

OSOBNÁ PÔSOBNOSŤ SMERNICE NIS 2 A JEJ TRANSPÓZÍCIA DO PRÁVNÝCH PORIADKOV VYBRANÝCH ČLENSKÝCH ŠTÁTOV EÚ¹

doc. JUDr. Jozef Andraško, PhD.

Univerzita Komenského v Bratislave, Právnická fakulta
Ústav práva informačných technológií a práva duševného vlastníctva
jozef.andrasko@flaw.uniba.sk

JUDr. Nataša Brabcová, LL.M., MBA

Akadémia Policajného zboru v Bratislave
Katedra verejnoprávnych vied
natasa.brabcova@akademiapz.sk

Osobná pôsobnosť smernice NIS 2 a jej transpozícia do právnych poriadkov vybraných členských štátov EÚ

Nová právna úprava kybernetickej bezpečnosti v podobe smernice NIS 2 predstavuje druhý pokus v otázke harmonizácie oblasti kybernetickej bezpečnosti v Európskej únii. Prvý legislatívny akt v podobe smernice NIS aj z dôvodu nesprávnej transpozície v otázkach osobnej pôsobnosti nenaplnil základný cieľ regulátora, ktorým bolo dosiahnuť harmonizáciu v tejto oblasti. Autori v predkladanom príspevku analyzujú smernicu NIS 2 v kontexte osobnej pôsobnosti. Konkrétne bude analyzované, akým spôsobom sa nová regulácia vzťahuje na regulované subjekty vo všeobecnosti a špecificky na subjekty verejnej správy a subjekty v oblasti vzdelávania. Analýze bude taktiež podrobená právna úprava kybernetickej bezpečnosti dvoch členských štátov Európskej únie, ktoré už transponovali smernicu NIS 2, konkrétne Chorvátsko a Belgicko.

¹ Tento článok bol podporený Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-23-0137 - Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti.

Personal Scope of the NIS 2 Directive and its Transposition into the Legal Systems of Selected EU Member States

The new cyber security legislation known as NIS 2 Directive is the second attempt to harmonize the area of cyber security in the European Union. The first legislative act, the NIS Directive, did not achieve the regulator's basic objective of harmonization in this area, partly due to incorrect transposition regarding personal scope. In this contribution, the authors analyze the NIS 2 directive in the context of personal scope. In particular, the analysis will focus on how the new regulation applies to regulated entities in general, including public administration entities and those in the field of education. The cyber security legislation of two states that have already transposed the NIS 2 Directive, namely Croatia and Belgium, will also be analyzed.

Kľúčové slová: smernica NIS 2, osobná pôsobnosť, subjekty verejnej správy

Key words: NIS 2 Directive, personal scope, public administration entities

<https://doi.org/10.62874/afi.2024.2.01>

Úvod

Prvým horizontálnym legislatívnym aktom v oblasti kybernetickej bezpečnosti na úrovni práva Európskej únie (ďalej len „EÚ“) bola smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „**smernica NIS**“).² Avšak aplikačná prax, ako aj závery Komisie poukázali na to, že cieľ smernice NIS, a teda dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci EÚ, sa nepodarilo naplniť. Pravidelný prieskum smernice NIS³ ukázal viaceré nedostatky tejto právnej úpravy a bol zároveň aj základom pre vypracovanie znenia návrhu

² K smernici NIS pozri: MARKOPOULOU, D. a kol. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review*, Volume 35, Issue 6, 2019. DUCUING, Ch. Understanding the rule of prevalence in the NIS directive: C-ITS as a case study, *Computer Law & Security Review*, Volume 40, 2021.

³ Príloha č. 6, EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final.*

smernice NIS 2. Z daného posúdenia vyplýva niekoľko oblastí, ktoré ukázali najvyššiu mieru nedostatočnosti. V prvom rade bola konštatovaná nedostatočná prepojenosť požiadaviek smernice NIS pre jednotlivé sektory (odvetvia)⁴. Ako jasný príklad nejednotnosti v oblasti (osobnej) pôsobnosti smernice NIS uvádza Komisia prípad poskytovateľov zdravotnej starostlivosti, ktorí v niektorých členských štátoch EÚ patria do rozsahu implementácie smernice NIS a podliehajú bezpečnostným a organizačným požiadavkám na kybernetickú bezpečnosť a naopak, v niektorých členských štátoch týmto požiadavkám musia prispôbiť procesy iba väčšie nemocnice. Podobná situácia nastala aj v prípade železničných prevádzkovateľov. Zatiaľ čo veľký európsky železničný prevádzkovateľ je zahrnutý do rozsahu pôsobnosti smernice NIS v jednom veľkom členskom štáte, na iného veľkého železničného prevádzkovateľa v inom veľkom členskom štáte sa bezpečnostné požiadavky smernice NIS nevzťahujú.⁵

Ďalej bolo konštatované nejasné vymedzenie pôsobnosti smernice a nejasné vymedzenie kompetencií národných dozorných autorít. V tejto súvislosti Komisia kritizovala odlišné kritéria pre identifikáciu poskytovateľov základných služieb naprieč členskými štátmi. Odlišnosť pri ich identifikovaní preto spôsobuje, že rovnaké entity v konkrétnom sektore podliehajú prísnejším opatreniam v jednom členskom štáte EÚ ako v ostatných. Tento prístup má za následok odlišnú implementáciu smernice NIS a fragmentáciu právneho rámca kybernetickej bezpečnosti. Problémom je aj zároveň nedostatočná informovanosť autorít v členských štátoch ohľadne svojich kompetencií voči prevádzkovateľom základných služieb.⁶

Taktiež boli identifikované odlišné bezpečnostné a notifikačné povinnosti naprieč členskými štátmi. Smernica NIS poskytla pomerne veľkú mieru slobody pri určovaní špecifik nahlasovania bezpečnostných incidentov. Členské štáty preto rozdielne pristúpili k otázkam, ktoré bezpečnostné incidenty je potrebné nahlásiť a v akej lehote. Tento

⁴ V texte článku sú pojmy sektor a odvetvie považované za synonymá.

⁵ EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. Brusel, 16.12.2020 SWD(2020) 345 final, s. 11.

⁶ Tamže, s. 15. K rovnakému záveru došla Európska Komisia vo svojej Správe o posúdení jednotnosti prístupov členských štátov pri identifikácii prevádzkovateľov základných služieb v súlade s článkom 23 ods. 1 smernice 2016/1148/EÚ o bezpečnosti sietí a informačných systémov. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52019DC0546>, cit. 2024-09-20.

prístup má za následok odlišnú implementáciu smernice NIS a fragmentáciu právneho rámca kybernetickej bezpečnosti.⁷

Z vyššie uvedených dôvodov sa pristúpilo k tvorbe nového legislatívneho aktu, ktorý by nahradil smernicu NIS. Návrh smernice NIS 2 bol 10. 11. 2022 schválený Európskym parlamentom⁸ a 28.11.2022 Radou Európskej únie.⁹ 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 (ďalej len „**smernica NIS 2**“) bola 27.12.2022 zverejnená v Úradnom vestníku Európskej únie a dvadsiatym dňom po tomto uverejnení nadobudla účinnosť. Členské štáty boli povinné transponovať smernicu do vnútroštátnych právnych predpisov do 17. 10. 2024.¹⁰

Cieľom predkladaného príspevku je analyzovať smernicu NIS 2 v kontexte zmien týkajúcich sa osobnej pôsobnosti. Špecificky bude analyzované, akým spôsobom sa nová regulácia vzťahuje na subjekty verejnej správy a subjekty v oblasti vzdelávania. Analýza bude podrobená aj kritickému pohľadu, ktorý by mal reflektovať základnú otázku či je smernica NIS 2 v porovnaní so smernicou NIS lepším harmonizačným právnym nástrojom v kontexte osobnej pôsobnosti. Autori si taktiež kladú za cieľ poukázať na stav transpozície predmetnej smernice vo vybraných členských štátoch EÚ, najmä v kontexte osobnej pôsobnosti. Analýze bude podrobená právna úprava kybernetickej bezpečnosti dvoch štátov, ktoré už transponovali smernicu NIS 2, konkrétne Chorvátsko a Belgicko.

⁷ Tamže. Ako ďalšie oblasti boli identifikované: nedostatočne efektívny dohľad a vymáhanie; neporovnateľné prerozdelenie financií pri otázkach kybernetickej bezpečnosti naprieč členskými štátmi; limitované zdieľanie informácií medzi členskými štátmi.

⁸ Cybersecurity. Parliament adopts new law to strengthen EU-wide resilience. Dostupné na: https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience_, cit. 2024-09-20.

⁹ EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. Dostupné na: <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/>, cit. 2024-09-20.

¹⁰ Smernica NIS 2, čl. 41 ods. 1.

1. Pôsobnosť smernice NIS 2

Smernica NIS 2 prináša zásadnú zmenu v otázke **rozsahu (osobnej) pôsobnosti**. Identifikácia prevádzkovateľov základnej služby a rozlišovanie medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb v zmysle smernice NIS sa ukázalo ako zastarané, pretože neodráža význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.¹¹

Subjekty, ktoré patria do rozsahu pôsobnosti smernice NIS 2 sa rozdeľujú do dvoch kategórií:

- **klúčové subjekty** (*essential entities*) a
- **dôležité subjekty** (*important entities*).

Klúčové a dôležité subjekty musia byť subjekty typu uvedeného v prílohe I alebo prílohe II. V **prílohe I** s názvom „**Odvetvia s vysokou úrovňou kritickosti**“ sú uvedené nasledujúce odvetvia: energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, pitná voda, odpadová voda, digitálna infraštruktúra, riadenie služieb IKT (medzi podnikmi), verejná správa a vesmír.

V **prílohe II** s názvom „**Iné kritické odvetvia**“ sú zadefinované nasledujúce odvetvia: poštové a kuriérske služby; odpadové hospodárstvo; výroba a distribúcia chemických látok; výroba, spracovanie a distribúcia potravín; výroba; poskytovatelia digitálnych služieb a výskum.

Na klúčové aj dôležité subjekty by sa mali vzťahovať rovnaké požiadavky na riadenie rizík a oznamovacie povinnosti. V prípade dohľadu a sankcií sa však na tieto dve kategórie subjektov neuplatňujú rovnaké ustanovenia.

1.1 Pravidlo obmedzenia veľkosti

Smernica NIS 2 neukladá členským štátom povinnosť identifikovať subjekty, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb („proces identifikácie“), tak ako to je upravené v smernici NIS. Namiesto toho sa v smernici NIS 2 stanovilo jednotné

¹¹ Smernica NIS 2, recitál 6. Bližšie k porovnaniu smernice NIS a smernice NIS 2 pozri VANDEZANDE, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. In *Computer Law & Security Review*, Volume 52, 2024 a SIEVERS, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *Int. Cybersecur. Law Rev.* 2, 2021, s. 223–231.

kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice.¹²

Toto kritérium spočíva v uplatňovaní **pravidla obmedzenia veľkosti** (*size-cap rule*), podľa ktorého sa smernica NIS 2 vzťahuje na všetky verejné alebo súkromné subjekty, ktoré sa považujú za **stredné podniky** podľa článku 2 prílohy k odporúčaniam Komisie zo 6. mája 2003 o definícii mikro, malých a stredných podnikov (oznámené pod číslom dokumentu C (2003) 1422) (2003/361/ES) (ďalej len „**odporúčanie Komisie**“), alebo ktoré **presahujú limity pre stredné podniky** stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v EÚ.¹³ Podniky presahujúce limity pre stredné podniky možno označiť za veľké podniky.

Odporúčanie Komisie definuje **stredné podniky** ako podniky, ktoré zamestnávajú menej ako 250 osôb a ktoré majú buď ročný obrat nepresahujúci 50 miliónov eur, alebo ročnú bilančnú sumu neprevyšujúcu 43 miliónov eur. V kontexte ukazovateľov pre ďalšie subjekty (malé podniky, mikropodniky) upravených v odporúčaní Komisie možno konštatovať, že za stredné podniky sa považujú podniky, ktoré zamestnávajú 50 až 249 osôb, s ročným obratom prevyšujúcim 10 miliónov EUR až do 50 miliónov EUR alebo ročnou bilančnou sumou prevyšujúcou 10 miliónov EUR až do 43 miliónov EUR.

Za **veľké podniky** sa považujú podniky, ktoré zamestnávajú 250 a viac osôb a ktoré majú buď ročný obrat prevyšujúci 50 miliónov eur, alebo ročnú bilančnú sumu prevyšujúcu 43 miliónov eur.

V zmysle odporúčania Komisie sa základný **počet pracovníkov** vyjadruje v **ročných pracovných jednotkách**. Osoby, ktoré v rámci podniku alebo v jeho mene pracovali na plný pracovný čas počas celého referenčného roka, sa považujú za jednu jednotku. Pracovníci na kratší pracovný čas, sezónni pracovníci a osoby, ktoré nepracovali celý rok, sa započítavajú ako zlomky jednej jednotky.¹⁴

Pre úplnosť je potrebné dodať, že v situáciách, ktoré zahŕňajú „partnerské“ alebo „prepojené“ podniky, sa na výpočet veľkosti musí vykonať pomerná konsolidácia údajov (ročné pracovné jednotky a obrat alebo bilančná suma) príslušného subjektu a iných subjektov.¹⁵

¹² Smernica NIS 2, recitál 7.

¹³ Smernica NIS 2, čl. 2 ods. 1 a recitál 7.

¹⁴ EURÓPSKA KOMISIA. Príručka pre používateľov k definícii MSP. 2019, s. 13. Dostupné na: <https://op.europa.eu/sk/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1>, cit. 2024-09-20.

¹⁵ Tamže, s. 18 - 23.

1.2 Výnimka z pravidla obmedzenia veľkosti

Zo všeobecného pravidla obmedzenia veľkosti existujú v zmysle smernice NIS 2 aj **výnimky**.

Určité malé podniky a mikropodniky, ktoré spĺňajú osobitné kritériá, ktoré naznačujú kľúčovú úlohu pre spoločnosť, hospodárstvo alebo pre určité odvetvia alebo druhy služieb, patria do rozsahu pôsobnosti smernice NIS 2.¹⁶ V tejto súvislosti možno konštatovať, že v osobitných prípadoch uvedených v smernici NIS 2 sa bude smernica NIS 2 vzťahovať aj na mikropodniky a malé podniky.

Odporúčanie Komisie 2003/361/ES definuje mikropodniky a malé podniky nasledovne:

*„Mikropodniky sa definujú ako podniky, ktoré zamestnávajú **menej ako 10 osôb** a ktorých ročný obrat alebo ročná bilančná suma nepresahuje **2 milióny eur**.“*

*„Malé podniky sa definujú ako podniky, ktoré zamestnávajú **menej ako 50 osôb** a ktorých ročný obrat alebo ročná bilančná suma nepresahuje **10 miliónov eur**.“*

Z vyššie uvedených definícií vyplýva, že pre posúdenie veľkosti subjektu v zmysle spomínaného odporúčania musí byť naplnený zamestnanecký, ako aj finančný ukazovateľ (ročný obrat alebo ročná bilančná suma). Avšak v prípade finančných ukazovateľov sa daný subjekt môže rozhodnúť, či bude spĺňať maximálnu hodnotu stanovenú pre obrat alebo maximálnu hodnotu stanovenú pre bilančnú sumu. Subjekt nemusí spĺňať obe požiadavky, pričom jednu z nich môže aj presiahnuť bez toho, aby to malo vplyv na jeho postavenie mikro, malého alebo stredného podniku.¹⁷

¹⁶ Smernica NIS 2, recitál 7.

¹⁷ Národný úrad pro kybernetickou a informační bezpečnost (ďalej len „NÚKIB“) uvádza vo svojom factsheetu pre posúdenie veľkosti subjektov nasledujúce príklady:

Príklad č.1: Podnik so 60 ročnými pracovnými jednotkami, ročným obratom 9 miliónov EUR a ročnou bilančnou sumou 9 miliónov EUR. Podnik bude považovaný za stredný, pretože presiahol zamestnanecký strop pre malé podniky.

Príklad č. 2: Podnik so 49 ročnými pracovnými jednotkami, ročným obratom 12 miliónov EUR a ročnou bilančnou sumou 8 miliónov EUR. Podnik bude považovaný za malý. Aj napriek prekročeniu stropu pre ročný obrat sa môže podnik posudzovať podľa ročnej bilančnej sumy, ktorá do stropov pre malé podniky spadá.

Príklad č. 3: Podnik s 8 zamestnancami, ročným obratom 30 miliónov EUR a ročnou bilančnou sumou 15 miliónov EUR. Podnik bude považovaný za stredný, pretože oba finančné ukazovatele presahujú hodnotu 10 miliónov EUR. Dostupné na: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>, cit. 2024-09-21.

Pre doplnenie je potrebné uviesť, že za podnik sa považuje: „každý subjekt, ktorý vykonáva hospodársku činnosť, bez ohľadu na jeho právnu formu“.¹⁸ Určujúcim faktorom nie je právna forma ale hospodárska činnosť. V praxi to znamená, že za podnik sa môžu považovať samostatne zárobkovo činné osoby, rodinné firmy, partnerstvá a združenia alebo akékoľvek iné subjekty, ktoré pravidelne vykonávajú hospodársku činnosť. Za hospodársku činnosť sa zvyčajne považuje: „predaj výrobkov alebo služieb za stanovenú cenu na určitom/priamom trhu“.¹⁹

Smernica NIS 2 sa vzťahuje na subjekty, typu uvedeného v prílohe I alebo prílohe II **bez ohľadu na ich veľkosť** keď:²⁰

- a) služby poskytujú:
 - poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb;
 - poskytovatelia dôveryhodných služieb;
 - registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén;
- b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;
- c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;
- d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;
- e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;
- f) subjekt je subjektom verejnej správy:
 - v ústrednej štátnej správe podľa definície členského štátu v súlade s vnútroštátnym právom; alebo
 - na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, ktorý po posúdení na základe rizík

¹⁸ EURÓPSKA KOMISIA. Príručka pre používateľov k definícii MSP. 2019, s. 10 - 11. Dostupné na: <https://op.europa.eu/sk/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1>, cit. 2024-09-20.

¹⁹ Tamže, s. 9.

²⁰ Smernica NIS 2, čl. 2 ods. 2.

poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

Smernica NIS 2 sa taktiež vzťahuje na subjekty identifikované ako **kritické subjekty** podľa smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (ďalej len „smernica o odolnosti kritických subjektov“) bez ohľadu na ich veľkosť a subjekty poskytujúce služby registrácie názvov domén bez ohľadu na ich veľkosť.²¹

Členské štáty môžu ustanoviť, že sa smernica NIS 2 vzťahuje na:²²

- a) subjekty verejnej správy na miestnej úrovni;
- b) vzdelávacie inštitúcie, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti.

V kontexte vyššie uvedeného možno konštatovať, že bude závisieť od členského štátu či sa medzi subjekty verejnej správy budú zaradiť len subjekty verejnej správy v ústrednej štátnej správe a regionálnej úrovni, alebo sa rozsah pôsobnosti rozšíri aj na subjekty verejnej správy na miestnej úrovni a vzdelávacie inštitúcie.

1.3 Negatívna pôsobnosť

Smernica NIS 2 sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov. Avšak, subjekty verejnej správy, ktorých činnosti s uvedenými oblasťami súvisia len okrajovo, by však nemali byť vylúčené z rozsahu pôsobnosti smernice NIS2.²³

Členské štáty môžu vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, alebo ktoré poskytujú služby výhradne subjektom verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva, v súvislosti s danými činnosťami alebo službami z povinností stanovených v článku 21 alebo článku 23 smernice NIS 2.²⁴

²¹ Smernica NIS 2, čl. 2 ods. 3 a 4.

²² Smernica NIS 2, čl. 2 ods. 5.

²³ Smernica NIS 2, čl. 2 ods. 7 a recitál 8.

²⁴ Smernica NIS 2, čl. 2 ods. 8.

Smernica NIS 2 sa taktiež nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 (DORA) v súlade s článkom 2 ods. 4 uvedeného nariadenia.²⁵

1.4 Kľúčové a dôležité subjekty

Ako už bolo vyššie spomínané, smernica NIS 2 už nerozlišuje medzi hospodárskymi subjektami prevádzkovateľ základnej služby a poskytovateľa digitálnej služby, tak ako to bolo v prípade smernice NIS ale zavádza nové druhy subjektov, ktorými sú kľúčové subjekty a dôležité subjekty. Za **kľúčové subjekty** sa považujú:²⁶

- a) subjekty typu uvedeného v prílohe I, ktoré presahujú limity pre stredné podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniam 2003/361/ES;
- b) kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne, ako aj poskytovatelia služieb DNS, bez ohľadu na ich veľkosť;
- c) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky podľa článku 2 prílohy k odporúčaniam 2003/361/ES;
- d) subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i);
- e) akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e);
- f) subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice;
- g) ak tak členský štát ustanoví, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom.

Subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 článku 3 smernice NIS 2, sa považujú za **dôležité subjekty**. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e) smernice NIS 2.²⁷

²⁵ Smernica NIS 2, čl. 2 ods. 10.

²⁶ Smernica NIS 2, čl. 3 ods. 1.

²⁷ Smernica NIS 2, čl. 3 ods. 2.

Do 17. apríla 2025 vypracujú členské štáty **zoznam kľúčových a dôležitých subjektov** ako aj subjektov poskytujúcich služby registrácie názvov domén. Členské štáty tento zoznam pravidelne prehodnocujú a podľa potreby aktualizujú najmenej každé dva roky po uvedenom dátume.²⁸

Na účely zostavenia zoznamu kľúčových a dôležitých subjektov členské štáty požadujú od týchto subjektov, aby príslušným orgánom predložili aspoň tieto informácie:²⁹

- a) názov subjektu;
- b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, IP adries a telefónnych čísel;
- c) podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohe I alebo II; a
- d) prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.

Kľúčové a dôležité subjekty bezodkladne a v každom prípade do dvoch týždňov odo dňa zmeny oznámia akékoľvek zmeny zasielaných údajov zasielaných.³⁰

Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) bez zbytočného odkladu poskytne usmernenia a vzory súvisiace s povinnosťami týkajúcich sa vytvorenia zoznamu, predloženia konkrétnych informácií či oznamovania zmien zasielaných údajov.³¹ Predmetné usmernenia a vzory sú obsiahnuté v **Usmernení Komisie k uplatňovaniu článku 3 ods. 4 smernice (EÚ) 2022/2555 (smernica NIS 2)**.³²

Členské štáty môžu zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa kľúčové a dôležité subjekty mohli zaregistrovať samé.³³

²⁸ Smernica NIS 2, čl. 3 ods. 3.

²⁹ Smernica NIS 2, čl. 3 ods. 4.

³⁰ Smernica NIS 2, čl. 3 ods. 4.

³¹ Smernica NIS 2, čl. 3 ods. 4.

³² Oznámenie Komisie Usmernenia Komisie k uplatňovaniu článku 3 ods. 4 smernice (EÚ) 2022/2555 (smernica NIS 2) 2023/C 324/02. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1716636475611&uri=CELEX%3A52023XC0914%2801%29>, cit. 2024-09-20.

³³ Smernica NIS 2, čl. 3 ods. 4.

2. Subjekty verejnej správy a odvetvie „Verejná správa“

V porovnaní so smernicou NIS sa smernica NIS 2 bude vzťahovať aj na konkrétne subjekty v rámci odvetvia „Verejná správa“.

Subjekt verejnej správy je legálne definovaný v článku 6 bod 35 smernice NIS 2. V zmysle smernice NIS 2 je subjekt verejnej správy: *„subjekt, ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom, okrem súdnicstva, parlamentov a centrálnych bánk, a ktorý spĺňa tieto kritériá:*

- a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;
- b) má právnu subjektivitu alebo je zo zákona oprávnený konať v mene iného subjektu s právnou subjektivitou;
- c) je financovaný prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojim riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;
- d) má právomoc vydávať fyzickým alebo právnickým osobám správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu;“

V zmysle legálnej definície nemôže ísť o subjekty komerčného alebo priemyselného charakteru, to znamená, že musia plniť úlohy verejného alebo všeobecného záujmu. Zároveň, musia disponovať právnou subjektivitou alternatívne mať zákonom stanovené oprávnenie konať v mene iného subjektu s právnou subjektivitou. Tretia podmienka pre subjekty verejnej správy je ustanovená alternatívne a týka sa financovania štátom alebo dohľadu vykonávaného štátom. Štvrtá podmienka sa týka vydávania správnych alebo regulačných rozhodnutí, ktoré majú vplyv na práva pri cezhraničnom pohybe osôb, tovarov, služieb a kapitálu. Požiadavky vplyvu na práva pri pohybe osôb, tovarov, služieb a kapitálu reflektuje pôsobnosť EÚ v oblasti jednotného vnútorného trhu. Požiadavku pre cezhraničný aspekt je potrebné vnímať v tom kontexte, že ide o pohyb v rámci jednotlivých členských štátoch EÚ. Nasvedčuje tomu aj legálna definícia pojmu „cezhraničné spracúvanie“ podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica

95/46/ES (všeobecné nariadenie o ochrane údajov), v zmysle ktorého je cezhraničné spracúvanie také „*spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte.*“³⁴ Takémuto výkladu nasvedčuje aj recitál 4 smernice NIS 2, v zmysle ktorého: „*Požiadavky na kybernetickú bezpečnosť uložené subjektom poskytujúcim služby alebo vykonávajúcim činnosti, ktoré sú ekonomicky významné, sa v jednotlivých členských štátoch značne líšia, pokiaľ ide o typ požiadaviek, ich úroveň podrobnosti a metódu dohľadu. Uvedené rozdiely spôsobujú dodatočné náklady a subjektom, ktoré ponúkajú tovar alebo služby cezhranične, spôsobujú ťažkosti. Požiadavky jedného členského štátu, ktoré sa líšia od požiadaviek iného členského štátu alebo sú s nimi dokonca v rozpore, môžu takéto cezhraničné činnosti podstatne ovplyvniť.*“

V prípade vyššie uvedených kritérií pre pojem subjekt verejnej správy ide o **kumulatívne kritériá**, čo znamená, že musia byť splnené všetky kritériá.

Taktiež je potrebné dodať, že hoci sa vylučujú z pojmu subjekt verejnej správy subjekty zo súdnictva, parlamentov a centrálnych bánk, nie je vylúčené, aby sa právna úprava vzťahovala napr. na Kanceláriu Národnej rady Slovenskej republiky, Kanceláriu Najvyššieho súdu Slovenskej republiky či Kanceláriu Ústavného súdu Slovenskej republiky.

Ako už bolo objasnené v predchádzajúcich častiach článku, v smernici NIS 2 sa aplikuje pravidlo obmedzenia veľkosti, čo znamená, že smernica sa vzťahuje na verejné alebo súkromné subjekty typu uvedeného v prílohe I alebo II, ktoré sa považujú za stredné podniky alebo presahujú limity pre stredné podniky. V prílohe I sú pre odvetvie „Verejná správa“ uvedené nasledujúce typy subjektov:

- a) subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom,
- b) subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom.

Pojem ústredná štátna správa sa spomína napr. v Správe o hodnotení vplyvu.³⁵ Ide napr. o správne orgány štátu (*administrative departments*

³⁴ Všeobecné nariadenie o ochrane údajov, čl. 4, bod 23 písm. a).

³⁵ EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final.*

of the state) a ďalšie ústredné orgány (*central agencies*), ktorých pôsobnosť pokrýva celé ekonomické územie krajiny (*whose responsibilities cover the whole economic territory of a country*).³⁶

V prípade ustanovenia čl. 2 ods. 2 smernice NIS 2, ktoré upravuje výnimky z pravidla obmedzenia veľkosti, možno v súvislosti so subjektami verejnej správy na regionálnej úrovni vidieť aj ďalšie požiadavky, ktoré v prílohe I v odvetví „Verejná správa“ nie sú pre subjekty verejnej správy na regionálnej úrovni uvedené. V zmysle ustanovenia čl. 2 ods. 2 písm. f) bod ii sa smernice NIS 2 vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak subjekt je subjektom verejnej správy na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, **ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti**. V prípade subjektov verejnej správy na regionálnej úrovni uvedených v predmetnom ustanovení sa v porovnaní s typom subjektu v prílohe I v odvetví Verejná správa navyše vyžaduje, aby išlo o subjekt, ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

2.1 Subjekty verejnej správy ako kľúčové subjekty a dôležité subjekty

Subjekty verejnej správy môžu byť v zmysle smernice NIS 2 považované za kľúčové subjekty a dôležité subjekty pri aplikácii rôznych ustanovení čl. 3 ods. 1 smernice NIS 2.

V prvom rade v zmysle čl. 3 ods. 1 písm. d) smernice NIS 2 sú za kľúčové subjekty považované subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i) smernice NIS 2. V prípade predmetného ustanovenia ide o subjekty verejnej správy na úrovni ústrednej štátnej správy podľa definície členského štátu v súlade s vnútroštátnym právom.³⁷

V ďalších ustanoveniach čl. 3 ods. 1 smernice NIS 2 sa už priamo neodkazuje na subjekty verejnej správy a mohlo by sa zdať, že len subjekty verejnej správy na úrovni ústrednej štátnej správy by mali byť považované za kľúčové subjekty. Avšak máme za to, že za kľúčové subjekty možno v prípade ďalších ustanovení čl. 3 ods. 1 smernice

³⁶ Tamže, s. 51.

³⁷ Smernica NIS 2, čl. 3 ods. 1 písm. d).

NIS 2 za určitých podmienok považovať aj subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode ii) smernice NIS 2 (subjekty verejnej správy na regionálnej úrovni), ako aj subjekty verejnej správy uvedené ako typy subjektov v odvetví, resp. pododvetví inom ako je odvetvie „Verejná správa“.

Napríklad ak bude subjekt verejnej správy na regionálnej úrovni identifikovaný ako kritický subjekt podľa smernice o odolnosti kritických subjektov, bude takýto subjekt považovaný za kľúčový subjekt. Subjekt verejnej správy môže byť prevádzkovateľom inteligentných dopravných systémov v odvetví „Doprava“, pododvetvie „Cestná doprava“ podľa prílohy I smernice NIS 2 ak presahuje limity pre stredné podniky. Taktiež platí, že v zmysle čl. 3 ods. 1 písm. g) smernice NIS 2 sa za kľúčové subjekty môžu považovať aj subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou NIS alebo vnútroštátnym právom. Je na rozhodnutí členského štátu EÚ či tieto subjekty bude považovať za kľúčové subjekty. V tejto súvislosti je však otázne či tieto subjekty budú spĺňať konkrétne kritéria a požiadavky v zmysle smernice NIS 2. Máme za to, že prevádzkovatelia základných služieb (identifikovaní pred 16. januárom 2023) by mali byť považovaní za kľúčové subjekty len za podmienky, že spĺňajú požiadavky na kľúčové subjekty v zmysle smernice NIS 2 (pravidlo obmedzenia veľkosti, resp. konkrétne výnimky z tohto pravidla, definičné znaky subjektu verejnej správy). V praktickej rovine môže nastať situácia, že medzi subjektami verejnej správy, ktoré boli pred 16. januárom 2023 identifikovaní ako prevádzkovatelia základnej služby môžu byť nie len subjekty verejnej správy na úrovni ústrednej štátnej správy, ale aj subjekty verejnej správy na regionálnej úrovni a subjekty verejnej správy mimo odvetvia „Verejná správa“.

V súvislosti s otázkou či subjekty verejnej správy môžu byť považované za dôležité subjekty je potrebné interpretovať ustanovenie čl. 3 ods. 2 smernice NIS 2, podľa ktorého: *„Na účely tejto smernice sa subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 tohto článku, považujú za dôležité subjekty. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e).“*

Z predmetného ustanovenia vyplýva, že medzi dôležité subjekty možno zaradiť len také subjekty:

- ktorých typ je uvedený v prílohe I alebo II, avšak sa nepovažujú za kľúčové subjekty v zmysle čl. 3 ods. 1 smernice NIS 2 a

- sú označené členskými štátmi ako dôležité subjekty podľa čl. 2 ods. 2 písm. b) až e) smernice NIS 2.³⁸

Logicky by sa mohlo zdať, že medzi dôležité subjekty by sme mohli zaradiť subjekty verejnej správy na regionálnej úrovni podľa ustanovenia čl. 2 ods. 2 písm. f), bod ii). Avšak subjekty verejnej správy na regionálnej úrovni nespĺňajú požiadavku na dôležité subjekty, v zmysle ktorej sú označené členskými štátmi ako dôležité subjekty podľa čl. 2 ods. 2 písm. b) až e) smernice NIS 2. Subjekty verejnej správy na regionálnej úrovni sú uvedené v čl. 2 ods. 2 písm. f), bod ii), a teda sú mimo rozmedzia písm. b) až e) spomínaného ustanovenia. Avšak ako bolo konštatované vyššie, subjekty verejnej správy môžu byť aj subjektami v iných odvetviach ako je „Verejná správa“ a môže sa na nich vzťahovať smernica NIS 2 aj z iného dôvodu ako len toho, že sú kategóriou subjektu verejnej správy podľa čl. 2 ods. 2 písm. f) smernice NIS 2 v rámci výnimky z pravidla veľkosti.

3. Transpozícia smernice NIS 2 do právnych poriadkov vybraných členských štátov

K septembru 2024 sú 4 členské štáty EÚ, ktorým sa podarilo transponovať smernicu NIS 2 do ich právnych poriadkov. Konkrétne ide o Belgicko, Chorvátsko, Maďarsko a Lotyšsko.³⁹ V prípade viacerých členských štátov EÚ je transpozičná legislatíva v legislatívnom procese.⁴⁰

V rámci tejto časti ozrejmime základné koncepty prístupu transpozície do právneho poriadku Chorvátska a Belgicka. Konkrétne sa zameriame na to, akým spôsobom bola do národných právnych poriadkov transponovaná osobná pôsobnosť smernice NIS 2.

³⁸ Zaujímavosťou je, že v prípade českého prekladu predmetného ustanovenia nie sú tieto dve požiadavky kumulatívne. Ustanovenie čl. 3 ods. 2: „*Pro účely této směrnice se za důležité subjekty považují subjekty druhu uvedeného v příloze I nebo II, které nelze považovat za základní subjekty podle odstavce 1 tohoto článku. Patří k nim i subjekty, jež členské státy označily za důležité podle čl. 2 odst. 2 písm. b) až e).*“

³⁹ The NIS2 directive in EU. A country-by-country breakdown. Dostupné na: <https://www.truid.app/blog/the-nis2-directive-in-eu-a-country-by-country-breakdown>.

⁴⁰ K septembru 2024 je v legislatívnom procese návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o zmene a doplnení niektorých zákonov. Dostupné na: <https://www.slov-lex.sk/legislativne-procesy/SK/LP/2024/264>, cit. 2024-09-20. V prípade Českej republiky je k septembru 2024 v legislatívnom procese návrh zákona o kybernetickej bezpečnosti – EU. Dostupné na: <https://www.psp.cz/sqw/historie.sqw?o=9&t=759>, cit. 2024-09-20.

3.1 Chorvátsko

Zákon o kybernetickej bezpečnosti (Zakon o kibernetičkoj sigurnosti NN 14/2024)⁴¹ (ďalej len „**chorvátsky zákon o kybernetickej bezpečnosti**“), ktorým sa transponuje smernica NIS 2 do chorvátskeho právneho poriadku nadobudol účinnosť vo februári 2024. Predmetný zákon nahrádza starý zákon o kybernetickej bezpečnosti prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb (NN 64/18), ktorý bol prijatý v roku 2018, ako aj nariadenie o kybernetickej bezpečnosti prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb (NN 68/18).

Chorvátsky zákon o kybernetickej bezpečnosti preberá v oblasti osobnej pôsobnosti terminológiu použitú v smernici NIS 2, a teda rozlišuje medzi kľúčovými subjektmi (*essential entities*) a dôležitými subjektmi (*important entities*). Pri zaradzovaní subjektov medzi kľúčové subjekty a dôležité subjekty predmetný zákon berie do úvahy pravidlo obmedzenia veľkosti. Taktiež upravuje špecifické prípady, kedy budú tieto subjekty zaradené bez ohľadu na ich veľkosť. V prílohe I predmetného zákona sú uvedené sektory s vysokou úrovňou kritickosti a v prílohe II iné kritické sektory po vzore smernice NIS 2. Spomínané sektory v zásade kopírujú sektory uvedené v smernici NIS 2 s tým rozdielom, že v prípade chorvátskeho zákona o kybernetickej bezpečnosti je v prílohe II pridaný sektor „Vzdelávací systém“.

V rámci sektorov s vysokou úrovňou kritickosti je uvedený aj sektor verejnej správy. V článku 12 predmetného zákona je upravená kategorizácia subjektov verejného sektora. Do kategórie kľúčových subjektov sa bez ohľadu na ich veľkosť zaraďujú:

- orgány štátnej správy a
- iné štátne orgány a právnické osoby s verejnou právomocou v závislosti od výsledkov posúdenia ich významu pre plynulý výkon kľúčových spoločenských alebo hospodárskych činností.

V osobitných prípadoch sa do kategórie kľúčových subjektov zaraďujú súkromné a verejné subjekty, ktoré spravujú, rozvíjajú alebo udržiavajú štátnu informačnú infraštruktúru v súlade so zákonom upravujúcim štátnu informačnú infraštruktúru, a to bez ohľadu na ich veľkosť.

Jednotky miestnej a regionálnej samosprávy sa bez ohľadu na ich veľkosť zaraďujú do kategórie dôležitých subjektov v závislosti od

⁴¹ Zakon o kibernetičkoj sigurnosti NN 14/2024. Dostupné: https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html, cit. 2024-09-21.

výsledkov posúdenia ich významu pre plynulý výkon kľúčových spoločenských alebo hospodárskych činností.

V prílohe II je taktiež uvedený sektor „Vzdelávací systém“. Pod tento sektor patria súkromné a verejné subjekty zo vzdelávacieho systému. Vzdelávací systém zahŕňa predškolské vzdelávanie, základné vzdelávanie, stredné vzdelávanie a vysokoškolské vzdelávanie, monitorovanie, hodnotenie a rozvoj systému a implementáciu programu. V zmysle článku 13 chorvátskeho zákona o kybernetickej bezpečnosti sú tieto subjekty bez ohľadu na ich veľkosť zaradené do kategórie dôležitých subjektov v závislosti od výsledkov hodnotenia ich osobitného významu na celoštátnej alebo regionálnej úrovni pre výkon výchovno-vzdelávacej práce.

Predmetný zákon obsahuje splnomocnenia na prijatie nariadenia, ktoré bude bližšie špecifikovať riadenie rizík kybernetickej bezpečnosti, hlásenie incidentov, pravidlá pre samohodnotenie, kritériá na klasifikáciu subjektov do kategórie kľúčových alebo dôležitých bez ohľadu na ich veľkosť a ďalšie dôležité pravidlá.

3.2 Belgicko

Zákonom z 26. apríla 2024, ktorým sa ustanovuje rámec pre kybernetickú bezpečnosť sietí a informačných systémov všeobecného záujmu pre verejnú bezpečnosť (ďalej len „**zákon NIS 2**“), sa v Belgicku transponuje smernica NIS 2. Predmetný zákon nadobúda účinnosť 18. októbra 2024.

Zákon NIS 2 nahrádza zákon zo 7. apríla 2019, ktorým sa stanovuje rámec pre bezpečnosť sietí a informačných systémov všeobecného záujmu pre verejnú bezpečnosť, tzv. zákon NIS 1. Nový právny predpis sprevádza kráľovský dekrét z 9. júna 2024, ktorým sa vykonávajú jeho ustanovenia, napríklad určením Centra pre kybernetickú bezpečnosť Belgicka ako národného orgánu pre kybernetickú bezpečnosť.

Na to, aby subjekt podliehal zákonu NIS 2, postačuje vykonávať bez ohľadu na jeho právnu formu aspoň jednu zo služieb (typ subjektu) uvedených v prílohe I (odvetvia s vysokou úrovňou kritickosti) alebo prílohe II (iné kritické odvetvia) zákona NIS 2 v rámci EÚ a byť považovaný prinajmenšom za stredný podnik v zmysle odporúčania Komisie. Zákon NIS 2 upravuje rovnaké odvetvia ako smernica NIS 2

a taktiež rozlišuje medzi kľúčovými subjektami a dôležitými subjektami.⁴²

Ak skombinujeme rôzne veľkosti subjektu s kritériom služby (typ subjektu), možno kľúčové subjekty a dôležité subjekty zaradiť v zmysle nasledujúcej tabuľky.⁴³

	Stredný podnik	Veľký podnik
Služby (typ subjektu) podľa prílohy I	Dôležité subjekty	Kľúčové subjekty
Služby (typ subjektu) podľa prílohy II	Dôležité subjekty	Dôležité subjekty

Napriek tomu existuje niekoľko výnimiek z pravidla obmedzenia veľkosti. Niektoré typy subjektov spadajú do pôsobnosti zákona NIS 2 bez ohľadu na ich veľkosť:⁴⁴

- Kvalifikovaní poskytovatelia dôveryhodných služieb (kľúčové subjekty).
- Nekvalifikovaní poskytovatelia dôveryhodných služieb (dôležité subjekty, ak ide o mikropodnik, malý alebo stredný podnik a kľúčové subjekty, ak ide o veľký podnik).
- Poskytovatelia služieb DNS (kľúčové subjekty).
- Registre názvov TLD (kľúčové subjekty).
- Služby registrácie doménových mien (len pre povinnosť registrácie).
- Poskytovatelia verejných elektronických komunikačných sietí (kľúčové subjekty).
- Poskytovatelia verejne dostupných elektronických komunikačných služieb (kľúčové subjekty).
- Subjekty identifikované ako prevádzkovatelia kritickej infraštruktúry podľa zákona z 1. júla 2011 o bezpečnosti a ochrane kritickej infraštruktúry (kľúčové subjekty).
- Subjekty verejnej správy závislé od spolkového štátu (kľúčové subjekty).

⁴² Center for Cybersecurity Belgium. Frequently Asked Questions (FAQ) NIS2 in Belgium. Version 1.0. 07/2024, s. 4. Dostupné na: <https://ccb.belgium.be/sites/default/files/NIS2%20FAQ%20Website%20v1.0%20EN.pdf>, cit. 2024-09-20. Kráľ môže pridať sektory alebo podsektory do príloh I a II dekrétom prerokovaným v Rade ministrov po konzultácii s príslušnými sektorovými orgánmi a národným orgánom pre kybernetickú bezpečnosť.

⁴³ Tamže, s.14.

⁴⁴ Tamže s. 13.

V súvislosti s verejnou správou definuje zákon NIS 2 subjekt verejnej správy ako správny orgán⁴⁵, ktorý spĺňa tieto kritériá:⁴⁶

- a) nie je priemyselnej alebo obchodnej povahy;
- b) nevykonáva ako hlavnú činnosť uvedenú v stĺpci druh subjektu iného odvetvia alebo pododvetvia niektorej z príloh zákona NIS 2;
- c) nie je právnickou osobou podľa súkromného práva.

V kontexte naplnenia osobnej pôsobnosti musí byť predmetná definícia subjektu verejnej správy spojená aj s typom subjektu v zmysle prílohy I zákona NIS 2. V rámci odvetvia „Verejná správa“ zákon NIS 2 rozlišuje medzi nasledujúcimi typmi subjektov. V tabuľke uvádzame aj ich zaradenie medzi kľúčové subjekty alebo dôležité subjekty v závislosti od ich veľkosti.

	Veľké podniky	Stredné podniky	Malé a mikro podniky
a) Verejná správa, ktorá závisí ⁴⁷ od spolkového štátu,	Kľúčové subjekty		
b) Verejná správa, ktorá závisí od federatívnych subjektov, (iba v prípade identifikácie na základe posúdenia rizík kritickosti poskytovanej služby)	Dôležité subjekty		
c) Núdzové zóny (vrátane hasičskej a pohotovostnej lekárskej služby regiónu Brusel – hlavné mesto). ⁴⁸			

⁴⁵ V zmysle v § 14 ods. 1 písm. 1 koordinovaných zákonov o Štátnej rade.

⁴⁶ Zákon NIS 2, čl. 8 ods. 34.

⁴⁷ Koncept závislosti („ktorá závisí od“) vychádza z článku 5 zákona z 30. júla 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov. Ide najmä o subjekty, ktoré sú súčasťou úrovne verejnej moci, pretože boli vytvorené týmito orgánmi verejnej moci, ich činnosť je financovaná najmä týmito orgánmi verejnej moci, ich hospodárenie podlieha kontrole zo strany týchto orgánov verejnej moci, resp. viac ako polovica členov ich správneho, riadiaceho alebo dozorného orgánu vymenúvajú tieto orgány.

⁴⁸ V zmysle článku 14 zákona z 15. mája 2007 o civilnej bezpečnosti alebo hasičskej a pohotovostnej lekárskej asistenčnej službe regiónu Brusel – hlavné mesto vytvorené výnosom z 19. júla 1990, ktorým sa zriaďuje hasičská a pohotovostná lekárska asistenčná služba Región hlavného mesta Brusel.

Subjekty verejnej správy na miestnej úrovni (napr. obce, provincie) automaticky nepodliehajú požiadavkám zákona NIS 2. Avšak na tieto subjekty sa vzťahujú ustanovenia zákona NIS 2, keď poskytujú službu uvedenú v prílohe I alebo II zákona NIS 2 a sú väčšie ako malý podnik. Subjekty verejnej správy na miestnej úrovni môžu byť identifikované aj v rámci procesu určenia Centrom pre kybernetickú bezpečnosť Belgicka, kedy sa identifikujú subjekty bez ohľadu na veľkosť.⁴⁹

V súvislosti s reguláciou vzdelávacích inštitúcií platí, že v prílohe I a II zákona NIS 2 nie je odvetvie vzdelávania explicitne uvedené. Avšak verejné vzdelávacie zariadenia ako univerzity alebo stredné školy by mohli byť zahrnuté v rámci definície subjekt verejnej správy ak by spĺňali požiadavku na kritérium veľkosti, mali sídlo v Belgicku, spĺňali definíciu subjektu verejnej správy podľa zákona NIS 2 a boli závislé od federálneho štátu alebo federatívnych subjektov. V špecifických prípadoch by sa napríklad univerzitná nemocnica mohla považovať za poskytovateľa zdravotnej starostlivosti v zmysle prílohy I zákona NIS 2.⁵⁰

Záver

Jedným z dôvodov, prečo došlo k zrušeniu smernice NIS a jej nahradeniu novou právnou úpravou v podobe smernice NIS 2, bola nejednotnosť v oblasti transpozície osobnej pôsobnosti. Odlišnosť pri identifikovaní prevádzkovateľov základnej služby spôsobovala, že rovnaké entity v konkrétnom sektore podliehali prísnejším opatreniam v jednom členskom štáte EÚ ako v ostatných. Výsledkom bola odlišná implementácia smernice NIS a fragmentácia právneho rámca kybernetickej bezpečnosti.

Smernica NIS 2 sa v porovnaní so smernicou NIS v oblasti osobnej pôsobnosti odkláňa od identifikácie subjektov na základe kritérií, ktoré si cez rôzne prahové hodnoty nastavili členské štáty. Pravidlo obmedzenia veľkosti by malo v oblasti harmonizácie v otázkach osobnej pôsobnosti dosiahnuť to, aby si členské štáty nevytvárali rôzne kritériá a prahové hodnoty pre tieto kritériá, ale aby sa posudzovala veľkosť daného subjektu a to či je subjektom v danom odvetví, resp. či spĺňa konkrétnu výnimku z pravidla obmedzenia veľkosti.

⁴⁹ Zákon NIS 2, čl. 11 ods. 1-3.

⁵⁰ Center for Cybersecurity Belgium. Frequently Asked Questions (FAQ) NIS2 in Belgium. Version 1.0. 07/2024, s. 10-11. Dostupné na: <https://ccb.belgium.be/sites/default/files/NIS2%20FAQ%20Website%20v1.0%20EN.pdf>, cit. 2024-09-20.

Rozšírenie odvetví regulovaných smernicou NIS 2 v prílohe I a II možno vnímať pozitívne. Členské štáty si v prípade smernice NIS vytvárali aj iné odvetvia a pododvetvia, ktoré boli stanovené v smernici NIS odvolávajúc sa na princíp minimálnej harmonizácie. Aj na základe skúseností s týmito dodatočnými odvetviami došlo k rozšíreniu zoznamu regulovaných odvetví, resp. pododvetví.

Z pravidla obmedzenia veľkosti však existuje v zmysle smernice NIS 2 mnoho výnimiek, kde sa nebude skúmať veľkosť daného subjektu. Je otáznne, akým spôsobom členské štáty implementujú tieto výnimky v rámci transpozície a či sa práve týmito výnimkami nenaruší hlavný cieľ, ktorým je harmonizácia.

Smernica NIS 2 taktiež v otázke osobnej pôsobnosti ponecháva na členské štáty či budú regulovať subjekty verejnej správy na miestnej úrovni či vzdelávacie inštitúcie, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti. V rámci transpozície smernice NIS 2 môže teda nastať, že v niektorých štátoch budú uvedené subjekty regulované, zatiaľ čo v iných nie.

Rozdiely v transpozícii medzi členskými štátmi by mohli ovplyvniť zamýšľanú harmonizáciu a mohli by sme po niekoľkých rokoch od účinnosti smernice NIS 2 dospieť k rovnakému záveru ako v prípade smernice NIS, a teda, že harmonizácia nebola úspešná. Už v súčasnosti možno v prípade právnych predpisov Chorvátska a Belgicka, ktorými bola smernica NIS 2 transponovaná vidieť v niektorých aspektoch osobnej pôsobnosti odlišné prístupy.

V prípade chorvátskeho zákona o kybernetickej bezpečnosti možno vidieť, že došlo k rozšíreniu odvetví v porovnaní so smernicou NIS 2. Konkrétne bol doplnený sektor „Vzdelávací systém“, pod ktorý patrí aj predškolské vzdelávanie, základné vzdelávanie, stredné vzdelávanie a vysokoškolské vzdelávanie. V prípade belgického zákona NIS 2 je zoznam sektorov totožný s tým, ktorý uvádza v prílohách smernica NIS 2.

Pri oboch analyzovaných právnych predpisoch možno vidieť taktiež iný prístup k pojmu subjekt verejnej správy a kategorizáciu týchto subjektov. Chorvátsky zákon o kybernetickej bezpečnosti zaraďuje do kategórie kľúčových subjektov bez ohľadu na ich veľkosť orgány štátnej správy a iné štátne orgány a právnické osoby s verejnou právomocou v závislosti od výsledkov posúdenia ich významu pre plynulý výkon kľúčových spoločenských alebo hospodárskych činností. Taktiež platí, že v osobitných prípadoch sa do kategórie kľúčových subjektov zaraďujú súkromné a verejné subjekty, ktoré spravujú, rozvíjajú alebo

udržiavajú štátnu informačnú infraštruktúru, a to bez ohľadu na ich veľkosť. Čo sa týka jednotiek miestnej a regionálnej samosprávy, tieto sa bez ohľadu na ich veľkosť zaraďujú do kategórie dôležitých subjektov v závislosti od výsledkov posúdenia ich významu pre plynulý výkon kľúčových spoločenských alebo hospodárskych činností. Ako je možné vidieť, v mnohých prípadoch sa pri subjektoch verejnej správy bude vykonávať posúdenie ich významu pre plynulý výkon kľúčových spoločenských alebo hospodárskych činností.

Belgický zákon NIS 2 obsahuje vlastnú definíciu subjektu verejnej správy, v zmysle ktorej musia byť splnené konkrétne definíčné kritériá. Subjekt verejnej správy nemôže byť priemyselnej alebo obchodnej povahy. Taktiež nemôže vykonávať ako hlavnú činnosť uvedenú v iných odvetviach, resp. v pododvetviach a nemôže byť právnickou osobou podľa súkromného práva. S prihliadnutím na belgický zákon NIS 2 možno očakávať, že aj ďalšie členské štáty si v rámci transpozície s odvolaním sa na špecifiká verejnej správy budú prispôsobovať definíciu subjektu verejnej správy a ich jednotlivé kategórie.

V prípade chorvátskeho zákona o kybernetickej bezpečnosti a belgického zákona NIS 2 je možné dopĺňať odvetvia a pododvetvia, ktoré nie sú v súčasnosti regulované na národnej úrovni, ani v samotnej smernici NIS 2. Je možné predpokladať, že ak sa v budúcnosti ukáže, že odvetvie, ktoré ešte nie je zahrnuté do rozsahu pôsobnosti, by malo byť zahrnuté z dôvodu jeho dôležitosti pre kritické spoločenské a/alebo hospodárske činnosti, môžu byť príslušné prílohy rozšírené aj o tieto nové odvetvia, resp. pododvetvia. V takýchto prípadoch nastanú situácie, kedy subjekty budú regulované v jednom členskom štáte, avšak v inom členskom štáte regulované nebudú, nakoľko daný štát takéto odvetvie, resp. pododvetvie neupravuje.

Zoznam použitej literatúry

1. Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
2. 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

3. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES
4. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
5. EURÓPSKA KOMISIA. Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final.
6. EURÓPSKA KOMISIA. Príručka pre používateľov k definícii MSP. 2019, 60 s. Dostupné na: <https://op.europa.eu/sk/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1>, cit. 2024-09-20.
7. EURÓPSKA KOMISIA. Správe o posúdení jednotnosti prístupu členských štátov pri identifikácii prevádzkovateľov základných služieb v súlade s článkom 23 ods. 1 smernice 2016/1148/EÚ o bezpečnosti sietí a informačných systémov. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52019DC0546>, cit. 2024-09-20.
8. Odporúčanie Komisie zo 6. mája 2003 o definícii mikro, malých a stredných podnikov (oznámené pod číslom dokumentu C (2003) 1422) (2003/361/ES)
9. Oznámenie Komisie Usmernenia Komisie k uplatňovaniu článku 3 ods. 4 smernice (EÚ) 2022/2555 (smernica NIS 2) 2023/C 324/02. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1716636475611&uri=CELEX%3A52023XC0914%2801%29>, cit. 2024-09-20.
10. VANDEZANDE, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. In *Computer Law & Security Review*, Volume 52, 2024.
11. SIEVERS, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *Int. Cybersec. Law Rev.* 2, 2021, s. 223–231.
12. MARKOPOULOU, D. a kol. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review*, Volume 35, Issue 6, 2019.
13. DUCUING, Ch. Understanding the rule of prevalence in the NIS directive: C-ITS as a case study, *Computer Law & Security Review*, Volume 40, 2021.
14. Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience. Dostupné na: <https://www.europarl.europa.eu/news/en/press->

- room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience., cit. 2024-09-20.
15. EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. Dostupné na: <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/>, cit. 2024-09-20.
 16. NÚKIB: Factsheet pre posúdenie veľkosti subjektov. Dostupné na: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>.
 17. Center for Cybersecurity Belgium. Frequently Asked Questions (FAQ) NIS2 in Belgium. Version 1.0. 07/2024, s. 4. Dostupné na: <https://ccb.belgium.be/sites/default/files/NIS2%20FAQ%20Website%20v1.0%20EN.pdf>, cit. 2024-09-20.
 18. Zákon z 26. apríla 2024, ktorým sa ustanovuje rámec pre kybernetickú bezpečnosť sietí a informačných systémov všeobecného záujmu pre verejnú bezpečnosť. Dostupné na: <https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel>, cit. 2024-09-22.
 19. The NIS2 directive in EU. A country-by-country breakdown. Dostupné na: <https://www.truid.app/blog/the-nis2-directive-in-eu-a-country-by-country-breakdown>.
 20. Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. O kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o zmene a doplnení niektorých zákonov. Dostupné na: <https://www.slov-lex.sk/legislativne-procesy/SK/LP/2024/264>, cit. 2024-09-20.
 21. Návrh zákona o kybernetickej bezpečnosti – EU. Dostupné na: <https://www.psp.cz/sqw/historie.sqw?o=9&t=759>, cit. 2024-09-20