KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.139-146
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

DODÁVATEĽSKÝ REŤAZEC A KYBERNETICKÁ BEZPEČNOSŤ

SUPPLY CHAIN AND CYBERSECURITY

ĽUBOMÍRA SOKOLOVÁ, MATÚŠ MADLEŇÁK, TIMOTEJ MAČUHA

ABSTRACT: The NIS2 Directive is an updated version of the original 2016 NIS Directive and aims to strengthen the protection and security of the EU's cyberspace. Unlike the first directive, NIS2 focuses on the cybersecurity and resilience of key entities and entire sectors in the face of modern threats. EU Member States are required to transpose it into their national legal systems. In Slovakia, the requirements of NIS2 were implemented through an amendment to the Act on Cybersecurity. The amendment, prepared by the National Security Authority, entered into force on January 1, 2025. It modifies and supplements the original Act No. 69/2018 Coll. and introduces several fundamental changes. One of the key elements is the enhancement of supply chain security. This protection is ensured primarily through contractual mechanisms based on the Act and on Decree No. 227/2025 of the National Security Authority. Contractual obligations must also reflect the requirements of the GDPR.
The article focuses mainly on contractual protection within supply chains and its alignment with GDPR requirements.

KEYWORDS: *supply chain, cybersecurity, data protection, measures.*

ÚVOD

Smernica NIS2 predstavuje revidovanú a aktualizovanú verziu pôvodnej smernice NIS z roku 2016, pričom jej primárnym cieľom je posilnenie ochrany a zabezpečenia kybernetického priestoru Európskej únie. Na rozdiel od predchádzajúcej úpravy, ktorá sa sústreďovala primárne na zabezpečenie základných služieb, NIS2 rozširuje rozsah pôsobnosti smernice na širšie spektrum kľúčových subjektov a sektorov, pričom reflektuje dynamicky sa vyvíjajúce a komplexnejšie kybernetické hrozby. Členské štáty EÚ majú legislatívnu povinnosť transponovať ustanovenia smernice do svojich vnútroštátnych právnych poriadkov. V slovenskom právnom systéme bola smernica NIS2 implementovaná prostredníctvom novely zákona o kybernetickej bezpečnosti, ktorú vypracoval Národný bezpečnostný úrad. Novela bola schválená Národnou radou Slovenskej republiky a nadobudla účinnosť 1. januára 2025. Predmetná novela modifikuje a dopĺňa Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a prináša viacero koncepčných zmien. Jednou z významných inovácií je posilnenie ochrany bezpečnosti v rámci dodávateľských reťazcov, ktoré sú považované za kritický prvok v komplexnom systéme kybernetickej odolnosti.

1. DODÁVATEĹSKÝ REŤAZEC

Dodávateľský reťazec predstavuje proces, ktorý zahŕňa určité kroky a aktivity potrebné na vytvorenie a dodanie tovaru resp. určitých služieb konečnému odberateľovi.

V súčasnosti sa v komerčnom sektore čoraz častejšie uplatňuje model, v ktorom podniky delegujú činnosti, ktoré nepovažujú za súčasť svojho hlavného predmetu podnikania (tzv. core business) na externé subjekty. Tento prístup je všeobecne známy ako outsourcing. Organizácie týmto spôsobom separujú podporné a vedľajšie procesy, čím získavajú možnosť koncentrovať svoje kapacity a expertízu na strategicky kľúčové oblasti (Kampová, 2024).

Zatiaľ čo z pohľadu ekonomickej efektívnosti a optimalizácie procesov patrí hodnotenie takéhoto procesu do pôsobnosti odborníkov na ekonomiku a procesný manažment, z hľadiska informačnej bezpečnosti je potrebné poukázať na kľúčový aspekt. Každé obstarávanie tovarov alebo služieb, ktoré zasahuje do správy informačných aktív organizácie, predstavuje špecifický typ rizika. Tento rizikový faktor musí byť systematicky identifikovaný, analyzovaný a primerane riadený v súlade s princípmi riadenia kybernetickej a informačnej bezpečnosti.

Rozhodovanie o outsourcingu by nemalo byť založené výlučne na ekonomických aspektoch, ale musí reflektovať aj hľadiská informačnej a kybernetickej bezpečnosti.

Organizácia by mala vykonať dôkladnú analýzu, na základe ktorej určí:
- ktoré činnosti ponechá vo vlastnej réžii (insourcing),
- ktoré aktivity je možné outsourcovať čiastočne – najmä v prípade menej kritických podporných procesov,
- a či je vôbec vhodné presunúť všetky hlavné aktivity mimo organizácie.

Pri tomto rozhodovaní je nevyhnutné zohľadniť dopad na informačné aktíva organizácie a úroveň ich ochrany, keďže každé presunutie činnosti na externý subjekt-dodávateľa, so sebou prináša potenciálne bezpečnostné riziká.
Outsourcing zahŕňa aj cloudové služby. V praktickom kontexte možno väčšinu cloudových modelov považovať za formu outsourcingu (Kampová, 2024).

Z tohto dôvodu je potrebné pristupovať k ich hodnoteniu a riadeniu s rovnakou mierou dôslednosti a prísnosti, ako pri iných typoch externých služieb, najmä z hľadiska bezpečnosti a ochrany informačných aktív. Veľké množstvo subjektov zapojených do dodávateľského reťazca a jeho priestorové usporiadanie si nevyhnutne vyžadujú, aby boli tieto integrované reťazce riadené.

Ak sa bezpečnostné riziká hodnotia až po výbere dodávateľa, môže to byť pre organizáciu veľmi nebezpečné. Zrušenie zmluvy býva často nákladné a komplikované. Podrobná analýza dokáže odhaliť slabé zabezpečenie, chýbajúce bezpečnostné opatrenia či väzby na rizikové subjekty ešte pred podpisom zmluvy. Včasná identifikácia problémov umožňuje vybrať bezpečnejšieho dodávateľa alebo prijať ochranné opatrenia. Neseriózni dodávatelia predstavujú osobitnú hrozbu – môžu mať za sebou porušenia zmlúv, úniky dát či zneužitie osobných údajov, čo vedie k právnym následkom aj strate dôvery klientov (Hotwagner, 2008).

2. POŽIADAVKY PRÁVNYCH PREDPISOV

Povinnosť zabezpečiť informačné aktíva prostredníctvom zmluvných mechanizmov v dodávateľských reťazcoch je zakotvená vo viacerých právnych a normatívnych rámcoch.

Medzi najvýznamnejšie patria.
- **Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti - NIS 2,**
- **Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti**, ako aj **zákon č. 95/2018 Z. z. o informačných technológiách verejnej správy**,
- **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(ďalej len „GDPR“) (čl. 28, čl. 32)** – ktoré upravuje povinnosti prevádzkovateľa pri zverení spracúvania osobných údajov sprostredkovateľovi(dodávateľovi),
- **Medzinárodné technické normy**, ako napríklad **STN ISO/IEC 27001 a 27002**, ktoré definujú osvedčené postupy pre riadenie informačnej bezpečnosti.
- **Sektorovo špecifické právne predpisy**, ktoré stanovujú dodatočné požiadavky v regulovaných odvetviach.

Tieto predpisy spolu vytvárajú záväzný rámec, v ktorom je zmluvná úprava vzťahov s dodávateľmi kľúčovým nástrojom na ochranu informačných aktív (Kampová, 2025).

Smernica NIS2 vytvorila nielen potrebu aktualizácie Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Po novele zákona bola vytvorená i Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach, ktorá stanovuje obsah riadenia rizík v dodávateľskom reťazci.

Riadeniu rizík sa venuje **§ 5 vyhlášky NBÚ č.227/2025**. Jej obsahom je:
- **identifikácia aktív** – systematické určenie všetkých relevantných informačných a technologických prostriedkov, ktoré podliehajú ochrane,
- **identifikácia rizík** – vrátane popisu existujúcich a realizovaných bezpečnostných opatrení, ktoré majú za cieľ eliminovať alebo zmierniť zistené hrozby,

- **analýza rizík** – v prípade, že prevádzkovateľ základnej služby využíva vlastnú bezpečnostnú metodiku, je potrebné zabezpečiť mapovanie rizík v súlade so štruktúrou uvedenou v referenčnej metodike dostupnej na oficiálnej webovej stránke príslušného úradu,
- **hodnotenie rizík** – kvantitatívne alebo kvalitatívne vyhodnotenie úrovne jednotlivých rizík na základe pravdepodobnosti výskytu a možného dopadu,
- **implementácia bezpečnostných opatrení** – na základe výsledkov hodnotenia rizík, vrátane zdokumentovania, ktoré opatrenia boli prijaté a ktoré nie, spolu s príslušným odôvodnením.
- **Pravidelné prehodnocovanie rizík** – minimálne raz ročne, s cieľom zabezpečiť aktualizáciu identifikovaných rizík a revíziu prijatých bezpečnostných opatrení v závislosti od zistených zmien a nových poznatkov (Vyhláška č.227/2025).

Súčasťou procesu riadenia rizík je aj analýza funkčného dopadu (Business Impact Analysis – BIA), ktorá zahŕňa hodnotenie potenciálneho vplyvu krízových scenárov na činnosť prevádzkovateľa základnej služby. Tieto scenáre môžu zasiahnuť kritické zdroje a aktíva, ktoré podporujú kľúčové procesy, a tým spôsobiť ohrozenie alebo prerušenie kontinuity poskytovania služieb. Neoddeliteľnou súčasťou analýzy funkčného dopadu je aj stanovenie cieľových úrovní obnovy a identifikácia prevádzkových a bezpečnostných požiadaviek, ktoré sú potrebné na zabezpečenie odolnosti organizácie.

- **Bezpečnostné opatrenia sú navrhované, implementované a realizované spôsobom, ktorý zabezpečuje elimináciu alebo zmiernenie všetkých rizík identifikovaných v rámci analýzy rizík.** Tieto opatrenia musia zároveň reflektovať strategické ciele kybernetickej bezpečnosti, byť v súlade s internou bezpečnostnou politikou a napĺňať legislatívne a normatívne požiadavky na informačnú a kybernetickú bezpečnosť (Vyhláška č.227/2025).

Bezpečnosť dodávateľského reťazca je zadefinovaná v zmysle povinností prevádzkovateľa základnej služby i priamo v zákone o kybernetickej bezpečnosti. Prevádzkovateľ základnej služby je povinný, ak vykonáva činnosť prostredníctvom tretej strany, ktorá priamo súvisí s dostupnosťou, dôvernosťou alebo integritou prevádzky jeho sietí a informačných systémov, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení. Pri uzatvorení zmluvy sa vykonáva analýza rizík. Počas trvania zmluvného vzťahu je tretia strana povinná vykonávať a uplatňovať bezpečnostné opatrenia v súlade s uzatvorenou písomnou zmluvou. V zmysle § 19 Zákona o kybernetickej bezpečnosti je prevádzkovateľ základnej služby povinný realizovať systematickú analýzu vzájomných závislostí svojich aktív, informačných systémov, využívaných produktov informačno-komunikačných technológií a služieb poskytovaných tretími stranami v rámci dodávateľského reťazca. Cieľom tejto analýzy je identifikácia a vyhodnotenie potenciálnych dopadov kybernetických bezpečnostných incidentov na prevádzku a poskytovanie služieb.

Analýza rizík slúži na určenie pravdepodobnosti výskytu škodlivej udalosti, ktorá môže nastať v dôsledku zneužitia existujúcej zraniteľnosti aktíva potenciálnou hrozbou, a to v kontexte aktuálne implementovaných bezpečnostných opatrení**.** Súčasťou tejto analýzy je aj identifikácia možných následkov narušenia základných bezpečnostných princípov – dôvernosti, integrity a dostupnosti daného aktíva. Výsledkom analýzy je kvalitatívne alebo kvantitatívne vyhodnotenie rizika, ktoré slúži ako podklad pre návrh a implementáciu adekvátnych opatrení na jeho elimináciu alebo zmiernenie. Analýza rizík podľa Filipa zahŕňa identifikáciu hrozieb, posúdenie pravdepodobnosti ich uskutočnenia a vyhodnotenie ich potenciálnych následkov. Je to komplexný nástroj manažmentu rizík, ktorý pomáha odpovedať na otázky, aké bezpečnostné riziká sa môžu vyskytnúť, aká je ich pravdepodobnosť a aké budú následky bezpečnostného konfliktu (Filip, 2011). Národný bezpečnostný úrad SR vypracoval metodiku analýzy rizík, ktorá je k dispozícii na ich webovej stránke (NBÚ, 2025).

Na základe výsledkov vykonanej analýzy rizík je prevádzkovateľ základnej služby povinný najneskôr do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby prijať, implementovať a udržiavať všeobecné bezpečnostné opatrenia minimálne v rozsahu stanovenom v § 20. Tieto opatrenia musia byť vykonávané s cieľom zabezpečiť primeranú úroveň kybernetickej bezpečnosti, odolnosti a kontinuity poskytovaných služieb (Zákon o kybernetickej bezpečnosti, 2025).

Zákon o kybernetickej bezpečnosti jasne stanovuje i ďalšie povinnosti, ktoré je potrebné v dodávateľskom reťazci dodržiavať. Prevádzkovateľ základnej služby je povinný realizovať systematickú analýzu vzájomných závislostí medzi vlastnými aktívami, informačnými systémami, využívanými produktmi a službami informačno-komunikačných technológií (IKT) tretích strán v rámci dodávateľského reťazca a poskytovaných služieb. Cieľom je identifikácia a hodnotenie potenciálnych dopadov kybernetických bezpečnostných incidentov na kontinuitu a integritu prevádzkovaných procesov.
Na základe výsledkov analýzy je prevádzkovateľ povinný prijať, implementovať a priebežne udržiavať bezpečnostné opatrenia v súlade s aktuálnymi bezpečnostnými metodikami a politikami príslušného úradu, pričom zohľadňuje najnovšie bezpečnostné trendy, príklady dobrej praxe a relevantné medzinárodné normy.

Tretia strana, ktorá má významný vplyv na zabezpečovanie kybernetickej bezpečnosti a je v zmluvnom vzťahu s prevádzkovateľom základnej služby vykonávajúcim kritickú základnú službu, nadobúda postavenie prevádzkovateľa základnej služby. Prevádzkovateľ kritickej základnej služby je povinný bezodkladne oznámiť príslušnému úradu uzatvorenie aj ukončenie zmluvného vzťahu s takouto treťou stranou. Táto tretia strana sa následne zapisuje do registra prevádzkovateľov základných služieb.
Zároveň je povinná uplatňovať a dodržiavať bezpečnostné opatrenia v súlade s platnou legislatívou a podlieha dohľadu a kontrole zo strany Národného bezpečnostného úradu (Zákon o kybernetickej bezpečnosti, 2025).

Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach v § 7 stanovuje obsah zmluvy v dodávateľskom reťazci nasledovne:

a) záväzok dodávateľa vykonávať činnosti, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“), a zároveň dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
b) potvrdenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,
c) ustanovenie určujúce rozsah, spôsob a možnosti výkonu kontrolných činností a auditu, ktoré môže prevádzkovateľ základnej služby uskutočniť u tretej strany,
d) ustanovenie o povinnosti tretej strany informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach, ktoré môžu mať vplyv na úroveň kybernetickej bezpečnosti, ako aj o povinnosti poskytnúť súčinnosť pri riešení takýchto incidentov.

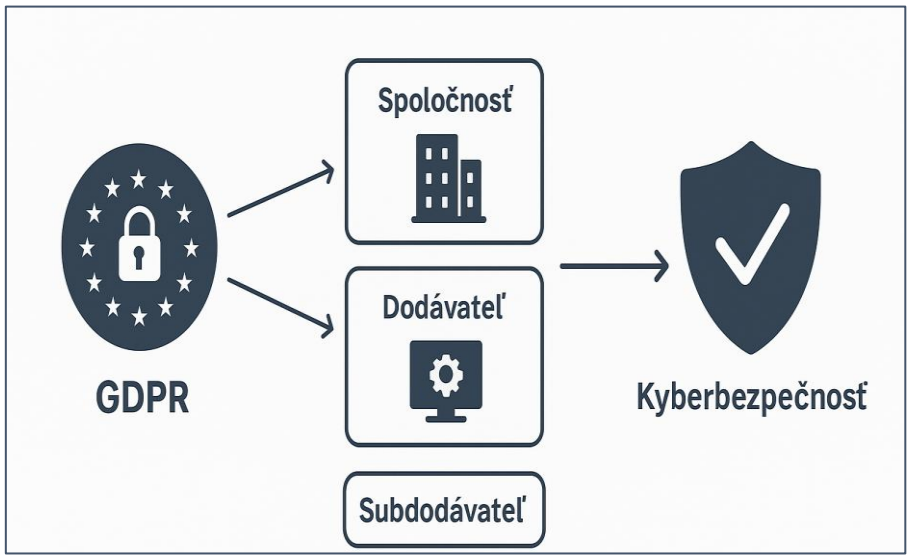
Rozsah bezpečnostných opatrení pre oblasť kybernetickej bezpečnosti podľa § 20 ods. 2 zákona sú upravené v **Prílohe č.1 k vyhláške č. 227/2025 Z. z.**

Tieto opatrenia sú stanovené pre:

- organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
- správu zraniteľností a kybernetických hrozieb,
- správu aktív a riadenie kybernetických hrozieb a rizík,
- riadenie udalostí a kybernetických bezpečnostných incidentov,
- riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
- bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,
- postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
- kryptografické opatrenia a zásady používania kryptografie,
- bezpečnosť a spôsobilosti ľudských zdrojov,
- správu identít a prístupov,
- bezpečnosť pri prevádzke sietí a informačných systémov,
- ochranu proti škodlivému kódu a nežiaducemu obsahu,
- systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
- monitorovanie, zaznamenávanie a hlásenie udalostí,
- fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
- ochranu záznamov, súkromia a označovanie informácií,
- dodávateľský reťazec.

3. GDPR A DODÁVATEĽSKÝ REŤAZEC V KYBERBEZPEČNOSTI

Do zmluvnej ochrany dodávateľského reťazca zasahujú nie len podmienky zákona o kybernetickej bezpečnosti a prislúchajúcej vyhlášky. Smernica NIS 2 upozorňuje i na požiadavky na bezpečnosť dodávateľského reťazca, ktoré kladie 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 (GDPR).



Obrázok 1 GDPR a dodávateľský reťazec

GDPR dáva dôraz na zodpovednosť prevádzkovateľa aj sprostredkovateľa(dodávateľa) pri spracúvaní osobných údajov. To znamená, že ak si firma najme externého dodávateľa (napr. cloudové služby, IT podporu, hosting), nesie zodpovednosť za to, že tento dodávateľ dodržiava primerané bezpečnostné opatrenia na ochranu dát.

Prepojenia medzi dodávateľským reťazcom a GDPR:

- Zodpovednosť za dodávateľov – Organizácia musí preveriť, či jej partneri a dodávatelia dodržiavajú GDPR (tzv. due diligence).
- Zmluvné vzťahy – GDPR vyžaduje uzatvoriť so sprostredkovateľmi (dodávateľmi) *zmluvy o spracúvaní osobných údajov* (DPA), kde sa definujú bezpečnostné opatrenia (článok 28 GDPR).
- Kybernetická bezpečnosť – Článok 32 GDPR prikazuje zaviesť primerané technické a organizačné opatrenia. To sa vzťahuje aj na dodávateľský reťazec (napr. šifrovanie dát, bezpečný prenos, prístupové práva).
- Riziká dodávateľského reťazca – Ak dôjde k úniku údajov cez dodávateľa, zodpovednosť padá aj na firmu, ktorá ho využíva. V praxi sa často rieši cez bezpečnostné audity, certifikácie (ISO 27001) alebo hodnotenie dodávateľov.
- Incidenty a oznamovanie porušení – GDPR ukladá povinnosť nahlásiť únik dát do 72 hodín. Ak únik spôsobí dodávateľ, musí o tom okamžite informovať objednávateľa (GDPR, 2016).

Tabuľka 1 GDPR požiadavky a dodávateľský reťazec (Zdroj: GDPR, 2016)

GDPR požiadavka	Ako sa premieta do dodávateľského reťazca	Príklad z praxe
Zodpovednosť prevádzkovateľa (čl. 24, 28)	Firma je zodpovedná aj za svojich dodávateľov, ktorí spracúvajú dáta.	E-shop používa externý cloud – musí preveriť, či cloudový poskytovateľ dodržiava GDPR.
Zmluvy o spracúvaní údajov (DPA)	Povinnosť uzatvoriť so sprostredkovateľom zmluvu s jasne definovanými bezpečnostnými opatreniami.	Firma outsourcuje účtovníctvo – v zmluve sa špecifikuje, ako budú chránené osobné údaje klientov.
Primerané bezpečnostné opatrenia (čl. 32)	Dodávateľ musí zaviesť technické a organizačné opatrenia (šifrovanie, prístupové práva, monitoring).	Hostingová firma musí mať zabezpečené servery proti neoprávnenému prístupu.
Hodnotenie rizík	Prevádzkovateľ musí vyhodnotiť riziká dodávateľského reťazca.	Banka preveruje IT dodávateľov cez bezpečnostný audit pred podpisom zmluvy.
Oznamovanie incidentov (čl. 33)	Dodávateľ je povinný informovať prevádzkovateľa o úniku dát bez zbytočného odkladu.	Ak IT firma zistí únik hesiel, musí okamžite kontaktovať svojho klienta, aby ten stihol nahlásiť porušenie Úradu na ochranu osobných údajov.
Medzinárodné prenosy dát	Dodávatelia mimo EÚ musia dodržiavať špeciálne pravidlá (napr. štandardné zmluvné doložky).	Firma využíva call centrum v Indii – musí mať právne ošetrený prenos dát.

Článok 28 GDPR stanovuje podmienky zmluvy. Ak sa spracúvanie osobných údajov vykonáva v mene prevádzkovateľa, ten je povinný využívať výlučne sprostredkovateľov(ďalších dodávateľov) , ktorí poskytujú dostatočné záruky o prijatí primeraných technických a organizačných opatrení zabezpečujúcich, že spracúvanie bude v súlade s požiadavkami tohto nariadenia a zároveň bude chrániť práva dotknutých osôb. Sprostredkovateľ (dodávateľ) nesmie poveriť spracúvaním ďalšieho sprostredkovateľa(dodávateľa) bez predchádzajúceho osobitného alebo všeobecného písomného súhlasu prevádzkovateľa. V prípade všeobecného písomného súhlasu je sprostredkovateľ povinný informovať prevádzkovateľa o všetkých plánovaných zmenách týkajúcich sa pridania alebo nahradenia ďalších sprostredkovateľov, aby prevádzkovateľ mal možnosť uplatniť námietky voči týmto zmenám (GDPR, 2016).

Sprostredkovateľ(dodávateľ):

- dodržiava podmienky zapojenia ďalšieho sprostredkovateľa (dodávateľa),
- po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby,
- po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov,
- dodržiava podmienky zapojenia ďalšieho sprostredkovateľa(dodávateľa),
- po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby,
- po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov (GDPR, 2016).

Bezpečnosť spracúvania GDPR upravuje i prostredníctvom článku 32. Zaväzuje v ňom prevádzkovateľa a sprostredkovateľa (dodávateľa) prijať primerané technické a organizačné opatrenia:

- pseudonymizácia a šifrovanie;
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania a služieb,
- schopnosť včas obnoviť dostupnosť v prípade fyzického alebo technického incidentu,

- zabezpečiť pravidelné testovanie, posudzovanie a hodnotenie účinnosti technických a organizačných opatrení (GDPR, 2016).

ZÁVER

Zákon o kybernetickej bezpečnosti stanovuje opatrenia pre oblasť riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, pričom je potrebné s dodávateľom uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti zmluvy. Obsah zmluvy je stanovený vyhláškou, pričom vzor bezpečnostnej dokumentácie a vzor zmluvy podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti sa zverejnia na webovom sídle úradu. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 (GDPR) významne ovplyvňuje riadenie dodávateľského reťazca. Organizácie nesú zodpovednosť za preverovanie svojich dodávateľov a musia mať s nimi uzatvorené zmluvy o spracúvaní osobných údajov. Celý reťazec musí dodržiavať primerané technické a organizačné bezpečnostné opatrenia podľa článku 32 GDPR, pričom konkrétne podmienky zmluvy, ktoré musia byť splnené, určuje článok 28 GDPR.
Predmetom tohto článku je sumarizácia zmluvných mechanizmov v rámci dodávateľských reťazcov v kybernetickej bezpečnosti, a to so zameraním na ich súlad s požiadavkami a zásadami stanovenými nielen zákonom o kybernetickej bezpečnosti ale i GDPR. Cieľom bolo identifikovať a zhodnotiť kľúčové prvky zmluvných vzťahov medzi prevádzkovateľmi a dodávateľmi, tzv. sprostredkovateľmi, ktoré zabezpečujú efektívne uplatňovanie zásad zákonnosti, minimalizácie údajov, transparentnosti a zodpovednosti v prostredí komplexných a viacúrovňových dodávateľských štruktúr.

POĎAKOVANIE

Financované Európskou úniou – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky v rámci projektu č. 17R05-04-V01-00005.

LITERATÚRA

Filip, S. Šimák, L., Kováč, M. 2011. Manažment rizika. ISBN 9788089393497.Učebnica.

Hotwagner, B.: Supply Chain Risk Management und dessen systemische Umsetzung im Unternehmen. In: Wirtschaft und Management, Band 8. Wien, Fachhochschule des BFI. 2008.ISSN 1812-9056

Kampová. K., 2024. In: Prednášky z predmetu Kontinuity manažment. 2024

Kampová. K., 2025. In: Prednášky z predmetu Kybernetická bezpečnosť. 2025

Metodika analýzy rizík. Riadenie kybernetických bezpečnostných rizík. 2025. [on line]. Dostupné na: https://www.nbu.gov.sk/metodika-analyzy-rizik/

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.(GDPR) [on line]. Dostupné na:

https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti.(NIS 2) [on line]. Dostupné na:

https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=sk

Vyhláška č. 227/2025 Z.z. o bezpečnostných opatreniach podľa zákona o kybernetickej bezpečnosti. [on line].

Dostupné na: https://www.aspi.sk/products/lawText/1/104541/1/2/vyhlaska-c-227-2025-zz-o-bezpecnostnych-opatreniach/vyhlaska-c-227-2025-zz-o-bezpecnostnych-opatreniach

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [on line]. Dostupné na:

https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

Ľubomíra Sokolová, Ing., PhD.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: lubomira.sokolova@uniza.sk

Matúš Madleňák, Ing.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: matus.madlenak@uniza.sk

Timotej Mačuha, Ing.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: timotej.macuha@uniza.sk