/2555) + návrhy revízií

- Národné stratégie kybernetickej bezpečnosti, jednotné miesta, plány riadenia kybernetických kríz
- CSIRT jednotky
- Kľúčové a dôležité subjekty (Prílohy I a II) – samoidentifikácia. Kritické subjekty (CER) = kľúčové
- Odvetvové právne akty Únie (DORA)
- Minimálna harmonizácia
- Koordinované zverejňovanie zraniteľností a EU databáza zraniteľností
- Governance a opatrenia riadenia kybernrizík
- Oznamovanie incidentov a výmena informácií

- Návrh nariadenia Digital Omnibus (COM/2025/837 final) – používanie jednotného kontaktného miesta pre nahlasovania incidentov stanovených v NIS 2 , GDPR, DORA, eIDAS a CER, a zefektívniť obsah nahlasovaných informácií pri vypracúvaní spoločných vzorov na podávanie správ pre NIS2 (čl. 23 ods. 11 + revNIS2 údaje k ransomvérovému útoku), CER alebo GDPR.

- Návrh revízie NIS2 (COM(2026) 13 final) - Obmedzenie pôsobnosti (napr. elektrina, DNS poskytovatelia), nová kategória pre kľúčové subjekty „malé podniky so strednou trhovou kapitalizáciou" (*small mid-cap enterprises*) (C(2025) 3500 final), Maximálna harmonizácia pri vykonávacích nariadeniach (čl. 21(5)), Certifikácia ako dôkaz súladu Európska certifikácia „cyber posture" sa môže použiť ako dôkaz splnenia čl. 21 NIS2 a dôvod, aby orgány neukladali dodatočné opatrenia

CER (2022/2557)

„sesterská" smernica k NIS2, upravuje najmä fyzickú odolnosť (ochrana objektov, ľudí„ prístupových režimov, kontinuita prevádzky a alternatívni dodávatelia), ale v praxi sa prekrýva s kybernetickou bezpečnosťou lebo incidenty v kritickej infraštruktúre bývajú kombinované .

- Minimálna harmonizácia (Zákon č. 367/2024 Z.z. o kritickej infraštruktúre)
- Stratégia na zvýšenie odolnosti kritických subjektov (do 17. januára 2026)
- Základná služba a nové sektory
- Identifikácia štátom (do 17. júla 2026), kritické subjekty = kľúčové podľa NIS2
- Identifikácia kritických subjektov osobitného európskeho významu (6 a viac štátov)
- Posúdenie rizika štátom aj subjektom (do 9 mes.) (vrátane fyzického rizika prírodných katastrof a zmeny klímy)
- Opatrenia kritických subjektov na zabezpečenie odolnosti (bezpečnostný plán)
- Previerky osôb
- Oznamovanie významných incidentov a hrozieb
- Sankcie určuje štát

CRA (2024/2847)

Nariadenie (Akt o kybernetickej odolnosti)

- Pravidlá kybernetickej bezpečnosti pri uvádzaní hardvéru a softvéru na trh
- Zodpovednosť za kybernetickú bezpečnosť produktu s digitálnymi prvkami
- Povinnosti výrobcov, distribútorov a dovozcov
- Základné požiadavky kybernetickej bezpečnosti na návrh, vývoj a výrobu produktov a na procesy riešenia zraniteľností počas predpokladaného obdobia používania produktov
- Harmonizované normy
- Posudzovanie zhody podľa úrovne rizika (samohodnotenie , posuzdorv) = "CE"
- Oznamovacie povinnosti (aktívne zneužívané zraniteľnosti, závažné incidenty, near missy)
- Dohľad a monitorovanie

EHDS (2025/327)

Nariadenie o európskom priestore pre zdravotné údaje (EHDS)

- spoločný rámec pre používanie a výmenu elektronických zdravotných údajov v celej EÚ.
- pravidlá a mechanizmy primárneho používania elektronických zdravotných údajov a sekundárneho používania elektronických zdravotných údajov (opakované použitie určitých údajov na účely verejného záujmu, podpory politiky a vedeckého výskumu).
- pravidlá pre systémy elektronických zdravotných záznamov („systémy EHR“) v súvislosti s dvoma povinnými harmonizovanými softvérovými komponentmi, a to európsky softvérový komponent interoperability pre systémy EHR a európsky softvérový komponent logovania pre systémy EHR, a pre wellness aplikácie
- Zároveň novelizuje nariadenie CRA (systémy EHR, ktoré sú produktmi s digitálnymi prvkami)

Cyber Solidarity Act (2025/38)

Je reakciou na to, že incidenty majú často cezhraničný dopad a členské štáty majú nerovnaké kapacity. Zmyslom nariadenia je budovať posilnenie kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne, najmä zriadením:

a) Európskeho systému varovania pred kybernetickobezpečnostnými hrozbami;

b) mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií a posilniť pripravenosť kľúčových a dôležitých subjektov v celej Únii a posilniť solidaritu rozvojom koordinovaného testovania pripravenosti a posilnených kapacít reakcie a zotavenie;

c) rezervy EÚ na účely kybernetickej bezpečnosti s cieľom pomáhať na požiadanie používateľom. Rezerva je poskytovaná vybranými dôveryhodnými poskytovateľmi riadených bezpečnostných služieb.

CSA (2019/881) (+CSA2)

- Nariadenie je základným kameňom rámca EÚ pre certifikáciu kybernetickej bezpečnosti. Poskytuje EÚ príležitosť vyvíjať schémy
- Zamerané na produkty, procesy a služby IKT. Po novelizácii v roku 2024, zahŕňa možnosť certifikácie riadených bezpečnostných služieb
- Mandát a ciele ENISA (Agentúra európskej únie pre kybernetickú bezpečnosť). Agentúra ENISA prispieva k tvorbe a vykonávaniu politiky a práva Únie, pomáha budovať kapacity, spolupracuje a vytvára synergie s inštitúciami, orgánmi, úradmi a agentúrami Únie vrátane tímu CERT-EU, útvarmi, ktoré sa zaoberajú počítačovou kriminalitou, podporuje certifikáciu (vypracúva kandidátske európske schémy certifikácie kybernetickej bezpečnosti), vzdelávanie, výskum a inovácie.

- Návrh CSA2: bezpečnosť dodávateľských reťazcov IKT, kľúčové IKT kompotenty (aj pre telco), zákaz používania IKT komponentov pre NIS2 subjekty, vysokorizikoví dodávatelia určení Komisiou (blacklist) – vylúčení z verejného obstarávania IKT, certifikácie, čerpania prostriedkov

GDPR, AIA, eIDAS(2), PSD2

Horizontálne predpisy, ktoré priamo zasahujú kyberbezpečnosť

GDPR upravuje priamo požiadavky na bezpečnosť osobných údajov. Prevádzkovateľ a sprostredkovateľ majú prijať primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú riziku, pričom uvedené opatrenia prípadne zahŕňajú aj: šifrovanie osobných údajov; zabezpečiť dostupnosť a odolnosť systémov spracúvania a služieb, schopnosť včas obnoviť dostupnosť osobných údajov po incidente ako aj proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení.

AI Akt prináša požiadavky na riadenie rizík a bezpečnosť vysokorizikových AI systémov a modelov AI na všeobecné účely so systémovými rizikami, kyberbezpečnosť je súčasť dôveryhodnosti a bezpečnej AI.

eIDAS zavádza rámec pre dôveryhodné služby, vďaka čomu sú elektronické transakcie rovnako právne záväzné ako papierové.
eIDAS 2.0 (Digitálna identita EÚ) aktualizované nariadenie, zavádza Európsku peňaženku digitálnej identity, ktorá umožňuje používateľom bezpečne ukladať a zdieľať identifikačné údaje.

PSD2 stanovuje prísne opatrenia v oblasti kybernetickej bezpečnosti a overovania pri elektronických platbách s cieľom znížiť počet podvodov a zabezpečiť údaje spotrebiteľov. Požaduje silnú autentifikáciu zákazníka(SCA) (2FA/MFA) pre väčšinu online transakcií.

Finančný sektor, Energetika, Letectvo, Digital, Verejná správa

Sektorové regulácie

Vo finančnom sektore **DORA** (2022/2554) kladie dôraz na riadenie IKT rizík, testovanie odolnosti, oznamovanie závažných incidentov, riadenie externého IKT rizika , vrátane dohľadu nad kritickými poskytovateľmi IKT služieb, a tiež výmenu informácií.

V energetike **Sieťový kódex o kybernetickej bezpečnosti (NCCS)** (2024/1366) dopĺňa ustanovenia NIS2 týkajúce sa odvetvia elektrickej energie, keďide o cezhraničné toky elektriny (povinnosti pre subjekty s veľkým a kritickým vplyvom)

V letectve **Part-IS** a súvisiace pravidlá, Vykonávacie nariadenie Komisie (EÚ) 2023/203 a 2022/1645 upravujú riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva, ktoré by mohli ovplyvniť systémy IKT a údaje používané na účely civilného letectva

Vykonávacie nariadenie Komisie 2024/2690 (sektorové technické a metodické požiadavky pre vybrané digitálne sektory)

Verejná správa (**zákon č. 95/2019 Z.z. a vyhláška**) upravujú požiadavky a opatrenia pre bezpečnosť informačných technológií verejnej správy (ITVS)

ZoKB

- Pôsobnosť zákona
- Postavenie NBÚ a ústredných orgánov
- Systém certifikácie kybernetickej bezpečnosti
- CSIRT (Národná jednotka CSIRT, Vládna jednotka CSIRT Akreditácia, Úlohy a povinnosti jednotky CSIRT)
- Jednotný informačný systém kybernetickej bezpečnosti (JISKB)
- Prevádzkovateľ základnej služby a Kritická základná služba
- Povinnosti prevádzkovateľa základnej služby
- Bezpečnostné opatrenia
- Osobitné povinnosti (subjekty z digitálnych sektorov)
- Kontrola a Ukladanie opatrení na nápravu

ZoKB po NIS2

- **Rozšírenie** pôsobnosti zákona **na nové subjekty**
- **Identifikácia regulovaného subjektu** na základe jeho zaradenia do sektora
- **Aplikácia bezpečnostných opatrení** na základe rizikovej analýzy
- **Bezpečnosť dodávateľského reťazca**
- **Hlásenia incidentov a iných bezpečnostných udalostí**
- **Koordinované zverejňovanie zraniteľností** (CVD)
- **Audit** a samohodnotenie
- **Certifikácia** bezpečnosti IKT produktov a služieb

Zmena koncepcie regulácie

- Predmetom regulácie nie je kybernetická bezpečnosť vo vzťahu k základným službám ale **kybernetická bezpečnosť a odolnosť kľúčových subjektov** a celých sektorov voči aktuálnym kybernetickým hrozbám.
- Termín „**základná služba" sa vypustil,** keďže povinné osoby sa už neidentifikujú podľa poskytovanej základnej služby**,** ale veľkostných kritérií a zaradenia do príslušného odvetvia.
- V kontexte základných služieb (ako modelu platného do 31.12.2024) sa „poskytovanie služieb" vzťahuje na činnosť**,** pri ktorej sú zo strany PZS zabezpečované určité služby pre tretie strany.

Zmena koncepcie regulácie

✅ **Subjekty so sídlom v SR a vykonávajúce alebo majúce postavenie definované ako PZS, ak spĺňajú veľkosť aspoň stredného podniku alebo aj bez splnenia podmienok veľkosti. Ministerstvo obrany SR** – len určené informačné systémy v jeho pôsobnosti

✅ **Poskytovatelia digitálnych služieb,** ak sú zapísaní v registri PZS **DNS služby, registrácia domén, Cloud computing, dátové centrá, Siete na sprístupňovanie obsahu, Riadené služby, Online trhy, internetové vyhľadávače, sociálne siete so sídlom mimo SR** (ak rozhodujú o bezpečnosti v SR, vykonávajú opatrenia alebo majú najväčšiu prevádzku v EÚ) **a mimo EÚ** (ak majú zástupcu v SR)

2. Na čo sa nevzťahuje? Na požiadavky na zabezpečenie sietí a informačných systémov

❌ **Utajované skutočnosti**
❌ **Spravodajské služby**
❌ **Osobitné predpisy pre vyšetrovanie, odhaľovanie, stíhanie trestných činov**
❌ **Bankovníctvo, finančný sektor**
❌ **Platobné systémy a zúčtovanie cenných papierov**

Rozhodné právo a one-stop-shop

- Subjekty, ktoré patria do rozsahu pôsobnosti ZoKB sa považujú za subjekty podliehajúce právomoci členského štátu, v ktorom **majú trvalý pobyt, miesto podnikania alebo sídlo**.
- Rozhodné právo sa určuje aj na základe osobitného určenia podľa § 2 ods. 2 ZoKB (osobu, ktorá poskytuje službu DNS, službu registrácie názvu domény, službu cloud computingu, službu dátového centra, sieť na sprístupňovanie obsahu, riadenú službu, bezpečnostnú službu, službu online trhu, službu internetového vyhľadávača alebo platformu služieb sociálnej siete, môžu byť zapísané do registra PZS a ZoKB sa na ňu vzťahuje **aj vtedy, ak nemá trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky**)

Povinnosti PZS - základné

- **Oznámiť činnosti na NBÚ** (§ 17 ods. 2,, § 18 ods. 2)
- **Implementovať bezpečnostné opatrenia** (§ 19 ods. 1) **a prijať, dodržiavať a vykonávať bezpečnostné opatrenia s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy, príklady dobrej praxe a medzinárodné normy** (§ 19 ods. 6 písm. g)
- **Audit alebo samohodnotenie** (§ 29)

Povinnosti PZS - incidenty

- Povinnosti podľa § 19 ods. 6

a) **riešiť kybernetický bezpečnostný incident,**

b) bezodkladne **hlásiť závažný** kybernetický bezpečnostný incident,

c) **spolupracovať** s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

d) v čase kybernetického bezpečnostného incidentu **zabezpečiť dôkaz alebo dôkazný prostriedok** tak, aby mohol byť použitý v trestnom konaní,

e) **oznámiť OČTK** skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

h) vytvoriť a zaviesť **účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov** o kybernetických hrozbách, zraniteľnostiach, kybernetických bezpečnostných incidentoch, udalostiach odvrátených v poslednej chvíli, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrenia rizík s cieľom dodržiavania tohto zákona,

Povinnosti PZS – incidenty (2)

- hlásiť **každý závažný kybernetický bezpečnostný incident** (§ 24 ods. 1) určeným spôsobom a v rozsahu (§ 24 ods. 3)
- hlásiť aj a) **významnú kybernetickú hrozbu**, o ktorej sa dozvie, b) **udalosť odvrátenú v poslednej chvíli**, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident, c) **zraniteľnosť** ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a PZS nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika. (§ 24 ods. 5)
- Ak je to vzhľadom na povahu alebo dôležitosť PZS potrebné a nedôjde k uzatvoreniu zmluvy podľa § 24 ods. 4, úrad môže rozhodnutím **uložiť PZS povinnosť automatizovaným spôsobom vyhodnocovať výskyt** kybernetického bezpečnostného incidentu **a nahlasovať** kybernetický bezpečnostný incident.
- **Plnenie povinnosti uloženej úradom prípade závažného kybernetického bezpečnostného incidentu alebo významnej kybernetickej hrozby** - riešiť kybernetický bezpečnostný incident, vykonať reaktívne opatrenie, poskytnúť návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu („ochranné opatrenie“) (§ 27 ods. 1)
- bezodkladne oznámiť a preukázať úradu prostredníctvom JISKB **vykonanie reaktívneho opatrenia a jeho výsledok a tiež predložiť ochranné oparenie na schválenie** (§ 27 ods. 6 a 8)

Povinnosti PZS – dodávatelia (1)

- analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu (§ 19 ods. 6 písm. f),
- zdržať sa používania konkrétneho produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 na poskytovanie služby alebo ich používanie obmedziť.(§ 27a Obmedzenie používania produktu, procesu, služby alebo tretej strany)

Povinnosti PZS – dodávatelia (2)

- **Uzatvoriť** s treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností **(**§ 19 ods. 2) Výnimky z povinnosti: dodávateľ je PZS**,** nízke riziko dodávateľa.
- **Tretia strana je** dodávateľ na výkon činností**,** ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre PZS.
- **Pri uzatvorení zmluvy vykonať analýzu rizík dodávateľa**
- **Zmluva musí mať minimálne náležitosti (napr.** § 7 ods. 2 Vyhlášky 227/2025 Z.z.**)**
- **Ďalšie požiadavky vyplývajú z bezpečnostných opatrení v oblasti bezpečnosti dodávateľského reťazca (príloha č. 1 k Vyhláške 227/2025 Z.z.) prijatých PZS po analýze rizík**

- PKZS je povinný úradu hlásiť uzatvorenie zmluvy s treťou stranou**, ktorá má významný vplyv** pri zabezpečovaní kybernetickej bezpečnosti a aj jej ukončenie (tretia strana sa **zapisuje do registra PZS) (**§ 19 ods. 7)

Povinnosti PZS – zmenové oznámenia

- **oznamovať úradu menovanie alebo zmenu štatutárneho orgánu, ak táto zmena nie je referenčným údajom** (§ 19 ods. 6 písm. i**).**
- **hlásiť zmeny v zapísaných údajoch, okrem referenčných údajov do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a ak prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, je povinný hlásiť úradu aj informáciu o uzatvorení zmluvy s treťou stranou o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti a aj informáciu o jej ukončení.**

Povinnosti PZS – audit

- Vykonať audit kybernetickej bezpečnosti **do dvoch rokov odo dňa zaradenia PZS** do registra PZS. Prevádzkovateľ základnej služby, ktorý nie je PKZS, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote podľa predchádzajúcej vety preverením účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom samohodnotením prostredníctvom JISKB (§ 29 ods. 1)
- Vykonať audit kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to **po každej zmene majúcej významný vplyv** na realizované bezpečnostné opatrenia a v určenom časovom intervale (§ 29 ods. 2)
- predložiť **záverečnú správu o výsledkoch auditu** úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu. (§ 29 ods. 5)
- **podriadiť sa nariadenému auditu** (§ 29 ods. 6)

Povinnosti PZS – kontrola

a) predložiť **výsledky kontrol alebo auditov** vykonaných inými orgánmi, ktoré súvisia s kontrolou vykonávanou úradom,

b) predložiť **vyžiadané originály alebo úradne osvedčené kópie dokladov**, písomností, záznamov dát na pamäťových médiách, a iné podklady súvisiace s kontrolou, vydať na vyžiadanie písomné potvrdenie o ich úplnosti a umožniť úradu alebo prizvanej osobe vyhotovovať si z nich kópie,

c) poskytnúť **súčinnosť** úradu alebo prizvanej osobe,

d) prijať **opatrenia na nápravu nedostatkov** zistených kontrolou a na odstránenie príčin ich vzniku uvedených v čiastkovej správe alebo v správe a predložiť úradu písomný zoznam prijatých opatrení v lehote určenej úradom,

e) predložiť a prepracovať v lehote určenej úradom **písomný zoznam prijatých opatrení**,

f) splniť prijaté opatrenia v primeranej lehote určenej úradom,

g) predložiť na výzvu úradu **dokumentáciu preukazujúcu splnenie** prijatých opatrení,

h) vytvoriť podmienky na vykonanie kontroly na mieste a zdržať sa konania, ktoré by ju mohlo ohroziť,

i) oboznámiť pri začatí kontroly na mieste úrad alebo prizvanú osobu **s bezpečnostnými predpismi miesta**

j) umožniť úradu alebo prizvanej osobe **vstup do objektu**, zariadenia, prevádzky, dopravného prostriedku, na pozemok alebo vstup do obydlia, ak sa používa aj na podnikanie alebo na vykonávanie inej hospodárskej činnosti, ktoré súvisia s poskytovaním služby prevádzkovateľa základnej služby.

Povinnosti PZS – Predbežné opatrenie

- Dodržiavať **predbežné opatrenie,** ktorým v rozsahu nevyhnutne potrebnom na predídenie vzniku vážnej škody alebo inej ujmy úrad a) uloží prevádzkovateľovi základnej služby**, aby niečo vykonal, niečoho sa zdržal alebo niečo strpel,** b) nariadi **zabezpečenie vecí, ktoré sú potrebné na vykonanie dôkazov** (§ 29i ods. 1)

Povinnosti PZS – Opatrenia na nápravu

- Plniť úradom uloženú povinnosť

a) vykonať audit kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote,

b) prijať opatrenia na nápravu,

c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, alebo

d) zakázať poskytovať službu do času nápravy nezákonného stavu, ak je takéto opatrenie nevyhnutne potrebné z dôvodu bezprostredného ohrozenia života alebo zdravia, iné opatrenia v rámci dohľadu neboli účinné a nebola vykonaná náprava v lehote určenej úradom; to neplatí, ak ide o PZS, ktorý je orgánom verejnej moci, alebo ktorý poskytuje službu na základe povinnosti uloženej zákonom alebo na jeho základe.(§ 29j ods. 1)

Povinnosti PZS – Opatrenia na nápravu – Obmedzenie prístupu

- Plniť **rozhodnutím súdu vydaným na návrh úradu povinnosť dočasne obmedziť prístup**

a) **odberateľov** dotknutých nezákonným stavom k službe, alebo

b) **k online rozhraniu**, prostredníctvom ktorého dochádza k porušeniu spôsobujúcemu nezákonný stav. (29k ods. 1)

- Za podmienky, že PZS neplní povinnosti uložené podľa § 29j ods. 1 riadne a včas, nezákonný stav pretrváva a spôsobuje vážnu škodu alebo inú ujmu a obsahuje znaky trestného činu proti životu, zdraviu alebo bezpečnosti osôb

Povinnosti PZS – Dohoda o náprave

- Plniť svoje záväzky z dohody o náprave (29l ods. 2)

Bezpečnostné opatrenia

- Nová štruktúra všeobecných bezpečnostných opatrení (§20 ods. 1 a 2)
- Podrobnejší popis bezpečnostných opatrení obsahuje vyhláška 227/2025 a jej príloha
- **Rozsah a spôsob implementácie bezpečnostných opatrení na základe rizikovej analýzy**
- Ak existuje **sektorový bezpečnostný štandard,** opatrenia sa aplikujú na jeho základe pri zachovaní základných spôsobilostí riadiť informačnú bezpečnosť, hlásiť a riešiť incidenty a pod. (§20 ods. 6)
- **Nariadenie Komisie 2024/2690 (Príloha)**

ISO27001:2022 Príloha A

ISO 27001 and ISO 27002. Information security controls, 2022

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 - www.patreon.com/AndreyProzorov

Control: measure that maintains and/or modifies risk

Porovnanie - príklad

Nariadenie Komisie 2024/2690 (Príloha)	**ISO 27001:2022**	**Položka V227/2025 (Príloha 1)**
3.2 Monitorovanie a logovanie (3.2.1 – 3.2.7) „vedú a zálohujú logy počas vopred stanoveného obdobia a chránia ich pred neoprávneným prístupom alebo zmenami “	A.5.28, A.8.15, A.8.16, A.8.17	116 (logy min. 12 mesiacov + integrita/prístup), 118–119 (monitoring nezvyčajného správania manuálne/automatizovane), 117 (obsah záznamov o činnostiach).

Porovnanie – príklad (2)

Nariadenie Komisie 2024/2690 (Príloha)	ISO 27001:2022	Položka V227/2025 (Príloha 1)
6.10 Riešenie zraniteľností a zverejňovanie informácií o nich „v prípade potreby v plánovaných intervaloch vykonávajú skenovanie zraniteľnosti a zaznamenávajú dôkazy o výsledkoch skenovania“ „stanovia postup na zverejňovanie informácií o zraniteľnostiach v súlade s platnou vnútroštátnou politikou koordinovaného zverejňovania informácií o zraniteľnostiach“	A.8.8	12–13 (informovanosť o hrozbách + získavanie info o zraniteľnostiach a mitigácia), 14–15 (pravidelné posudzovanie min 6m PKZS/12m PZS/OT + 16 priority aktualizácií), 17 (kontaktné údaje na nahlasovanie zraniteľností – pre určité kategórie). Chýba explicitná zmienka o CVD politike

Porovnanie štandardov

- **Nariadenie 2024/2690 aj Vyhláška 227/2025 (ich prílohy) predstavujú minimálne požiadavky uplatňované na základe analýzy rizík (možnosť neuplatnenia konkrétneho opatrenia so zdokumentovaným odôvodnením),**
- ISO 27001 je **komplexný ISMS katalóg**

- Oblasti kde Vyhláška 227/2025 je detailnejšia ako nariadenie 2024/2690 aj ISO 27001, sú napríklad:

a) **OT architektúra a segmentácie** (111–115),
b) **zálohovanie s konkrétnou metodikou a periodicitou** (28, 31–34),
c) **min. doba uchovávania logov je 12 mesiacov** (116),
d) **konkrétne opatrenia pre vzdialené relácie, OT relácie, monitoring rádiofrekvenčných zariadení** (108, 87)

- Z ISO 27001 nie sú vo vyhláške a nariadení výslovne spomenuté ako samostatné opatrenia napr. **data masking, DLP, web filtering, threat intelligence**.
- Pre nariadnenie 2024/2690 existuje Technická príručka pre implementáciu od ENISA

- Certifikácia ISO 27001 poskytuje regulovanému subjektu dobrý základ pre splnenie požiadaviek v oblasti kybernetickej bezpečnosti, ale nezaručuje úplný súlad s požiadavkami ZoKB/Vyhlášky 227/2025, alebo sektorových predpisov.

Technická príručka ENISA

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

COM(2026) 13 - Návrh smernice na zjednodušujúce opatrenia NIS2

- Dňa 20. januára 2026 Komisia zverejnila návrh smernice na zjednodušujúce opatrenia a zosúladenie s CSA 2.
- **Cesta k úplnej harmonizácia opatrení pre PZS**, ak Komisia vydá vykonávacie nariadenie pre všetky sektory (podobne ako už je Vykonávacie nariadenie2024/2690 pre vymedzené sektory)
- Článok 21 ods. 5 druhý pododsek sa nahrádza takto: „Komisia môže prijať **vykonávacie akty, ktorými sa stanovia technické a metodické požiadavky, ako aj sektorové požiadavky, v prípade potreby, na opatrenia uvedené v odseku 2, pokiaľ ide o kľúčové a dôležité subjekty iné ako tie**, ktoré sú uvedené v prvom pododseku tohto odseku. (pozn. iné ako subjekty v digitálnych sektoroch)"
- Návrh nového piateho pododsek v článku 21 smernice NIS2: „**Ak Komisia prijme vykonávacie akty** uvedené v prvom a druhom pododseku tohto odseku, členské štáty neuložia subjektom, na ktoré sa vzťahujú tieto vykonávacie akty, **žiadne ďalšie technické, metodické ani sektorové požiadavky týkajúce sa opatrení uvedených v článku 21 ods. 2** smernice (EÚ) 2022/2555."