

Bird & Bird

Prehľad kľúčových európskych právnych aktov pre kybernetickú bezpečnosť

4. apríla 2024

Katarína Ondrovičová



O čom budeme hovoriť?

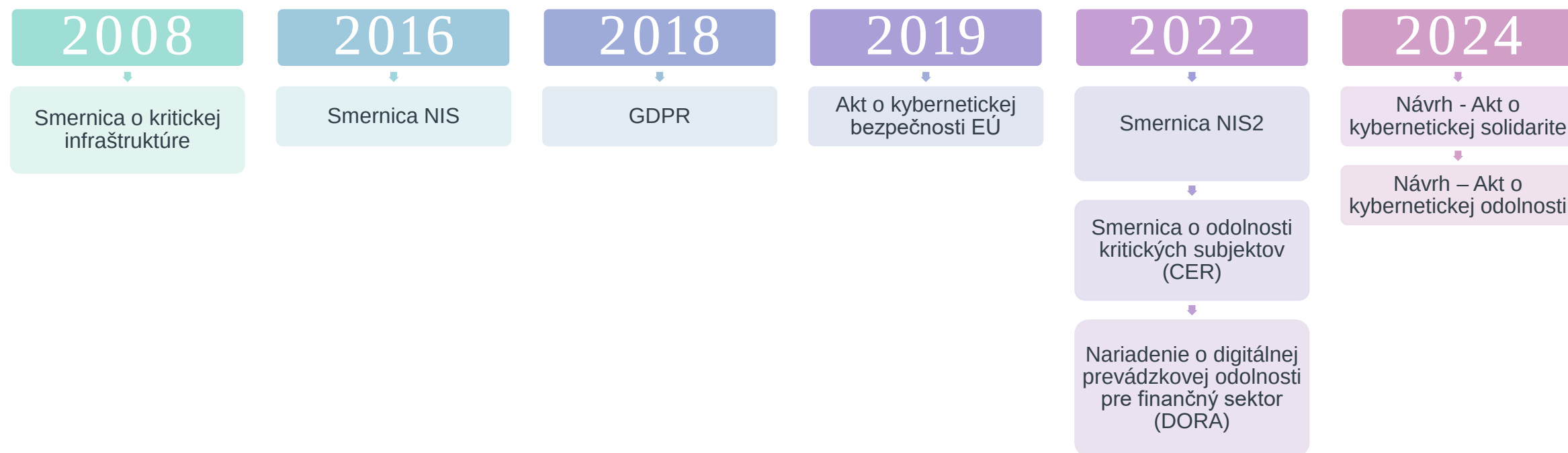
- | | |
|----|---------------------------------------|
| 01 | Stručný prehľad európskej legislatívy |
| 02 | NIS2 |
| 03 | Smernica CER |
| 04 | Ako sa pripraviť |

01

Stručný prehľad európskej legislatívy

Európske právne predpisy v oblasti kybernetickej bezpečnosti

Vývoj – stručný prehľad



Európska regulácia kybernetickej bezpečnosti



Smernica o odolnosti kritických subjektov (Smernica CER)

- dôraz na služby nevyhnutné pre zachovanie najdôležitejších spoločenských funkcií alebo hospodárskych činností



Smernica NIS2

- kyberbezpečnosť poskytovateľov regulovaných služieb



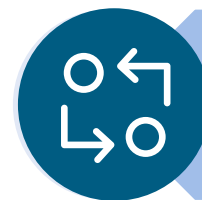
Nariadenie DORA

- odolnosť finančného sektora



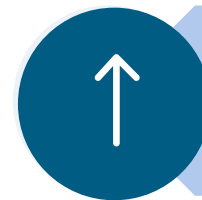
Akt o kyberbezpečnosti

- celoeurópske kyberbezpečnostné certifikačné mechanizmy



Cyber Solidarity Act (návrh)

- celoeurópske koordinácia v oblasti kyberbezpečnosti



Cyber Resilience Act (návrh)

- Nariadenie o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami



Ďalšie sektorové predpisy (návrh)



02

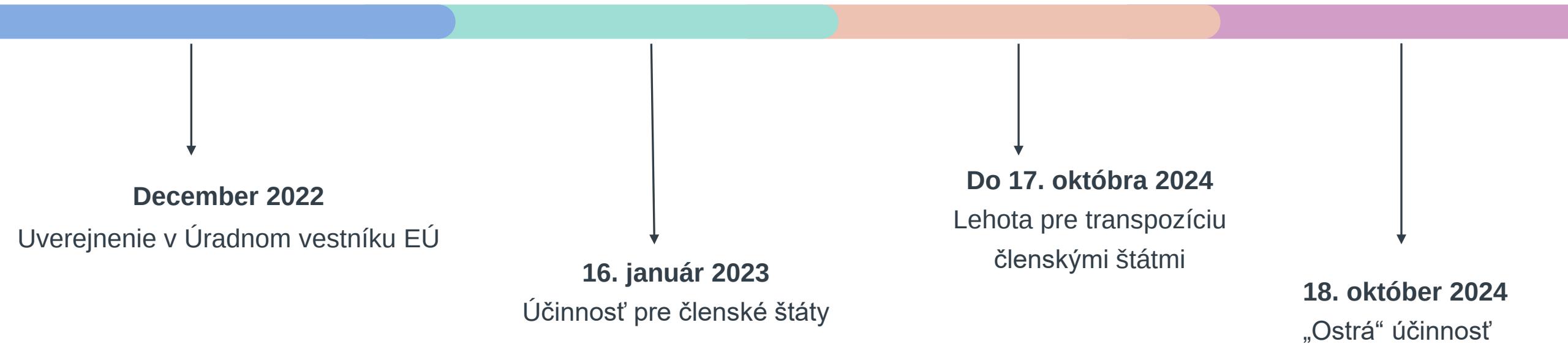
NIS2

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ)
2022/2555 zo 14. decembra 2022 o opatreniach na
zabezpečenie vysokej spoločnej úrovne kybernetickej
bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ)
č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica
(EÚ) 2016/1148 (smernica NIS 2)



Smernica NIS2

Vývoj



Súčasný stav a ďalšie kroky

Prebieha transpozícia a vnútroštátne odchýlky sú možné

Táto smernica **nebráni** členským štátom, aby prijali alebo ponechali v platnosti ustanovenia na zaistenie **vyššej úrovne kybernetickej bezpečnosti**, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únie.

Status	
	Adoption of the national implementing act
	Publication of the proposal
	Consultation phase
	No developments

NIS2 Directive



Smernica NIS2 – Cieľ:

*Vysoká spoločná úroveň kybernetickej bezpečnosti v EÚ
na účely lepšieho fungovania vnútorného trhu*

- Koordinovaný regulačný rámec
- Pravidlá spolupráce
- Aktualizovaný zoznam regulovaných odvetví
- Opatrenia na riadenie rizík KB
- Oznamovacie povinnosti

Smernica NIS2

Vysoká spoločná úroveň kybernetickej bezpečnosti v EÚ



Opatrenia

- Identifikácia rizík
- Predchádzanie incidentov
- Odhaľovanie, reakciu na incidenty
- Zotavenie, zmiernenie vplyvu

Opatrenia

- Primerané rizikám
- Zohľadniť technický vývoj
- Normy
- Certifikované IKT produkty, služby, procesy

Na koho sa vzťahuje NIS2 (1/4)

NIS2 upravuje a rozširuje organizácie, ktoré spadajú pod smernicu NIS

- **Odvetvia a pododvetvia** v Prílohe 1 (vysoká kritickosť) a prílohe 2 (iné kritické odvetvia)
 - **Pravidlo veľkosti:** do jeho pôsobnosti patria všetky stredné a veľké podniky
 - Určité subjekty bez ohľadu na veľkosť (NIS2, členský štát)
 - **Kľúčové a dôležité subjekty**
 - Kritické subjekty podľa smernice CER
 - Prevádzkovatelia základných služieb podľa NIS1 – ak štát označil
 - Do 17.4.2025 členské štáty vypracujú **zoznam**
 - Mechanizmy „samoregistrácie“
- 50 zamestnancov a
 - €10Mio ročný obrat/ celková ročná súvaha



Na koho sa vzťahuje NIS2 (2/4)

Kritické odvetvia a pododvetvia podľa NIS2



Verejná správa



Energetika



Výrobný priemysel



Potravinársky priemysel



Chemický priemysel



Vodné hospodárstvo



Odpadové hospodárstvo



Doprava



Digitálna infraštruktúra a služby



Finančný trh a bankovníctvo



Zdravotníctvo



Výskum



Poštové a kuriérske služby



Bezpečnosť



Vesmírny priemysel

Na koho sa vzťahuje NIS2 (3/4)

Digitálna infraštruktúra, služby a riadenie služieb IKT

NIS 2 – Digitálna infraštruktúra	z.č. 69/2019 Z.z.
poskytovatelia internetových prepojavacích uzlov	poskytovateľ služby výmenného uzla internetu na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené
poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov	poskytovateľ služieb systému doménových mien na internete
správcovia názvov TLD	subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne
poskytovatelia služieb cloud computingu	Digitálna služba
poskytovatelia služieb dátového centra	x
poskytovatelia sietí na prístupovanie obsahu	x
poskytovatelia dôveryhodných služieb	x
poskytovatelia verejných elektronických komunikačných sietí	Siete a služby pevných a mobilných EK, ktoré sú prvkom KI
poskytovatelia verejne dostupných elektronických komunikačných služieb	Siete a služby pevných a mobilných EK, ktoré sú prvkom KI
NIS 2 – Riadenie služieb IKT (medzi podnikmi)	
poskytovatelia riadených služieb	x
poskytovatelia riadených bezpečnostných služieb	x
NIS 2 - Poskytovatelia digitálnych služieb	
poskytovatelia online trhov	Digitálna služba
poskytovatelia internetových vyhľadávačov	Digitálna služba
poskytovatelia platforiem služieb sociálnej siete	x

Na koho sa vzťahuje NIS2 (4/4)

Príklad

„Poskytovateľ riadených služieb“

subjekt, ktorý poskytuje **služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou** produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov **formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku.**

„Poskytovateľ riadených bezpečnostných služieb“

poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík.



Cezhraničné poskytovanie služieb

Ktorá jurisdikcia bude relevantná?

Štát, v ktorom je subjekt usadený, neplatí pre:



Verejná správa:

Štát, ktorý zriadil
subjekt verejnej správy



PECS/PECN

Štát, v ktorom
poskytuje služby



Určité digitálne služby

Štát, v ktorom má
hlavnú prevádzkareň

ENISA - register

- poskytovatelia služieb DNS
- správcovia názvov TLD
- subjekty - služby registrácie názvov domén
- poskytovatelia služieb cloud computingu
- poskytovatelia služieb dátového centra
- poskytovatelia sietí na sprístupňovanie obsahu
- poskytovatelia riadených služieb
- poskytovatelia riadených bezpečnostných služieb
- poskytovatelia online trhov
- internetové vyhľadávače
- platformy služieb sociálnych sietí

Povinnosti subjektov

Opatrenia na riadenie kybernetických rizík

Opatrenia

- Technické, operačné, organizačné
- Zohľadniť všetky riziká a veľkosť subjektu, závažnosť, dosah, pravdepodobnosť ...

Cieľ

- chrániť siete, IS a fyzické prostredie
- prevencia a minimalizácia vplyvu incidentov

Analýza rizík

Riešenie incidentov

Ohlasovanie incidentov

Kontinuita činností

Bezpečnosť dodávateľského reťazca

Bezpečnosť sietí a IS pri nadobúdaní, vývoji, údržbe, riešenie zraniteľností

Posúdiť účinnosť opatrení

Odborná príprava, kybernetická hygiena

Bezpečnosť ľudských zdrojov

Postupy používanie kryptografie, šifrovania...

Riadiaci orgán:

- právomoc zabezpečiť dodržiavanie NIS2
- zodpovednosť za porušenie úlohy zabezpečiť dodržiavanie smernice
- dočasný zákaz vykonávať riadiace funkcie v subjekte

Povinnosti subjektov

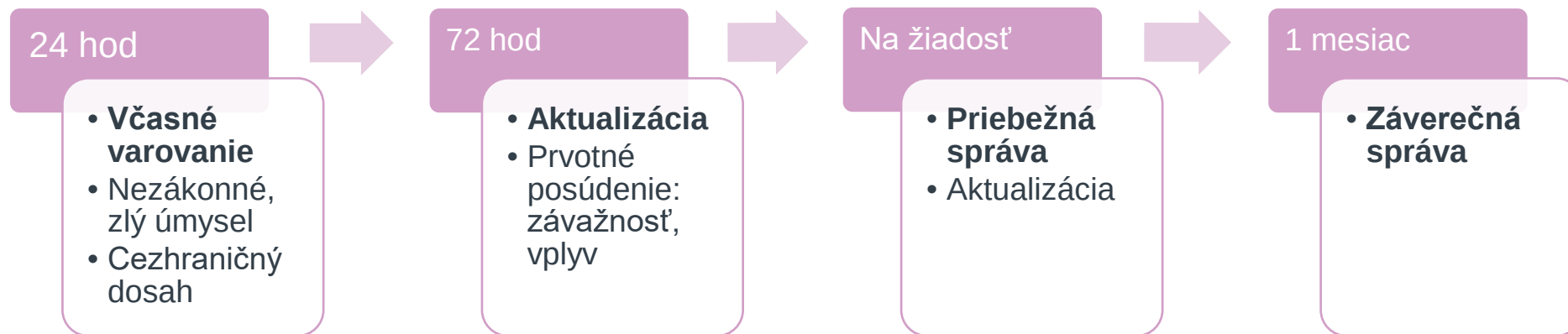
Notifikačné povinnosti

Významný incident:

- a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu **závažné prevádzkové narušenie služieb alebo finančnú stratu**;
- b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí **značnú majetkovú alebo nemajetkovú ujmu**.

CSIRT

- spätná väzba, usmernenia, pokyny
- cezhraničná spolupráca, ENISA
- informovanie verejnosť, OČTK



Členské štáty

Koordinované rámce kybernetickej bezpečnosti

- Národná stratégia KB
- Jednotné kontaktné miesto
- Orgány pre riadenie kyb. kríz
- CSIRT
- Koordinované zverejňovanie zraniteľností, databáza

Spolupráca

- Vnútroštátna
- Na úrovni EÚ:
 - Skupina pre spoluprácu
 - Sieť jednotiek CSIRT
 - EU-CyCLONE
- Medzinárodná

Dohľad a presadzovanie

- inšpekcie, kontroly
- audit - pravidelný / ad hoc
- žiadosti o informácie, dôkazy, údaje...
- zodpovednosť manažmentu
- pozastavenie certifikácie

POKUTY

- 10 Mio/2% - kľúčový subjekt
- 7Mio / 1,4% - dôležitý

03

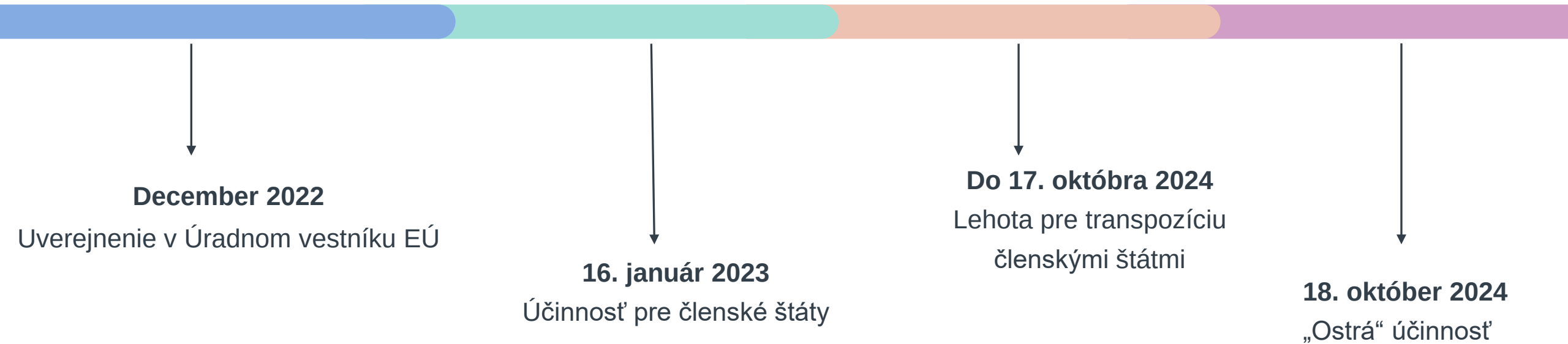
Smernica CER

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ)
2022/2557 zo 14. decembra 2022 o odolnosti kritických
subjektov a o zrušení smernice Rady 2008/114/ES



Smernica NIS2

Vývoj

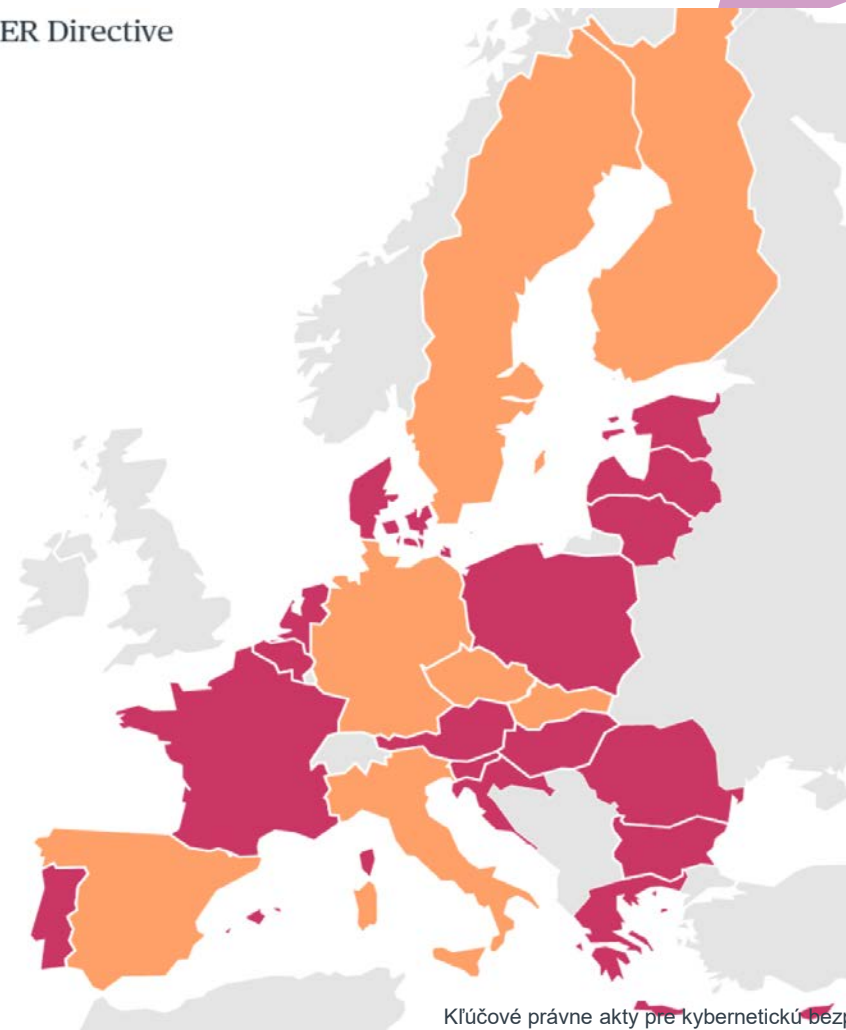


Súčasný stav a ďalšie kroky

Prebieha transpozícia a sú možné vnútroštátne odchýlky

Táto smernica nebráni členským štátom, aby prijali alebo ponechali v platnosti ustanovenia vnútroštátneho práva, ktorých cieľom je dosiahnuť **vyššiu úroveň odolnosti kritických subjektov**, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únie.

CER Directive





Smernica CER – Cieľ:

Nerušené poskytovanie základných služieb

- Povinnosti na zvýšenie odolnosti a schopnosti poskytovať služby nerušene
- Pravidlá spolupráce
- Pravidlá dohľadu a presadzovania
- Opatrenia na zvýšenie odolnosti,
- Oznamovacie povinnosti

Základná služba – zásadný význam z hľadiska zachovania životne dôležitých:

- spoločenských funkcií
- hospodárskych činností
- verejného zdravia a bezpečnosti alebo
- životného prostredia

Smernica CER - členské štáty

Cieľ: dosiahnuť a udržať vysokú úroveň odolnosti

Stratégia na zvýšenie odolnosti kritických subjektov

- ciele, priority na zvýš. odolnosti
- riadenie, úlohy, zodpovednosti
- opis opatrení na zvýšenie odolnosti
- opis posúdenia rizika
- opis procesu identifikácie KS
- rámce pre koordináciu, spoluprácu, zdieľanie informácií

Posúdenie rizika

- zohľadňujú všetky riziká:
 - prírodné, ľudská činnosť, nehody, katastrofy, ohrozenie verejného zdravia, terorizmus...
 - použijú na účely identifikácie kritických subjektov

Identifikácia kritických subjektov

- stratégia + posúdenie rizika
- odvetvia a pododvetvia v prílohe
 - základná služba
 - pôsobí a kritická infraštruktúra sa nachádza na území ČŠ
 - incident by mal **významne rušivé vplyvy na poskytovanie základných služieb** subjektu alebo iných základných služieb v sektoroch

Smernica CER

Súčinnosť so smernicou NIS2



Subjekty označené ako kritické subjekty podľa smernice CER sú kľúčovými subjektmi podľa NIS2!

Kritické subjekty (1/2)

Posúdenie rizík, ktoré môžu narušiť činnosť

Opatrenia na zabezpečenie ich odolnosti – plán odolnosti

Prevenia incidentov

opatrenia na zníženie
rizika katastrof a
prispôsobenie sa
zmene klímy

Primeraná fyzická ochrana

oplotenie, bariéry,
nástroje a postupy
monitorovania
bezpečnostnej zóny,
detekčné zariadenia
a kontroly prístupu

Bezpečnosť dodávateľského reťazca

Primerané riadenie bezpečnosti ľudských zdrojov

Určenie - kritické
funkcie, prístupové
práva, previerky,
odborná príprava,
školenia, cvičenia

Kritické subjekty (2/2)

Posúdenie rizík, ktoré môžu narušiť činnosť

Opatrenia na zabezpečenie ich odolnosti – Plán odolnosti

Odolnosť voči incidentom - reakcia a zmiernenie ich následkov

vykonávanie postupov a
protokolov riadenia rizík a
krízového riadenia a
výstražné varovania

Zotavenie z incidentov

BCP a identifikácia
alternatívnych
dodávateľských
reťazcov, plynulé
obnovenie služby

Oznamovanie incidentov

- bez zbytočného odkladu, max. 24hod.
- 1M – podrobná správa
- Komisii – vplyv na kontinuitu ZS vo viac štátoch

Styčný úradník pre kontakt s príslušnými orgánmi

Presadzovanie CER

Vnútroštátna úprava

- **Kontroly a inšpekcie** na mieste v priestoroch využívaných na poskytovanie základných služieb,
- Dohľad nad opatreniami odolnosti kritických subjektov,
- **Audity**
- Právo požadovať príslušné **informácie a dôkazy**
- **Príkazy** na prijatie potrebných a primeraných opatrení na nápravu zisteného porušenia a na poskytnutie informácií o prijatých opatreniach
- **Spolupráca** s orgánmi dohľadu podľa NIS2
- **Sankcie**
 - Sankcie vo vnútroštátnych právnych predpisoch
 - Sankcie musia byť účinné, primerané a odrádzajúce

04

Ako sa pripravit' na NIS2 a CER

Ako sa pripraviť na NIS2 (a CER)

Analýza uplatniteľnosti

Monitorovať implementáciu a pochopenie požiadaviek právnej úpravy

GAP analýza a odstránenie nedostatkov

Dodržiavanie súladu
Monitorovanie a reagovanie (nielen) na nové riziká

Zabezpečenie konzistentnosti v rôznych oblastiach
(IT zmluvy, ochrana osobných údajov, sektorové predpisy).

Ako sa pripraviť na NIS2 (a CER)

Určiť

- Služby/produkty a subjekty v rozsahu pôsobnosti
- Jurisdikcie
- GAP analýza
- Následné opatrenia

Aktualizácia

- Smernice a postupy
- Plány reakcie na incidenty
- Školenia
- Dodávateľský reťazec

Správa záväzkov

- Zmluvy so zákazníkmi, predajcami atď.
- Riziko na úrovni riadenia
- Vzťahy s regulačnými orgánmi

Udržiavať

- Monitoring
- Primerané riadenie
- Súčinnosť s inými právnymi predpismi



Katarína Ondrovičová

Senior Associate

katarina.ondrovicova@twobirds.com

twobirds.com

Abú Dabí • Amsterdam • Bratislava • Brusel • Budapešť • Casablanca • Kodaň • Dubaj • Düsseldorf • Frankfurt
• Haag • Hamburg • Helsinki • Hong Kong • Londýn • Lyon • Madrid • Miláno • Mníchov • Paríž • Peking
• Praha • Rím • San Francisco • Šanghai • Šen-čen • Singapur • Štokholm • Sydney • Varšava

Bird & Bird je medzinárodná advokátska kancelária skladajúca sa z Bird & Bird LLP a jej pobočiek a pridružených zastúpení.

Bird & Bird LLP je registrované v Anglicku a Walse pod registračným číslom OC340318 a je regulované SRA – Regulačnou autoritou. Jej sídlom a miestom podnikania je 12 New Fetter Lane, Londýn, EC4A 1JP. Zoznam členov skupiny Bird & Bird LLP a nečlenov, ktorí sú vymenovaní za partnerov a ich príslušné odborné kvalifikácie, sú k dispozícii k nahliadnutiu na tejto adrese.