ULC | Čarnogurský Law firm

PRO BONO ŠPECIÁL

júl /2025

Naši verní čitatelia si určite spomenú na novembrové číslo bulletinu ULC Čarnogurský Pro Bono z minulého roka 2024, ktorého jeden článok sme venovali kybernetickej bezpečnosti. Podrobnosti nájdete v priloženom linku: https://www.ulclegal.com/buletin/novela-zakona-o-kybernetickej-bezpecnosti-2/. V predmetnom článku sme sa venovali novele zákona o kybernetickej bezpečnosti, ktorá bola prijatá ako reakcia na európsku legislatívu.

Vzhľadom na rozsah a dôležitosť úpravy kybernetickej bezpečnosti, sme sa rozhodli, že v našom aktuálnom letnom, júlovom vydaní bulletinu, Vám prinesieme **rozšírený pohľad na konkrétnu európsku legislatívu upravujúcu oblasť (i) kybernetickej bezpečnosti** a **(ii) digitálnej prevádzkovej odolnosti finančného sektora**, aplikáciu európskej legislatívy a pohľad na podstatné skutočnosti do praxe. Predstavíme Vám takzvanú smernicu NIS 2, ktorej ustanovenia boli transponované do novelizovaného zákona o kybernetickej bezpečnosti a ďalej sa zameriame najmä na nariadenie DORA.

Želáme príjemné čítanie.

1. **POVINNOSŤ OCHRANY VLASTNÝCH DÁT. POZOR, HROZIA POKUTY!**
   Dodržiavanie povinnosti ochrany vlastných dát je s ohľadom na súčasnú legislatívu pre subjekty rovnako dôležité ako uplatňovanie práv fyzických a právnických osôb na ochranu údajov a elektronických dát. Európska a národná legislatíva po novom určuje povinnosti subjektov na ochranu vlastných dát prostredníctvom nových manažérskych postupov a nových povinností. V našom úvodnom článku Vám zhrnieme o aké povinnosti ide, z čoho vyplývajú a na ktoré subjekty sa povinnosti vzťahujú.

2. **SMERNICA NIS 2, JEJ PODSTATA, ROZSAH ÚPRAVY A PRÁVA A POVINNOSTI**
   Smernicou NIS 2 sa stanovuje jednotný právny rámec na podporu kybernetickej bezpečnosti v 18 kritických odvetviach v celej Európskej únií. Smernicou NIS 2 sa zvyšuje spoločná úroveň ambícií Európskej únie v oblasti kybernetickej bezpečnosti prostredníctvom širšieho rozsahu pôsobnosti, jasnejších pravidiel a silnejších nástrojov dohľadu.

3. **NARIADENIE DORA**
   Nariadenie DORA je súčasťou balíka opatrení EÚ, ktorých cieľom je zmierniť riziká kybernetických útokov posilnením digitálnej prevádzkovej odolnosti inštitúcií pôsobiacich na finančnom trhu. Cieľom nariadenia DORA je konsolidovať a vylepšiť požiadavky na riziko informačných a komunikačných technológií ako súčasť požiadaviek na prevádzkové riziko. Zároveň nariadenie DORA upravuje vzťahy vo vybraných oblastiach kybernetickej bezpečnosti finančných inštitúcií, v ktorých je nariadenie DORA považované za nadradený právny akt.

4. **RIADENIE RIZÍK INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ**
   Finančné subjekty musia mať v súlade s nariadením DORA zavedený rámec vnútornej správy a riadenia a kontroly, ktorým sa zabezpečí účinné a obozretné riadenie rizík informačných a komunikačných technológií (IKT) s cieľom dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti. Od finančných subjektov sa vyžaduje, aby vytvorili komplexný rámec riadenia rizík IKT. Čo je riadením rizík a aké opatrenia manažment rizík zahŕňa, sa dočítate na našom článku.

5. **RIADENIE, KLASIFIKÁCIA A NAHLASOVANIE INCIDENTOV SÚVISIACICH S IKT**
   Finančné subjekty sú povinné podľa nariadenia DORA vymedziť, zaviesť a vykonávať proces riadenia incidentov súvisiacich s IKT s cieľom odhaľovať, riadiť a oznamovať incidenty súvisiace s IKT. Finančné subjekty sú povinné zaznamenávať všetky incidenty súvisiace s IKT a významné kybernetické hrozby. S tým súvisí, aby finančné subjekty stanovili vhodné postupy a procesy na zaistenie konzistentného a integrovaného monitorovania, riešenia a následných opatrení v prípade incidentov súvisiacich s IKT s cieľom zabezpečiť, aby sa hlavné príčiny identifikovali, zdokumentovali a riešili s cieľom zabrániť výskytu takýchto incidentov. Podrobnosti v príslušnom článku.

6. **TESTOVANIE DIGITÁLNEJ PREVÁDZKOVEJ ODOLNOSTI**
   Nariadenie DORA vyžaduje, aby poskytovatelia finančných služieb testovali svoje systémy na základe súvisiacich rizík. Testovanie digitálnej prevádzkovej odolnosti je povinné a jeho cieľom je posúdiť pripravenosť na riešenie incidentov súvisiacich s IKT, identifikovať slabé stránky, nedostatky a medzery v digitálnej prevádzkovej odolnosti a urýchlene zaviesť nápravné opatrenia. V našom článku sa podrobnejšie dočítate aj o takzvaných penetračných testoch.

7. **RIADENIE EXTERNÉHO RIZIKA INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ**
   Finančné subjekty sú podľa nariadenia DORA povinné zabezpečiť dôkladné monitorovanie rizík, ktoré plynú od poskytovateľov IKT tretích strán, nahlásiť svoj kompletný register outsourcovaných činností vrátane vnútroskupinových služieb a akékoľvek zmeny v zadávaní kritických služieb externým poskytovateľom služieb IKT, zabezpečiť, aby zmluvy s poskytovateľmi IKT tretích strán obsahovali všetky potrebné podrobnosti. Tieto a ďalšie podrobnosti ohľadom riadenia externého rizika v našom článku.

POVINNOSŤ OCHRANY VLASTNÝCH DÁT. POZOR, HROZIA POKUTY!

1. ABSTRAKT

Dodržiavanie povinnosti ochrany vlastných dát je s ohľadom na súčasnú legislatívu pre subjekty rovnako dôležitá ako uplatňovanie práv fyzických a právnických osôb na ochranu údajov a elektronických dát. Európska a národná legislatíva po novom určuje povinnosti subjektov na ochranu vlastných dát prostredníctvom nových manažérskych postupov a nových povinností. V našom úvodnom článku Vám zhrnieme o aké povinnosti ide, z čoho vyplývajú a na ktoré subjekty sa povinnosti vzťahujú.

2. PRÁVNY RÁMEC

Zhrňme si najpodstatnejšie legislatívne akty, ktoré upravujú povinnosti ochrany vlastných dát.

2.1 Zákon o kybernetickej bezpečnosti

Na národnej úrovni reprezentuje legislatívny rámec **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov v platnom znení (ďalej v celom Pro Bone len ako „**zákon o kybernetickej bezpečnosti**“).

O novele zákona o kybernetickej bezpečnosti, ktorá bola transpozíciou smernice uvedenej nižšie v bode 2.2, sme Vás oboznámili v minuloročnom Pro Bone:
https://www.ulclegal.com/buletin/novela-zakona-o-kybernetickej-bezpecnosti-2/

Novelizovaný zákon o kybernetickej bezpečnosti teda priniesol:

(i) pôsobnosť na prevádzkovateľov základných služieb a prevádzkovateľov kritických základných služieb;

(ii) povinnosť prijímať bezpečnostné opatrenia – firmy, ktoré prevádzkujú základné služby a kritické základné služby musia implementovať opatrenia v oblastiach, ako sú monitorovanie kybernetických hrozieb, správa zraniteľností, riadenie bezpečnostných incidentov a zabezpečenie IT infraštruktúry;

(iii) prísne nahlasovanie kybernetických incidentov, kedy regulovaný subjekt (firma pôsobiaca v kritickej infraštruktúre) má povinnosť hlásiť kybernetické incidenty do 24 hodín od zistenia incidentu musí byť odoslané predbežné hlásenie, do 72 hodín musí byť predložená podrobná správa s analýzou incidentu a do jedného mesiaca od incidentu musí firma predložiť záverečnú správu s implementovanými nápravnými opatreniami;

(iv) dôraz na bezpečnosť dodávateľského reťazca, čo znamená, že firmy musia vykonávať hodnotenie rizík v rámci svojho dodávateľského reťazca a prispôsobiť bezpečnostné politiky podľa výsledkov týchto analýz;

(v) audity, čo znamená, že firmy musia povinne vykonávať pravidelné audity a hodnotenie svojej bezpečnosti a povinne certifikovať bezpečnosť pre vybrané IT produkty a služby.

2.2 Smernica NIS 2

Na úrovni európskej legislatívy je jedným z dôležitých aktov Smernica Európskeho parlamentu a Rady (EÚ) č. 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 (spolu ďalej v celom Pro Bone len ako „**smernica NIS 2**“).

Smernicou NIS 2 sa stanovil jednotný právny rámec na podporu kybernetickej bezpečnosti v 18 kritických odvetviach v celej Európskej únii.

2.3 Nariadenie DORA

Ďalším veľmi podstatným aktom na úniovej úrovni je Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2022/2554 o digitálnej prevádzkovej odolnosti

finančného sektora (ďalej v celom texte Pro Bona ako „**DORA**“)

DORA sa uplatňuje od 17. januára 2025. **Povinnosti z neho vyplývajúce sa však priebežne aplikujú, niektoré ešte len nastanú a pre mnohé subjekty je nariadenie DORA stále veľkou neznámou.**

3. ROZDIELY MEDZI NIS 2 A DORA

Rozdiely medzi NIS2 a DORA spočívajú v:

3.1 Právnej forme:

NIS 2 je **smernica**, čo znamená, že nie je priamo účinná bez transpozície do národného právneho poriadku; transpozícia NIS 2 sa uskutočnila novelou zákona o kybernetickej bezpečnosti.

DORA je **nariadenie**, čo znamená, že je priamo aplikovateľné a má priamy vertikálny a horizontálny účinok na fyzické a právnické osoby.

3.2 Rozsahu pôsobnosti:

Široký sektor - NIS 2 sa vzťahuje na subjekty pôsobiace v **kritickej infraštruktúre, ktorá je nevyhnutná na fungovanie spoločnosti a hospodárstva** štátu; rozsah pôsobnosti NIS 2 zahŕňa celkovo 18 sektorov, akými sú energetika, zdravotníctvo, digitálny sektor, verejné orgány, doprava, zásobovanie vodou, a pod.; ide o rozsah pôsobnosti na oblasti, ktoré môžu mať významný vplyv na verejnú bezpečnosť, poriadok a hospodársku stabilitu v prípade bezpečnostných incidentov, podrobnosti uvádzame v druhom článku tohto špeciálu Pro Bona.

Finančný sektor - DORA, čo znamená, že pre subjekty vo finančnom sektore, ktorí ponúkajú alebo využívajú digitálne služby, napríklad banky, poisťovne, investičné firmy, iných poskytovateľov finančných služieb, poskytovateľov služieb v sektore kryptomien, má DORA prednosť pred NIS 2.

Ide o automatickú reguláciu týchto subjektov nariadením DORA.

3.3 Cieľoch:

Všeobecná kyberbezpečnosť - NIS 2 má posilniť celkovú úroveň kybernetickej bezpečnosti naprieč rôznymi kritickými sektormi v celej EÚ.

Digitálna operačná odolnosť - DORA má zabezpečiť digitálnu operačnú odolnosť finančných inštitúcií, aby mohli odolať a rýchlo sa zotaviť z IT narušení.

3.4 Štruktúre dohľadu:

Podľa **smernice NIS2 monitorovanie vykonávajú výlučne vnútroštátne orgány**, nad subjektmi dotknutými smernicou NIS2 neexistuje priamy dohľad zo strany orgánov EÚ, dohľad je preto výlučne na vnútroštátnej úrovni, na Slovensku je to Národný bezpečnostný úrad (NBÚ).

Naproti tomu **v rámci DORA** sú finančné spoločnosti síce tiež primárne pod dohľadom národných orgánov dohľadu, na Slovensku je to Národná banka Slovenska, ale tie **úzko spolupracujú s orgánmi EÚ**; napríklad Európsky orgán pre cenné papiere a trhy (ESMA), Európsky orgán pre bankovníctvo (EBA) a Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (EIOPA) zohrávajú ústrednú úlohu pri monitorovaní a presadzovaní nariadenia DORA na európskej úrovni; tieto orgány koordinujú činnosti dohľadu a podporujú národné orgány pri zabezpečovaní digitálnej odolnosti vo finančnom sektore.

3.5 Sankciách:

Nedodržiavanie smernice NIS2 a nariadenia DORA môže viesť k významným sankciám. Sankčné mechanizmy týchto dvoch politík však majú odlišné prístupy.

V smernici NIS2 sú pokuty konkrétne definované – subjektom v kritickej infraštruktúre, ako napríklad subjektom v sektore energetiky, dopravy a zdravotníctva, môžu byť udelené pokuty **až do výšky 10 miliónov EUR alebo 2 % ich celosvetového ročného obratu** (podľa toho, ktorá suma je vyššia).

Pre dôležité organizácie, akými sú poskytovatelia digitálnych služieb a chemické spoločnosti, je maximálna pokuta 7 miliónov EUR alebo 1,4 % z celosvetového ročného obratu za predchádzajúci finančný rok.

Nariadenie **DORA, naopak, nestanovuje fixné pokuty za všeobecné nedodržiavanie** predpisov. Existujú však špecifické **pravidlá pre poskytovateľov služieb informačných a komunikačných technológií** (IKT). **DORA umožňuje popredným regulačným orgánom ukladať poskytovateľom IKT pokuty vo výške 1 % z priemerného denného celosvetového obratu** poskytovateľa v predchádzajúcom finančnom roku. Poskytovatelia môžu byť pokutovaní denne až šesť mesiacov, kým nebudú dodržiavať predpisy.

Článok 50 ods. 1 nariadenia DORA stanovuje, že príslušné **orgány musia mať všetky potrebné právomoci v oblasti dohľadu, vyšetrovania a ukladania sankcií** na zabezpečenie uplatňovania tohto nariadenia.

Právomoci zahŕňajú aspoň právomoci (i) mať prístup ku každému dokumentu alebo údaju v akejkoľvek forme, ktorý príslušný orgán považuje za relevantný pre plnenie svojich povinností, a dostať alebo si vyhotoviť jeho kópiu, **(ii)** vykonávať inšpekcie na mieste alebo vyšetrovania, ktoré zahŕňajú, ale neobmedzujú sa na predvolanie zástupcov finančných subjektov, aby podali ústne alebo písomné vysvetlenie k skutočnostiam alebo dokumentom týkajúcim sa predmetu a účelu vyšetrovania, a zaznamenávanie odpovedí a vypočutie akejkoľvek inej fyzickej alebo právnickej osoby, ktorá s týmto vypočutím súhlasí, s cieľom získať informácie týkajúce sa predmetu vyšetrovania, **(iii)** požadovať nápravné a opravné opatrenia v prípade porušení požiadaviek tohto nariadenia.

Bez toho, aby bolo dotknuté právo členských štátov ukladať trestnoprávne sankcie, **členské štáty stanovia pravidlá, ktorými sa zavádzajú primerané administratívne sankcie a nápravné opatrenia za porušenia tohto nariadenia**, a zabezpečia ich účinné vykonávanie. Tieto sankcie a opatrenia musia byť účinné, primerané a odrádzajúce.

Členské štáty **udelia príslušným orgánom právomoc uplatňovať aspoň tieto administratívne sankcie alebo nápravné opatrenia za porušenia tohto nariadenia (i) vydať príkaz,** ktorým sa od fyzickej alebo právnickej osoby požaduje, aby ukončila konanie, ktoré je porušením tohto nariadenia, a zdržala sa opakovania tohto konania, **(ii) požadovať dočasné alebo trvalé ukončenie** uplatňovania akéhokoľvek postupu alebo správania, ktoré sú podľa príslušného orgánu v rozpore s ustanoveniami tohto nariadenia, a zabrániť opakovanému uplatneniu takéhoto postupu alebo správania, **(iii) prijať akýkoľvek druh opatrenia vrátane opatrenia peňažnej povahy** s cieľom zabezpečiť, aby finančné subjekty naďalej dodržiavali právne požiadavky, (iv) požadovať, ak to povoľuje vnútroštátne právo, existujúce **záznamy** o prenose údajov, ktoré má telekomunikačný operátor, ak existuje dôvodné podozrenie porušenia tohto nariadenia a ak takéto záznamy môžu byť relevantné pri vyšetrovaní porušení tohto nariadenia, a (v) vydávať verejné oznámenia vrátane verejných vyhlásení, v ktorých sa uvádza totožnosť fyzickej alebo právnickej osoby a povaha porušenia.

Pri určovaní druhu a úrovne administratívnej sankcie alebo nápravného opatrenia, ktoré sa majú uložiť podľa článku 50, príslušné orgány zohľadňujú rozsah, v ktorom je porušenie úmyselné alebo vyplýva z nedbanlivosti, a všetky iné relevantné okolnosti.

Členské štáty sa môžu rozhodnúť, že nestanovia pravidlá týkajúce sa administratívnych sankcií alebo nápravných opatrení za porušenia, na ktoré

sa podľa ich vnútroštátneho práva vzťahujú trestnoprávne sankcie.

Spoločným aspektom sankčných mechanizmov oboch nariadení je však osobná zodpovednosť manažmentu. NIS2 aj DORA stanovujú, že členovia manažmentu firiem môžu byť zodpovední za hrubú nedbanlivosť alebo úmyselné porušenie pravidiel. To znamená, že manažéri nie sú zodpovední len za implementáciu požiadaviek kybernetickej bezpečnosti, ale môžu čeliť aj osobným dôsledkom za ich nedodržanie.

3.6 Povinnostiach podávania správ:

DORA vyžaduje, aby finančné inštitúcie poskytovali podrobné správy o incidentoch, ktoré by mohli ovplyvniť prevádzkovú odolnosť. Tieto správy musia byť vypracované včas a musia obsahovať podrobné informácie o povahe incidentu a prijatých opatreniach.

NIS2 na druhej strane stanovuje prísnejšie lehoty na hlásenie bezpečnostných incidentov, zvyčajne do 24 hodín, a poskytuje špecifické formáty hlásení v závislosti od sektora. Povinnosti hlásenia podľa NIS2 sú preto často rozsiahlejšie a časovo kritickejšie.

4. REGISTRÁCIA NA NBÚ

V zmysle smernice NIS 2 a zákona o kybernetickej bezpečnosti sa **každý subjekt pôsobiaci v kritickej infraštruktúre musí takzvane samoidentifikovať**, či pod NIS2 spadá a ak áno, v takom prípade sa **zaregistrovať na Národnom bezpečnostnom úrade (NBÚ)**.

Ako sme uviedli vyššie a podrobnejšie uvádzame v druhom článku tohto špeciálu, všeobecne platí, že **pod NIS2 spadajú vybrané subjekty z 18 sektorov, ktoré sú rozdelené do dvoch skupín: (i)** odvetvia s vysokou kritickosťou **a (ii)** iné kritické sektory. Podrobné rozdelenie uvádzame v druhom článku.

Nie všetky subjekty v regulovaných odvetviach automaticky podliehajú NIS 2. Smernica, respektíve zákon o kybernetickej bezpečnosti, sa týka najmä **stredných a veľkých podnikov**, teda tých, ktoré sa **ako stredné a veľké identifikujú na základe hraničných kritérií uvedených v bode 4.1 nižšie**.

Podrobnosti k určovaniu veľkosti podniku uvádza odporúčanie Komisie č. 2003/361/ES, pričom hraničné hodnoty určovania v praxi a prípadové štúdie uvádza napríklad aj Národný bezpečnostný úrad na svojom webovom sídle.

4.1 Definície veľkosti podnikov a hraničné kritériá

Hoci pre účely povinností vyplývajúcich z smernice NIS 2 sú kľúčové stredné a veľké podniky, musíme si zadefinovať komplexné ponímanie veľkosti podnikov podľa odporúčania Komisie č. 2003/361/ES.

V definícii malých a stredných podnikov sa berú do úvahy **hraničné kritériá (i)** počtu pracovníkov, **(ii)** ročného obratu **a (iii)** celkovej ročnej bilančnej sumy.

Porovnaním údajov firmy s takzvanými hraničnými hodnotami pre tieto tri kritériá môže podnik určiť, či je mikropodnikom, malým podnikom alebo stredným podnikom.

Pri posudzovaní veľkosti podniku sa berie do úvahy hraničné kritérium počtu pracovníkov. Zamestnanci/pracovníci sa prepočítavajú na plné úväzky za rok, takzvané ročné pracovné jednotky. 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.

Do počtu pracovníkov sa **nezapočítavajú (i)** učni alebo študenti, ktorí absolvujú odbornú prípravu a majú zmluvy o učňovskej príprave alebo odbornom výcviku **a (ii)** zamestnanci na materskej alebo rodičovskej dovolenke.

Druhé hraničné kritérium si podnik môže vybrať. Môže sa pri posudzovaní **rozhodnúť, či bude spĺňať** maximálnu hodnotu stanovenú pre

obrat alebo maximálnu hodnotu stanovenú pre bilančnú sumu **(súvahu)**. Nemusí spĺňať obe požiadavky, pričom jednu z nich môže aj presiahnuť bez toho, aby to malo vplyv na posudzovanie.

Ročný obrat sa určuje na základe výpočtu príjmov, ktoré podnik počas príslušného roka získal z predaja výrobkov a poskytovania služieb, ktoré patria k bežným činnostiam spoločnosti, po odpočítaní prípadných zliav. Do obratu sa nezapočítava daň z pridanej hodnoty (DPH) ani iné nepriame dane, napríklad spotrebné dane.

4.1.1 Mikropodnik

Mikropodniky sú definované ako podniky, ktoré zamestnávajú **menej než 10 osôb a súčasne ak ich ročný obrat alebo súvaha je menej než 2 milióny** EUR. Mikropodnik nie je pre účely posudzovania aplikácie smernice NIS 2 vo všeobecnosti relevantný, okrem skutočností uvedených nižšie v bode 4.3 tohto článku.

4.1.2 Malý podnik

Malé podniky sú definované ako podniky, ktoré zamestnávajú **menej než 50 osôb a súčasne ich ročný obrat alebo súvaha je menej než 10 miliónov** EUR.

4.1.3 Stredný podnik

Stredné podniky sú definované ako podniky, ktoré zamestnávajú **menej než 250 osôb a súčasne majú buď ročný obrat nižší než 50 miliónov** EUR, **alebo celkovú súvahu menej než 43 miliónov** EUR.

4.1.4 Veľký podnik

Veľkým podnikom je firma v prípade, **ak nie je ani malým a ani stredným podnikom**.

4.2 Príklady posudzovania veľkosti

S ohľadom na hraničné kritériá uvedieme praktické príklady posudzovania veľkosti podniku.

Napríklad podnik, ktorý zamestnáva 51 zamestnancov (ročné pracovné jednotky), má ročný obrat 9 miliónov Eur a rovnako 9 miliónov Eur súvahu. Podnik je napriek obratu a súvahe STREDNÝ, pretože prekročil kritérium veľkosti počtu zamestnancov pre malé podniky.

Príkladom malého podniku je aj ten, ktorý zamestnáva 49 zamestnancov (ročné pracovné jednotky) a má ročný obrat 11 miliónov Eur a ročnú súvahu 9 miliónov Eur. Podnik je MALÝ, pretože kritérium pre súvahu spĺňa hodnoty pre malé podniky.

Napokon, ak napríklad podnik, ktorý zamestnáva 7 zamestnancov (ročné pracovné jednotky), má však ročný obrat 25 miliónov Eur a súvahu 13 miliónov Eur, bude považovaný za STREDNÝ podnik, pretože obe finančné kritériá prekračujú hodnoty malého podniku.

4.3 Kedy veľkosť podniku nie je rozhodujúca

Dôležité však je, že **existujú výnimky, ktoré pod NIS2 spadajú BEZ OHĽADU na veľkosť** podniku, napríklad poskytovatelia verejných elektronických komunikačných sietí alebo služieb, poskytovatelia dôveryhodných služieb a registrov názvov domén najvyššej úrovne, či poskytovatelia DNS služieb.

5. VYSOKÉ SANKCIE

Subjekty spadajúce pod NIS2, teda podniky aktívne v sektore kritickej alebo inej kritickej infraštrukúre, spĺňajúce podmienku veľkosti podniku, resp. bez ohľadu na veľkosť, ak ide o poskytovateľov uvedených v odseku vyššie, majú **povinnosť registrovať sa do 60 dní odo dňa, keď začali vykonávať** podnikateľskú aktivitu podliehajúcu regulácii.

Ak ste podnikom, ktorý už existuje a po nadobudnutí účinnosti smernice NIS 2 ste začali spadať pod jej pôsobnosť, **je potrebné zaregistrovať sa čo najskôr, ak ste tak neurobili do marca 2025, keďže možno očakávať postupný nábeh kontrolných mechanizmov** NBÚ ako orgánu dohľadu.

V prípade nesplnenia registrácie hrozí pokuta za takzvaný správny delikt v sume až do 500 000 eur.

Nesmieme opomenúť aj ďalšie hroziace pokuty, a to až do výšky **7 000 000 eur alebo 1,4 percenta celkového celosvetového ročného obratu za nesplnenie ďalších povinností, ako napríklad (i)** porušenie povinnosti mať prijatú bezpečnostnú dokumentáciu, **(ii)** porušenie povinnosti nahlásiť kybernetický bezpečnostný incident, **(iii)** porušenie povinnosti zasielať automatizovaným spôsobom určené systémové informácie, **(iv)** riešiť kybernetický bezpečnostný incident na základe rozhodnutia úradu podľa § 27 ods. 3 zákona o kybernetickej bezpečnosti, vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5 zákona o kybernetickej bezpečnosti alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok, **(v)** predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie.

V neposlednom rade, NBÚ môže podľa § 31 ods. 3 uložiť pokutu od 500 eur **do 10 000 000 eur alebo do výšky 2 % celkového celosvetového ročného obratu** za predchádzajúce účtovné obdobie, podľa toho, ktorá suma je vyššia, prevádzkovateľovi základnej služby, ktorý prevádzkuje kritickú základnú službu, ktorý sa dopustí správneho deliktu tým, že poruší niektorú z povinností uvedenú v odseku 2, teda niektorú z povinností, ktorú sme uviedli vyššie.

Dôležité postupy v rámci riadenia firiem, za účelom zabezpečenia kybernetickej bezpečnosti firmy podľa nariadenia NIS 2 a zákona o kybernetickej bezpečnosti, **nájdete v našom druhom článku nižšie, najmä v bode 6**, a to vrátane dôležitej novej funkcie v manažovaní firmy, a to funkcie **manažéra kybernetickej bezpečnosti**.

6. DÔLEŽITÉ LEHOTY

Dôležitým je marec 2026. Totiž podľa § 19 ods. 1 zákona o kybernetickej bezpečnosti je prevádzkovateľ základnej služby povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti. Keďže do 2. marca 2025 bolo povinným oznámenie NBÚ zo strany firiem, že sú prevádzkovatelia základnej služby, je zrejmé, že **marec 2026 je hraničná lehota pre prijatie bezpečnostných opatrení** na úseku kybernetickej bezpečnosti.

Dôležitým je tiež marec 2027, keďže podľa § 27 zákona o kybernetickej bezpečnosti je prevádzkovateľ základnej služby povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základnej služby. **Čiže prvý audit alebo samohodnotenie je povinné pre firmy do marca 2027.**

7. ZÁVER

Nariadenie NIS 2 a DORA a všetky k nim delegované nariadenia, sú skutočne rozsiahle a ich dopad na príslušné subjekty, je značný. Podrobnejšiemu výkladu sa venujeme v nasledovných šiestich článkoch letného špeciálu ULC Čarnogurský PRO BONO. V prípade nejasností sme Vám samozrejme k dispozícii, spolu s našim odborne vyškoleným personálom na úseku kybernetickej bezpečnosti.

Publikované dňa 04.09.2025.

SMERNICA NIS 2, JEJ PODSTATA, ROZSAH ÚPRAVY A PRÁVA A POVINNOSTI

1. ABSTRAKT

Smernicou NIS 2 sa stanovil jednotný právny rámec na podporu kybernetickej bezpečnosti v 18 kritických odvetviach v celej Európskej únii. Smernicou NIS 2 sa zvyšuje spoločná úroveň ambícií Európskej únie v oblasti kybernetickej bezpečnosti prostredníctvom širšieho rozsahu pôsobnosti, jasnejších pravidiel a silnejších nástrojov dohľadu.

Smernica je právnym aktom EÚ, ktorý je záväzný pre každý členský štát, ktorému je určený. Smernicou sa stanovujú ciele, ktoré majú dosiahnuť členské štáty EÚ, pričom sa voľba foriem a metód ponecháva na ich vnútroštátne orgány. To znamená, že smernica NIS 2 nie je priamo uplatniteľná sama osebe, ale je potrebná jej tzv. transpozícia do právneho poriadku členského štátu EÚ.

Členské štáty Únie boli povinné prijať a uverejniť do 17. októbra 2024 opatrenia potrebné na dosiahnutie súladu so smernicou NIS 2.

V tomto smere sa vrátime k úvodu nášho špeciálu, kde uvádzame, že v novembrovom čísle 2024 sme Vám predstavili **novelu zákona o kybernetickej bezpečnosti**. Predmetná novela, účinná od 1. januára 2025, bola transpozíciou smernice NIS 2 do slovenského právneho poriadku. Účelom špeciálneho vydania je predstaviť Vám smernicu NIS 2 podrobnejšie, spolu s pohľadom do praxe a jednotlivými právami a povinnosťami, ktoré transponovaná smernica NIS 2 prináša.

2. RÁMCOVÝ POHĽAD NA SMERNICU NIS 2

Kybernetická bezpečnosť zahŕňa **ochranu** sietí a **informačných systémov**, ich používateľov a iných dotknutých osôb pred kybernetickými incidentmi a hrozbami. Smernicou NIS 2 sa zvyšuje spoločná úroveň ambícií EÚ v oblasti kybernetickej bezpečnosti prostredníctvom širšieho rozsahu pôsobnosti, jasnejších pravidiel a silnejších nástrojov dohľadu. Členské štáty EÚ boli, resp. stále sú na základe smernice NIS 2 povinné posilniť **svoje spôsobilosti v oblasti kybernetickej bezpečnosti** a zároveň zaviesť opatrenia na riadenie rizík a požiadavky na podávanie správ subjektom z viacerých odvetví a stanoviť pravidlá spolupráce, výmeny informácií, dohľadu a presadzovania opatrení v oblasti kybernetickej bezpečnosti.

NIS 2 každému členskému štátu ukladá povinnosť prijať **národnú stratégiu kybernetickej bezpečnosti**, ktorá zahŕňa politiky v oblasti bezpečnosti dodávateľského reťazca, riadenia zraniteľnosti a vzdelávania a informovanosti v oblasti kybernetickej bezpečnosti. NIS 2 ukladá každému členskému štátu povinnosť **vytvoriť a pravidelne aktualizovať zoznam prevádzkovateľov základných služieb a zabezpečiť, aby tieto subjekty spĺňali požiadavky smernice**.

NIS 2 obsahuje aj ustanovenia o dohľade, presadzovaní a dobrovoľných partnerských preskúmaniach s cieľom posilniť vzájomnú dôveru a spôsobilosti v oblasti kybernetickej bezpečnosti v celej EÚ. Zavádza sa ním aj zodpovednosť vrcholového manažmentu za nedodržiavanie opatrení na riadenie kyberneticko-bezpečnostných rizík, čím sa kybernetická bezpečnosť musí dostať do pozornosti riadiacich orgánov firiem a spoločností, ktoré spadajú pod 18 kritických odvetví, ktoré si samozrejme neskôr zadefinujeme.

Smernicou sa zriaďuje sieť jednotiek pre riešenie počítačových bezpečnostných incidentov, takzvaných **jednotiek CSIRT**, a to na výmenu informácií o kybernetických hrozbách a reakciu na incidenty.

S cieľom riadiť rozsiahle kybernetické incidenty alebo krízy sa smernicou NIS 2 vytvára **Európska sieť styčných organizácií pre kybernetické krízy, takzvaná EU-CyCLONe**. Táto sieť podporuje koordinované riadenie a zabezpečuje pravidelnú výmenu informácií medzi členskými štátmi a inštitúciami EÚ v prípade rozsiahlych incidentov a kríz.

Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti je zároveň platformou zriadenou smernicou na uľahčenie strategickej spolupráce a výmeny informácií medzi členskými štátmi EÚ, Európskou komisiou a Agentúrou EÚ pre kybernetickú bezpečnosť, takzvaná skupina ENISA. Skupina uverejňuje nezáväzné usmernenia a odporúčania na podporu vykonávania smernice NIS.

3. KYBERNETICKÁ BEZPEČNOSŤ

Vnútorný trh je v plnom rozsahu a viac než kedykoľvek predtým závislý od fungovania internetu. Služby takmer všetkých kľúčových a dôležitých subjektov sú závislé od služieb poskytovaných cez internet. V záujme zabezpečenia bezproblémového poskytovania služieb kľúčovými a dôležitými subjektmi je dôležité, aby všetci poskytovatelia verejných elektronických komunikačných sietí mali zavedené **vhodné opatrenia na riadenie kybernetických rizík a aby oznamovali významné incidenty, ktoré sa ich týkajú**. Ako uvádza smernica NIS 2, členské štáty by mali zabezpečiť zachovanie bezpečnosti verejných elektronických komunikačných sietí a ochranu svojich životne dôležitých bezpečnostných záujmov pred sabotážou a špionážou. Keďže medzinárodná konektivita zlepšuje a urýchľuje konkurencieschopnú digitalizáciu Európskej únie a jej hospodárstva, **incidenty na úrovni kybernetického priestoru sa majú oznamovať príslušným subjektom, teda tzv. jednotke CSIRT alebo prípadne príslušnému orgánu**. V národnej stratégii kybernetickej bezpečnosti by sa v prípade potreby mala zohľadňovať kybernetická bezpečnosť a mala by zahŕňať mapovanie potenciálnych kybernetických rizík a zmierňujúce opatrenia na zabezpečenie najvyššej úrovne ich ochrany.

Smernica NIS 2 stanovuje opatrenia, ktorých zámerom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii **na účely lepšieho fungovania vnútorného trhu**.

Na uvedený účel smernica NIS 2 stanovuje (i) povinnosti, ktorými sa od členských štátov vyžaduje, aby prijali národné stratégie kybernetickej bezpečnosti a určili alebo zriadili príslušné orgány, orgány pre riadenie kybernetických kríz, jednotné kontaktné miesta pre kybernetickú bezpečnosť (jednotné kontaktné miesta) a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT); **(ii) opatrenia** na riadenie kybernetických rizík a oznamovacie povinnosti pre príslušné subjekty, ako aj pre subjekty identifikované ako kritické subjekty, **(iii) pravidlá a povinnosti výmeny** informácií o kybernetickej bezpečnosti, **(iv) povinnosti členských štátov** v oblasti dohľadu a presadzovania práva.

Smernica NIS 2 pokrýva viac sektorov a zvyšuje rozsah spoločností, resp. firiem a podnikov podliehajúcich regulácii.

Smernica NIS 2 zavádza prísnejšie bezpečnostné opatrenia pre zlepšenie kybernetickej ochrany.

Smernica NIS 2 zvyšuje zodpovednosť a transparentnosť, spoločnosti, resp. firmy a podniky musia poskytovať pravidelné správy o svojich bezpečnostných opatreniach.

Smernica NIS 2 vytvára mechanizmy pre lepšiu výmenu informácií a koordináciu reakcií na incidenty medzi členskými štátmi EÚ.

Smernica NIS2 podporuje výstavbu a údržbu pokročilých systémov na detekciu a reakciu na kybernetické hrozby.

4. ROZSAH PÔSOBNOSTI

Je potrebné zdôrazniť, že smernica NIS2 sa týka členských štátov EÚ.

Pokiaľ ide o konkrétnu pôsobnosť voči konkrétnemu subjektu, či firme, ich sa dotýka novelizovaný zákon o kybernetickej bezpečnosti, ktorý prevzal jednotlivé ustanovenia zo smernice NIS 2 a o ktorom sa dočítate v našom samostatnom článku: https://www.ulclegal.com/buletin/novela-zakona-o-kybernetickej-bezpecnosti-2/.

Smernica NIS 2, ako aj predmetná novela zákona o kybernetickej bezpečnosti (vyplývajúci aj z NIS2) vyžaduje od spoločností zlepšenie bezpečnostných politík, zavedenie opatrení proti kybernetickým hrozbám a posilnenie incidentného manažmentu.

Spoločnosti by mali vykonávať **pravidelné bezpečnostné audity, aktualizovať svoje bezpečnostné systémy a školiť zamestnancov** v oblasti kybernetickej bezpečnosti. Pomôcť môžu aj firmy a odborníci v oblasti kyberbezpečnosti.

Nesúlad s legislatívou môže viesť k vysokým finančným pokutám, právnym dôsledkom a poškodeniu reputácie spoločnosti na trhu.

5. DELENIE SUBJEKTOV

Smernica NIS 2 sa zameriava na zvýšenie odolnosti a schopnosti reakcie na kybernetické hrozby nielen verejných subjektov, ale podstatným spôsobom **rozširuje pôsobnosť aj na súkromný sektor**, akým je napríklad automobilový priemysel, potravinárstvo či výroba.

V nadväznosti na rámcovú úpravu smernicou NIS 2 novela zákona o kybernetickej bezpečnosti, o ktorej sme písali v minuloročnom vydaní nášho bulletinu, sú **regulované subjekty povinné zaviesť prísnejšie bezpečnostné opatrenia, ako je monitorovanie sietí, správu zraniteľností či včasné hlásenie kybernetických incidentov**.

Regulované subjekty sú súčasťou 18 sektorov určených smernicou NIS 2.

Subjekty sú podľa zákona rozdelené do dvoch kategórií, a to **sektory s vysokou kritickosťou** (podľa prílohy č. 1 smernice NIS 2) a **iné kritické sektory** (podľa prílohy č. 2 smernice NIS 2).

Celkovo ide o 18 sektorov.

5.1 Sektory s vysokou kritickosťou

Medzi sektory s vysokou kritickosťou smernica NIS 2 zaraďuje (i) energetiku, **(ii)** dopravu, **(iii)** bankovníctvo, **(iv)** infraštruktúru finančných trhov, **(v)** zdravotníctvo, **(vi)** sektor pitnej vody, **(vii)** sektor odpadovej vody, **(viii)** digitálnu infraštruktúru, **(ix)** riadenie služieb informačných a komunikačných technológií, **(x)** verejnú správu, **(xi)** vesmír.

5.2 Iné kritické sektory

Medzi iné kritické sektory smernica NIS 2 zaraďuje (xii) poštové a kuriérske služby, **(xiii)** odpadové hospodárstvo, **(xiv)** výrobu a distribúciu chemických látok, **(xv)** výrobu, spracovanie a distribúciu potravín, **(xvi)** výrobu, **(xvii)** poskytovateľov digitálnych služieb **a (xviii)** výskum.

Zdôrazňujeme však, že nestačí, ak subjekt iba vykonáva činnosť v niektorom z vyššie uvedených sektorov prípadne podsektorov, ktoré sú uvedené v prílohách č. 1 a 2 smernice NIS 2.

Musí sa aj samoidentifikovať ako typ subjektu.

Pravidlá smernice NIS 2 prevzal novelizovaný zákon o kybernetickej bezpečnosti a **existuje prahová hodnota veľkosti subjektu** (stredné podniky podľa článku 2 prílohy k odporúčaniu Komisie 2003/361/ES alebo presahujúce limity pre stredné podniky). Veľkosť podniku sa posudzuje podľa Odporúčania Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003). Prvým kritériom na posudzovanie veľkosti podniku je **počet zamestnancov** a druhým kritériom na posudzovanie veľkosti podniku je **ročný obrat alebo celková ročná bilancia, teda súvaha**.

Čiže na to, aby bol subjekt zaradený do registra prevádzkovateľov základnej služby, musí subjekt spĺňať zároveň aj veľkostné kritérium – ide o **minimálne stredný podnik určený na základe kritérií, ktoré sme Vám vysvetlili v prvom článku v bode 4.1.**

Sú tu však aj subjekty, na ktorých sa povinnosti zákona vzťahujú, a to aj bez splnenia tohto veľkostného kritéria či zaradenia do sektora, a tým sú (i) ústredné orgány štátnej správy a iné štátne orgány s celoštátnou pôsobnosťou, **(ii) kritický subjekt**, **(iii) štátne orgány vykonávajúce pôsobnosť v najmenej dvoch okresoch a vyšší územný celok**, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, **(iv) mesto**, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, **(v) správca informačných technológií verejnej správy** po predchádzajúcej konzultácii s príslušným ústredným orgánom, **(vi) osoba, ktorá poskytuje službu registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik **alebo (vii) tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti**, má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

Smernica NIS 2 spolu s novelizovaným zákonom o kybernetickej bezpečnosti zaviedla takzvané **kritické základné služby, ktorými sú (i)** výkon pôsobnosti ústredného orgánu štátnej správy alebo iného štátneho orgánu s celoštátnou pôsobnosťou, **(ii)** činnosti v sektoroch podľa prílohy č. 1 smernice NIS 2, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá presahuje podmienky veľkosti pre stredný podnik (min. 250 zamestnancov alebo obrat 50 mil. EUR / súvaha 43mil. EUR a viac), **(iii)** kvalifikovaná dôveryhodná služba, **(iv)** správa domén najvyššej úrovne, **(v)** služba DNS, teda systému názvov domén, **(vi)** poskytovanie verejnej EK siete alebo verejnej EK služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik, **(vii)** poskytovanie základnej služby kritickým subjektom, **(viii)** informačná činnosť a elektronické služby, vykonávané s použitím informačných technológií verejnej správy.

6. OPATRENIA NA RIADENIE KYBERNETICKÝCH RIZÍK

Smernica NIS 2 určila členským štátom EÚ, aby zabezpečili, aby kľúčové a dôležité subjekty v kritických sektoroch prijali vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby.

Uvedené **opatrenia sú založené na prístupe zohľadňujúcom všetky riziká**, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi, a **zahŕňajú aspoň (i) zásady analýzy** rizík a bezpečnosti informačných systémov, **(ii) riešenie incidentov, (iii) kontinuitu činností**, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie, **(iv) bezpečnosť dodávateľského reťazca** vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb, **(v) bezpečnosť pri nadobúdaní, vývoji a údržbe siete** a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach, **(vi) zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík, (vii) základné postupy kybernetickej hygieny** a odborná príprava v oblasti kybernetickej bezpečnosti, **(viii) zásady a postupy používania kryptografie**, prípadne šifrovania, **(ix) bezpečnosť ľudských zdrojov**, zásady kontroly prístupu a správu aktív, **(x) v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie**, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

Z uvedeného vyplýva pre **spoločnosti a firmy spĺňajúce definíciu subjektu** v rámci kritickej infraštruktúry a kritických sektorov, že **musia**:

(i) zaviesť systém riadenia kybernetickej bezpečnosti, ktorý určí zodpovednosti a procesy na ochranu ich údajov a systémov,

(ii) aktívne monitorovať a aktualizovať svoje systémy na ochranu pred novými zraniteľnosťami a hrozbami,

(iii) mať zavedené postupy na detekciu, reakciu a riešenie kybernetických bezpečnostných incidentov,

(iv) zabezpečiť, aby ich systémy zostali funkčné aj počas krízových situácií, napríklad vďaka zálohovaniu dát a testovaniu obnovy systémov,

(v) priebežne identifikovať a riadiť riziká a potenciálne nedostatky v informačných systémoch a včas eliminovať alebo minimalizovať ich vplyv,

(vi) zabezpečiť, aby softvérové a sieťové vybavenie prešli bezpečnostnými auditmi pred uvedením do prevádzky,

(vii) pravidelne hodnotiť účinnosť svojich bezpečnostných opatrení, napríklad prostredníctvom auditov,

(viii) zaviesť systém správy identít a prístupov a určiť kto môže pristupovať k jednotlivým systémom a údajom, a pod akými podmienkami, teda určenie mechanizmu overovania prístupu pomocou viacfaktorovej autentifikácie,

(ix) na ochranu citlivých údajov používať šifrovacie technológie a kryptografiu,

(x) pravidelne monitorovať a ochraňiť dátové prenosy,

(xi) vzdelávaním svojich zamestnancov zabezpečiť, aby rozumeli kybernetickým hrozbám a dodržiavali bezpečnostné zásady,

(xii) používať softvérové riešenia na detekciu a blokovanie škodlivého obsahu,

(xiii) zabezpečiť, aby všetky dôležité udalosti a incidenty boli sledované, zaznamenávané a vyhodnocované a hlásené kompetentným orgánom,

(xiv) chrániť citlivé informácie, zabezpečiť súkromie svojich používateľov,

(xv) riadiť riziká spojené s dodávateľmi, ktorí môžu mať prístup k ich aktívam,

(xvi) implementovať bezpečnostné opatrenia na ochranu priestorov a kontrolovať prístup k týmto priestorom.

Zjednodušene povedané, ide o povinnosť nasledovných opatrení zo strany firiem:

- identifikovať zraniteľnosti, kybernetické hrozby a riziká;
- detegovať nežiaduce udalosti a incidenty;
- reagovať na identifikované zraniteľnosti a incidenty a minimalizovať ich vplyv;
- riešiť a reagovať na kybernetické bezpečnostné incidenty;
- obnoviť informačné aktíva, napraviť negatívne dopady po vzniku incidentu a uviesť poskytované služby do požadovaného stavu;
- vykonávať analýzu rizík a bezpečnosti sietí a systémov;
- dohliadať na bezpečnosť sietí a informačných systémov;
- zabezpečiť kontinuitu činností, riadenie zálohovania a obnovu systému incidente;
- krízové riadenie;
- zabezpečiť bezpečnosť dodávateľského reťazca;
- dodržiavať zásady a postupy posudzovania účinnosti prijatých bezpečnostných opatrení na riadenie kybernetických rizík;
- dodržiavať zásady a postupy používania kryptografie alebo šifrovania;
- dodržiavať bezpečnosť ľudských zdrojov;
- využívať viacstupňovú alebo kontinuálnu autentifikáciu.

Uvedené povinnosti sú transponované do zákona o kybernetickej bezpečnosti.

6.1 Oznamovacie povinnosti

Oznamovacie povinnosti v zmysle nariadenie NIS 2, transponované do novely zákona o kybernetickej bezpečnosti, sme si podrobnejšie vysvetlili v minuloročnom článku nášho bulletinu: https://www.ulclegal.com/buletin/novela-zakona-o-kybernetickej-bezpecnosti-2/

6.2 Manažér kybernetickej bezpečnosti

Smernica NIS 2 a zákon o kybernetickej bezpečnosti určili, aby firmy spadajúce pod pôsobnosť týchto legislatívnych aktov, mali tzv. **manažéra kybernetickej bezpečnosti.**

Ide o novú, povinnú funkciu, respektíve externú funkciu v štruktúre firmy.

Určenie manažéra kybernetickej bezpečnosti je jedným z minimálnych bezpečnostných opatrení firmy.

Manažér kybernetickej bezpečnosti je v zmysle zákona o kybernetickej bezpečnosti pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti.

Samohodnotenie je tiež vykonávané manažérom kybernetickej bezpečnosti. Ide vlastne o audit firmy na úseku kybernetickej bezpečnosti. Prvý audit sa musí vykonať do marca 2027.

Manažér kybernetickej bezpečnosti je novou viazanou živnosťou, nazvanou „Certifikovaný audítor kybernetickej bezpečnosti“.

Manažéri kybernetickej bezpečnosti musia spĺňať požiadavky medzinárodných štandardov ISO/IEC noriem radu 27000, ktoré predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti.

7. NÁRODNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI

Smernica NIS 2 určila, že každý členský štát EÚ prijme **národnú stratégiu kybernetickej bezpečnosti**, v ktorej stanoví strategické ciele, zdroje potrebné na dosiahnutie týchto cieľov a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti.

Národná stratégia kybernetickej bezpečnosti sietí obsahuje (i) ciele a priority stratégie kybernetickej bezpečnosti členského štátu najmä pre kritické odvetvia uvedené vyššie, **(ii)** rámec riadenia na dosiahnutie cieľov a priorít uvedených v prvom bode, vrátane politík zameraných na kybernetickú bezpečnosť, **(iii)** rámec riadenia na objasnenie úloh a povinností relevantných zainteresovaných strán na vnútroštátnej úrovni, ktorý je základom spolupráce a koordinácie na vnútroštátnej úrovni medzi príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT podľa tejto smernice, ako aj koordináciu a spoluprácu medzi uvedenými orgánmi a príslušnými orgánmi podľa odvetvových právnych aktov Únie, **(iv)** mechanizmus na identifikáciu relevantných prostriedkov a hodnotenie rizík v danom členskom štáte, **(v)** identifikáciu opatrení na zabezpečenie pripravenosti a schopnosti reakcie na incidenty a zotavenia z nich vrátane spolupráce medzi verejným a súkromným sektorom, **(vi)** zoznam rôznych orgánov a zainteresovaných strán zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti, **(vii)** politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa smernice NIS 2 a príslušnými orgánmi za účelom výmeny informácií o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch, prípadne pri plnení úloh dohľadu, **(viii)** plán vrátane potrebných opatrení na zvýšenie všeobecnej úrovne informovanosti občanov o kybernetickej bezpečnosti.

Národná stratégia kybernetickej bezpečnosti Slovenska je dostupná na webovom sídle Národného bezpečnostného úradu: https://www.nbu.gov.sk/data/att/396.pdf.

Národný bezpečnostný úrad SR je zároveň najvyšším štátnym orgánom na úseku kybernetickej bezpečnosti a zabezpečuje komplexnú koncepciu štátnej politiky na úseku kybernetickej bezpečnosti, ako orgán v súlade so smernicou NIS 2.

8. NÁRODNÁ JEDNOTKA CSIRT

Smernica NIS 2 určila, že každý členský štát EÚ je **povinný zriadiť tzv. jednotku CSIRT**. Skratka CSIRT znamená Computer Security Incident Response Team, teda jednotka pre riešenie počítačových bezpečnostných udalostí (incidentov).

Národná jednotka CSIRT je **zriadená ako samostatný odbor na Ministerstve investícií, regionálneho rozvoja a informatizácie SR** a zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci celej IT VS. Poskytuje aj služby preventívneho a vzdelávacieho charakteru.

Národná jednotka CSIRT (i) rieši kybernetické bezpečnostné incidenty v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí informačných technológií verejnej správy, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy), **(ii)** buduje a rozširuje povedomie verejnosti vo vybraných oblastiach informačnej, resp. kybernetickej bezpečnosti, **(iii)** kooperuje s partnerskými organizáciami a združeniami v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni.

Národné jednotky CSIRT sú v zmysle smernice NIS 2 povinné spĺňať vysokú odbornosť a a vysokú úroveň dostupnosti komunikačných kanálov, byť vybavené odborným personálom, byť vybavené vhodnými systémami riadenia, a podobne.

Jednotky CSIRT (i) monitorujú a analyzujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni a na požiadanie poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom s ohľadom na monitorovanie ich sietí a informačných systémov v reálnom alebo takmer v reálnom čase, **(ii) zasielajú** včasné varovania, výstrahy a oznámenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch dotknutým kľúčovým a dôležitým subjektom, ako aj príslušným orgánom a ďalším relevantným zainteresovaným stranám pokiaľ možno takmer v reálnom čase, **(iii) podľa potreby reagujú na incidenty a poskytujú pomoc** dotknutým kľúčovým a dôležitým subjektom, **(iv) zhromažďujú a analyzujú forenzné údaje** a poskytujú dynamickú analýzu rizík a incidentov a informácie o situácii v kybernetickej bezpečnosti, **(v) na žiadosť kľúčového alebo dôležitého subjektu umožňujú aktívne skenovanie** siete a informačných systémov dotknutého subjektu s cieľom odhaľovať zraniteľnosti s potenciálnym významným dosahom, **(vi)** majú účasť v sieti jednotiek CSIRT a poskytujú vzájomnú pomoci podľa svojich kapacít a kompetencií ostatným členom siete jednotiek CSIRT na ich žiadosť, **(vii) v prípade potreby pôsobia ako koordinátor** na účely koordinovaného zverejňovania zraniteľností, **(viii)** prispievajú k zavádzaniu bezpečných nástrojov na výmenu informácií.

Jednotky CSIRT **môžu vykonávať aktívne nerušivé skenovanie verejne prístupných sietí a informačných systémov** kľúčových a dôležitých subjektov. Takéto skenovanie sa vykonáva s cieľom odhaliť zraniteľné alebo nezabezpečene nakonfigurované siete a informačné systémy a informovať dotknuté subjekty. Takéto skenovanie nesmie mať negatívny vplyv na fungovanie služieb subjektov.

Na účely koordinovaného zverejňovania zraniteľností určí každý členský štát jednu zo svojich jednotiek CSIRT za koordinátora. Jednotka CSIRT určená za koordinátora koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby sprostredkuje interakciu medzi fyzickou alebo právnickou osobou, ktorá na žiadosť niektorej zo strán oznamuje zraniteľnosť a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov informačných

a komunikačných technológií (ďalej len „IKT“) alebo služieb IKT.

K úlohám jednotky CSIRT určenej za koordinátora patrí **(i) identifikácia a kontaktovanie dotknutých subjektov, (ii) pomoc fyzickým alebo právnickým osobám** oznamujúcim zraniteľnosti **a (iii) vyjednávanie harmonogramu zverejňovania a riadenie zraniteľností**, ktoré majú dosah na viaceré subjekty.

Smernica NIS 2 určila, že každý štát EÚ má zabezpečiť, aby **fyzické alebo právnické osoby mohli na požiadanie nahlásiť zraniteľnosť jednotke CSIRT určenej za koordinátora, a to anonymne**. Jednotka CSIRT určená za koordinátora zabezpečí v súvislosti s oznámenou zraniteľnosťou vykonanie dôsledných následných opatrení a zabezpečí anonymitu fyzickej alebo právnickej osoby, ktorá túto zraniteľnosť oznámila. Ak by oznámená zraniteľnosť mohla by mať významný vplyv na subjekty vo viac ako jednom členskom štáte, jednotka CSIRT každého dotknutého členského štátu určená za koordinátora v prípade potreby spolupracuje s inými jednotkami CSIRT určenými za koordinátorov v rámci siete jednotiek CSIRT.

Samozrejme, smernica NIS 2 stanovuje spoluprácu jednotlivých členských štátov a jednotiek CSIRT na základe skupín pre spoluprácu.

Jednoducho povedané, celospoločenská kybernetická bezpečnosť je komplexne zastrešená na vnútroštátnej a úniovej úrovni na základe spolupráce a výmeny informácií a siete jednotlivých jednotiek CSIRT každého členského štátu.

9. SIEŤ EU-CyCLONe

Smernica NIS 2 určila, že takzvaná **sieť EU-CyCLONe sa zriaďuje s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni** a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie.

Sieť EU-CyCLONe tvoria **zástupcovia orgánov členských štátov pre riadenie kybernetických kríz** a v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetický incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti patriace do rozsahu pôsobnosti tejto smernice, aj zástupcovia Komisie. Vo všetkých ostatných prípadoch sa Komisia zúčastňuje na činnostiach siete EU-CyCLONe ako pozorovateľ.

Sieť EU-CyCLONe (i) zvyšuje úroveň pripravenosti na riadenie rozsiahlych kybernetických incidentov a kríz, **(ii) rozvíja spoločné situačné povedomie** o rozsiahlych kybernetických incidentoch a krízach, **(iii) posudzuje dôsledky a vplyv** relevantných rozsiahlych kybernetických incidentov a kríz a navrhuje možné zmierňujúce opatrenia, **(iv) koordinuje riadenie rozsiahlych kybernetických incidentov** a kríz a podporuje rozhodovanie na politickej úrovni v súvislosti s takýmito incidentmi a krízami, **(v) na žiadosť príslušného členského štátu prediskutuje národné plány** reakcie na rozsiahle kybernetické incidenty a krízy.

Táto sieť samozrejme spolupracuje s národnými jednotkami CSIRT.

10. SANKCIE

Smernica NIS 2 určuje, že členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení vnútroštátnych opatrení prijatých podľa tejto smernice, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce.

Sankcie sú upravené v novelizovanom zákone o kybernetickej bezpečnosti.

Sankcie sú stanovené na skutočne vysokej úrovni, a to od 300 EUR **až do 10.000.000 EUR, resp. až do výšky 2 percent z celkového celosvetového ročného obratu firmy**, ktorá je subjektom kritickej infraštruktúry, a to v závislosti od charakteru a závažnosti porušenia zákona o kybernetickej bezpečnosti.

Zákon určuje veľmi podrobný rozsah porušenia povinností subjektu kritickej infraštruktúry, uvedieme **porušenia** azda tých **najdôležitejších povinností, napríklad porušenie (i)** povinnosti prijať bezpečnostnú dokumentáciu, **(ii)** povinnosti nahlásiť závažný kybernetický incident, **(iii)** povinnosti zasielať automatizovaným spôsobom určené systémové informácie, **(iv)** povinnosti riešiť kybernetický bezpečnostný incident, a ďalšie.

11. DÔLEŽITÉ LEHOTY

Do registra prevádzkovateľov základnej služby sú subjekty kritickej infraštruktúry, ústredné orgány štátnej správy a vybrané subjekty určené ust. § 17 ods. 1 zákona o kybernetickej bezpečnosti, teda subjekty, ktoré uvádzame v tomto článku vyššie, povinné sa **zaregistrovať do 60 dní odo dňa začatia vykonávania činnosti v kritických sektoroch**. Tie **subjekty, ktoré už činnosť vykonávajú, mali povinnosť registrácie do 2. marca 2025**.

Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti.

Čiže bezpečnostné opatrenia je povinné prijať do marca 2026.

Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených zákonom o kybernetickej bezpečnosti **vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov** základnej služby, **potom každé 2 roky alebo pri významnej zmene**.

Čiže prvý audit je povinné zrealizovať do marca 2027.

Zopakujeme tiež dôležité lehoty v rámci procesu hlásenia závažných kybernetických bezpečnostných incidentov, a to nahlásiť taký incident **bez zbytočného odkladu, avšak (i) najneskôr do 24 hodín od jeho zistenia** sa hlási včasné varovanie, v ktorom sa uvádza, či incident mohol byť spôsobený protiprávnym konaním, alebo či môže mať cezhraničný vplyv (ak ide o poskytovateľa dôveryhodných služieb, uvádza sa aj vplyv na poskytovanie týchto služieb), **(ii) najneskôr do 72 hodín** od jeho zistenia sa hlási oznámenie o závažnom kybernetickom bezpečnostnom incidente, v ktorom sa aktualizujú a dopĺňajú informácie z včasného varovania (prvé posúdenie incidentu, jeho závažnosti a následkov (v prípade poskytovateľa dôveryhodných služieb najneskôr do 24 hodín).

Rozsah a dopad nariadenia NIS 2 a zákona o kybernetickej bezpečnosti, do ktorého SR transponovala uvedenú smernicu, je značný. V prípade nejasností alebo konzultácie, nás neváhajte kontaktovať.

Publikované dňa 04.09.2025.

NARIADENIE DORA

1. ABSTRAKT

Nariadenie DORA sa uplatňuje od 17. januára 2025. **Povinnosti z neho vyplývajúce sa však priebežne aplikujú, niektoré ešte len nastanú a pre mnohé subjekty je nariadenie DORA stále veľkou neznámou.**

Nariadenie DORA je súčasťou balíka opatrení EÚ, ktorých cieľom je ďalej umožniť a podporiť potenciál digitálnych financií v oblasti inovácií a hospodárskej súťaže a zároveň zmierniť príslušné riziká kybernetických útokov posilnením digitálnej prevádzkovej odolnosti inštitúcií pôsobiacich na finančnom trhu. Cieľom nariadenia DORA je konsolidovať a vylepšiť požiadavky na riziko informačných a komunikačných technológií ako súčasť požiadaviek na prevádzkové riziko. Zároveň nariadenie DORA upravuje vzťahy vo vybraných oblastiach kybernetickej bezpečnosti finančných inštitúcií, v ktorých je nariadenie DORA považované za nadradený právny akt.

DORA je nariadením, teda právnym aktom EÚ, ktorý je priamo účinný pre všetky relevantné subjekty.

Nebola potrebná transpozícia nariadenia DORA do slovenského právneho poriadku, avšak niektoré ustanovenia, ktoré sú nevyhnutné k harmonizácii slovenského právneho poriadku s týmto nariadením, bolo potrebné novelizovať. V tomto smere ešte na jeseň roka 2024, došlo v októbri 2024 k schváleniu novely zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v platnom znení, ako aj novely ďalších zákonov, súvisiace s implementáciou smernice DORA v sektorových zákonoch finančného trhu - zákon o bankách, zákon o cenných papieroch, zákon o burze cenných papierov, zákon o doplnkovom dôchodkovom sporení, zákon o platobných službách, zákon o kolektívnom investovaní, zákon o riešení krízových situácií a zákon o poisťovníctve.

2. JEDNOTNĚ POŽIADAVKY

S cieľom dosiahnuť vysokú spoločnú úroveň digitálnej prevádzkovej odolnosti sa v tomto **nariadení stanovujú tieto jednotné požiadavky týkajúce sa kyberbezpečnosti sietí a informačných systémov** podporujúcich obchodné procesy finančných subjektov:

(i) **riadenie a identifikácia rizík súvisiacich s informačno-komunikačnými technológiami** (ďalej len „IKT“) - DORA vymedzila základné požiadavky a povinnosti na kyberbezpečnosť, čo znamená, že manažment finančného subjektu je zodpovedný za riadenie rizík súvisiacich s IKT; finančné subjekty musia mať zavedený spoľahlivý, komplexný a dobre zdokumentovaný rámec riadenia rizík, ktorý im umožní riešiť IKT riziká rýchlo, efektívne a komplexne;

(ii) **incidenty súvisiace s IKT** - finančné subjekty sú povinné vyvinúť a zaviesť proces riadenia IKT incidentov so schopnosťou monitorovať, riešiť a dosledovať tieto incidenty, závažné incidenty musia byť nahlásené príslušným dotknutým orgánom;

(iii) **simulácie a testovanie prevádzkovej digitálnej odolnosti** - DORA zaviedla povinnosť testovania digitálnej prevádzkovej odolnosti; pre vybrané finančné subjekty sa testovanie posúva od bežného testovania až na testovanie treťou stranou, kde sa simuluje bežný incident alebo útok, aby sa overilo, nielen aký je bezpečnostný stav systémov, ale aj riadenie incidentov a schopnosť rozpoznať útok a reagovať;

(iv) **spolupráca a komunikácia medzi finančnými subjektmi** - aby sa posilnila digitálna prevádzková bezpečnosť a zvýšilo sa povedomie o aktuálnych hrozbách, finančné subjekty

môžu medzi sebou zdieľať informácie o útokoch a rizikách v rámci dôveryhodných spoločenstiev a v súlade s ochranou dát, obchodného tajomstva a konkurencieschopnosti;

(v) **outsourcing a riadenie tretích strán** - DORA vyžaduje od finančných subjektov, aby viedli register zmlúv a zmluvných podmienok so všetkými dodávateľmi IKT; po novom sú IKT firmy hodnotené dohľadnými orgánmi Európskych dozorných úradov;

(vi) vzdelávanie **pracovníkov** - pravidelné školenie pracovníkov podľa požiadaviek DORA má za cieľ pochopenie požiadaviek a krokov v súvislosti s bezpečnostnými hrozbami v kyberpriestore;

(vii) **pravidlá zriadenia a vykonávania rámca dozoru** nad kritickými externými poskytovateľmi IKT služieb.

3. ROZSAH PÔSOBNOSTI A SUBJETKY

Nariadenie sa vzťahuje na rôzne druhy entít z finančného sektora – tzv. **„finančné subjekty“**.

Ide o (i) úverové inštitúcie, **(ii)** platobné inštitúcie vrátane platobných inštitúcií vyňatých podľa smernice (EÚ) 2015/2366, **(iii)** poskytovateľov služieb informovania o účte, **(iv)** inštitúcie elektronického peňažníctva vrátane inštitúcií elektronického peňažníctva vyňatých podľa smernice 2009/110/ES, **(v)** investičné spoločnosti, **(vi)** poskytovateľov služieb kryptoaktív, ktorým bolo udelené povolenie podľa nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (ďalej len „nariadenie o trhoch s kryptoaktívami“) a emitenti tokenov krytých aktívami, **(vii)** centrálne depozitáre cenných papierov, **(viii)** centrálne protistrany, **(ix)** obchodné miesta, **(x)** archívy obchodných údajov, **(xi)** správcov alternatívnych investičných fondov, **(xii)** správcovské spoločnosti, **(xiii)** poskytovateľov služieb vykazovania údajov, **(xiv)** poisťovne a zaisťovne, **(xv)** sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia, **(xvi)** inštitúcie zamestnaneckého dôchodkového zabezpečenia, **(xvii)** ratingové agentúry, **(xviii)** správcov kritických referenčných hodnôt, **(xix)** poskytovateľov služieb hromadného financovania, **(xx)** archívy sekuritizačných údajov **a (xxi)** externých poskytovateľov IKT služieb.

V skratke, nariadenie je priamo účinné a dotýka sa od bánk, poisťovní cez investičné spoločnosti až po štatutárnych audítorov, vrátane externých dodávateľov, ktorí poskytujú digitálne a dátové služby, vrátane cloud computingu, softvéru, služieb analýzy dát, dátových centier.

Naopak, nariadenie DORA sa neuplatňuje na (i) správcov alternatívnych investičných fondov, ako sa uvádza v článku 3 ods. 2 smernice 2011/61/EÚ; **(ii)** poisťovne a zaisťovne, ale iba podľa článku 4 smernice 2009/138/ES, **(iii)** inštitúcie zamestnaneckého dôchodkového zabezpečenia, ktoré prevádzkujú dôchodkové plány, ktoré spolu nemajú viac ako 15 členov, **(iv)** fyzické alebo právnické osoby oslobodené podľa článkov 2 a 3 smernice 2014/65/EÚ, **(v)** sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia, ktorými sú mikropodniky alebo malé alebo stredné podniky, **(vi)** poštové sporožírové inštitúcie ako sa uvádza v článku 2 ods. 5 bode 3 smernice 2013/36/EÚ.

Výnimkou sú teda, v skratke povedané, poskytovatelia hardvérových komponentov a spoločnosti, ktoré poskytujú elektronické komunikačné služby alebo im bolo udelené povolenie podľa práva Únie.

4. VYMEDZENIE POJMOV

Považujeme za dôležité pred tým, než v ďalších článkoch prejdeme k praktickej stránke aplikácie nariadenia DORA, vymedziť niektoré pojmy, s ktorými nariadenie pracuje. Vyberáme iba niektoré pojmy, ktoré považujeme za kľúčové.

„Digitálna prevádzková odolnosť“ je schopnosť finančného subjektu budovať, zabezpečovať a preskúmavať svoju prevádzkovú integritu a spoľahlivosť tak, že priamo alebo nepriamo prostredníctvom využívania služieb poskytovaných externými poskytovateľmi IKT služieb zabezpečí celú škálu spôsobilostí súvisiacich s IKT, ktoré sú potrebné na zaistenie bezpečnosti sietí a informačných systémov, ktoré finančný subjekt využíva, a ktoré podporujú nepretržité poskytovanie finančných služieb a ich kvalitu, a to aj počas narušení.

„IKT riziko“ je každá primerane identifikovateľná okolnosť v súvislosti s používaním sietí a informačných systémov, ktorá, ak k nej dôjde, môže ohroziť bezpečnosť sietí a informačných systémov, akéhokoľvek nástroja alebo procesu závislého od technológií, ako aj bezpečnosť operácií a procesov alebo poskytovania služieb vytvorením nepriaznivých účinkov v digitálnom alebo fyzickom prostredí.

„IKT aktívum“ je softvérové alebo hardvérové aktívum v sieťach a informačných systémoch, ktoré používa finančný subjekt.

„Incident súvisiaci s IKT“ je jedna udalosť alebo séria prepojených udalostí, ktoré finančný subjekt neplánoval a ktoré narúšajú bezpečnosť sietí a informačných systémov a majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo na služby, ktoré poskytuje finančný subjekt.

„Prevádzkový alebo bezpečnostný incident súvisiaci s platbami“ je jedna udalosť alebo séria prepojených udalostí, ktoré finančné subjekty neplánovali, bez ohľadu na to, či súvisia s IKT alebo nie, a ktoré majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov súvisiacich s platbami, alebo na služby súvisiace s platbami, ktoré poskytuje finančný subjekt.

„Závažný incident súvisiaci s IKT“ je incident súvisiaci s IKT, ktorý má veľký nepriaznivý vplyv na siete a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu.

„Závažný prevádzkový alebo bezpečnostný incident súvisiaci s platbami“ je prevádzkový alebo bezpečnostný incident súvisiaci s platbami, ktorý má veľký nepriaznivý vplyv na poskytované služby súvisiace s platbami.

„Významná kybernetická hrozba“ je kybernetická hrozba, ktorej technické charakteristiky naznačujú, že by mohla mať potenciál viesť k závažnému incidentu súvisiacemu s IKT alebo závažnému prevádzkovému alebo bezpečnostnému incidentu súvisiacemu s platbami.

„Kybernetický útok“ je zlomyseľný incident súvisiaci s IKT spôsobený prostredníctvom pokusu, ktorého sa dopustil akýkoľvek aktér hrozby, o zničenie, odhalenie, zmenu, znefunkčnenie, krádež alebo získanie neoprávneného prístupu k aktívu, alebo o neoprávnené použitie aktíva.

„Penetračné testovanie na základe konkrétnej hrozby“ alebo „TLPT“)“ je rámec, ktorý simuluje taktiku, techniky a postupy reálnych aktérov hrozby považovaných za subjekty predstavujúce skutočnú kybernetickú hrozbu a ktorým sa realizuje kontrolovaný, individualizovaný test kritických živých produkčných systémov finančného subjektu založený na spravodajských informáciách (červený tím).

Jednotlivá terminológia bude pre pochopenie v aplikačnej praxi vysvetlená aj v ďalších článkoch.

Publikované dňa 04.09.2025.

RIADENIE RIZÍK INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ

1. ABSTRAKT

Finančné subjekty musia mať v súlade s nariadením DORA zavedený **rámec vnútornej správy a riadenia a kontroly**, ktorým sa zabezpečí účinné a obozretné riadenie rizík informačných a komunikačných technológií (IKT) s cieľom dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti. Od finančných subjektov sa vyžaduje, aby vytvorili komplexný rámec riadenia rizík IKT. Čo je riadením rizík a aké opatrenia manažment rizík zahŕňa, sa dočítate na našom článku.

2. SPRÁVA A RIADENIE A ORGANIZÁCIA

Riadiaci orgán finančného subjektu vymedzuje a schvaľuje vykonávanie všetkých opatrení súvisiacich s rámcom riadenia IKT rizika, vykonáva nad ním dozor a zodpovedá zaň.

Riadiaci orgán finančného subjektu (i) nesie konečnú zodpovednosť za riadenie IKT rizika finančného subjektu, **(ii) zavádza politiky** zamerané na zabezpečenie zachovania vysokých noriem dostupnosti, pravosti, integrity a dôvernosti údajov, **(iii) stanovuje jasné úlohy a zodpovednosti** pre všetky funkcie súvisiace s IKT a zavádza vhodné mechanizmy správy a riadenia s cieľom zabezpečiť účinnú a včasnú komunikáciu, spoluprácu a koordináciu medzi týmito funkciami, **(iv) nesie celkovú zodpovednosť za stanovenie a schválenie stratégie digitálnej prevádzkovej odolnosti**, vrátane určenia primeranej úrovne tolerancie IKT rizika finančného subjektu, **(v) schvaľuje, vykonáva dozor a pravidelne preskúmava vykonávanie politiky** kontinuity činností finančného subjektu v oblasti IKT a plánov reakcie a obnovy v oblasti IKT, ktoré sa môžu prijať ako osobitná politika tvoriaca neoddeliteľnú súčasť celkovej politiky kontinuity činností finančného subjektu a plánu reakcie a obnovy finančného subjektu, **(vi) schvaľuje a pravidelne preskúmava plány vnútorných auditov IKT**, ktoré vypracúva finančný subjekt, audity IKT a ich podstatné zmeny, **(vii) prideľuje a pravidelne preskúmava primeraný rozpočet** na splnenie potrieb finančného subjektu v oblasti digitálnej prevádzkovej odolnosti, pokiaľ ide o všetky druhy zdrojov, vrátane relevantných programov zvyšovania informovanosti o bezpečnosti v oblasti IKT a školení o digitálnej prevádzkovej odolnosti a IKT zručností pre všetkých zamestnancov, **(viii) schvaľuje a pravidelne preskúmava politiku finančného subjektu týkajúcu sa opatrení súvisiacich s využívaním IKT služieb, ktoré poskytujú externí** poskytovatelia IKT služieb, **(ix) zavádza na podnikovej úrovni kanály nahlasovania**, ktoré mu umožnia, aby bol riadne informovaný o: a) dojednaniach o využívaní IKT služieb uzavretých s externými poskytovateľmi IKT služieb, b) akýchkoľvek relevantných plánovaných podstatných zmenách týkajúcich sa externých poskytovateľov IKT služieb, c) potenciálnom vplyve takýchto zmien na kritické alebo dôležité funkcie, ktoré podliehajú uvedeným dojednaniam, vrátane zhrnutia analýzy rizík na posúdenie vplyvu uvedených zmien, a aspoň o závažných incidentoch súvisiacich s IKT a ich vplyve, ako aj o opatreniach zameraných na reakciu, obnovu a nápravu.

3. RÁMEC RIADENIA IKT RIZIKA

Finančné subjekty musia mať **ako súčasť svojho celkového systému riadenia rizika zavedený spoľahlivý, komplexný a dobre zdokumentovaný rámec riadenia IKT rizika**, ktorý im umožňuje riešiť IKT riziko rýchlo, efektívne a komplexne a zabezpečiť vysokú úroveň digitálnej prevádzkovej odolnosti.

Rámec riadenia IKT rizika zahŕňa aspoň stratégie, politiky, postupy, IKT protokoly a nástroje, ktoré sú potrebné na riadnu a primeranú ochranu všetkých informačných aktív a IKT aktív vrátane

počítačového softvéru, hardvéru, serverov, ako aj ochranu všetkých relevantných fyzických zložiek a infraštruktúr, ako sú priestory, dátové centrá a citlivé určené oblasti s cieľom zabezpečiť, aby boli všetky informačné aktíva a IKT aktíva primerane chránené pred rizikami vrátane poškodenia a neoprávneného prístupu či používania.

Rámec riadenia IKT rizika sa **zdokumentuje a preskúma aspoň raz ročne**, alebo pravidelne v prípade mikropodnikov, ako aj pri výskyte závažných incidentov súvisiacich s IKT, pričom sa riadi pokynmi alebo závermi dohľadu vyplývajúcimi z príslušných procesov testovania alebo auditu digitálnej prevádzkovej odolnosti.

Rámec riadenia IKT rizika finančných subjektov iných ako mikropodnikov **podlieha pravidelnému vnútornému auditu** vykonávanému audítormi v súlade s plánom auditu finančných subjektov.

4. IDENTIFIKÁCIA, OCHRANA A PREVENCIA A DETEKCIA NA ÚSEKU KYBERNETICKÝCH HROZIEB

Ako súčasť rámca riadenia IKT rizika finančné subjekty identifikujú, klasifikujú a primerane dokumentujú všetky obchodné funkcie, úlohy a povinnosti podporované IKT, informačné aktíva a IKT aktíva podporujúce uvedené funkcie a ich úlohy a závislosti vo vzťahu k IKT riziku**. Finančné subjekty podľa potreby, najmenej však raz ročne, preskúmavajú primeranosť tejto klasifikácie a akejkoľvek relevantnej dokumentácie.**

Finančné subjekty **nepretržite identifikujú všetky zdroje IKT rizika**, najmä rizikovú expozíciu voči iným finančným subjektom a pochádzajúcu od nich, a posudzujú kybernetické hrozby a zraniteľné miesta v oblasti IKT relevantné z hľadiska ich obchodných funkcií podporovaných IKT, informačných aktív a IKT aktív. **Finančné subjekty pravidelne a aspoň raz ročne preskúmavajú rizikové scenáre, ktoré na ne majú vplyv.**

Finančné subjekty identifikujú všetky informačné aktíva a IKT aktíva vrátane aktív na vzdialených miestach, sieťové zdroje a hardvérové zariadenia a zmapujú tie, ktoré sa považujú za kritické.

Finančné subjekty iné než mikropodniky pravidelne a aspoň raz ročne vykonávajú osobitné posúdenie IKT rizika vo všetkých pôvodných IKT systémoch.

Na účely primeranej ochrany IKT systémov a s cieľom organizovať opatrenia v oblasti reakcie finančné subjekty nepretržite monitorujú a kontrolujú bezpečnosť a fungovanie IKT systémov a nástrojov a minimalizujú vplyv IKT rizika na IKT systémy tak, že zavedú vhodné nástroje, politiky a postupy v oblasti bezpečnosti IKT. 2. Finančné subjekty navrhujú, obstarávajú a realizujú stratégie, politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, ktorých cieľom je zabezpečiť odolnosť, kontinuitu a dostupnosť IKT systémov, najmä tých, ktoré podporujú kritické alebo dôležité funkcie, a zachovať vysoké štandardy dostupnosti, pravosti, integrity a dôvernosti údajov, či už v pokoji, pri používaní alebo pri prenose.

Finančné subjekty musia mať zavedené mechanizmy na rýchle odhaľovanie anomálnych činností vrátane problémov s výkonnosťou IKT siete a incidentov súvisiacich s IKT, ako aj na identifikáciu potenciálnych závažných jednotlivých miest zlyhania. Všetky detekčné mechanizmy sa musia pravidelne testovať.

5. REAKCIA A OBNOVA V PRÍPADE INCIDENTU NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

Finančné subjekty vykonávajú politiku kontinuity činností v oblasti IKT prostredníctvom špecializovaných, primeraných a zdokumentovaných opatrení, plánov, postupov a mechanizmov zameraných na (i) zabezpečenie kontinuity kritických alebo dôležitých funkcií finančného subjektu, **(ii)** rýchlu, primeranú a účinnú reakciu na všetky incidenty súvisiace s IKT a ich riešenie,, a to spôsobom, ktorý obmedzuje škody a uprednostňuje obnovenie činností a opatrenia zamerané na obnovu, **(iii)** bezodkladnú aktiváciu špecializovaných plánov, ktoré umožňujú uplatniť opatrenia, procesy a technológie na zamedzenie

šírenia vhodné pre každý typ incidentu súvisiaceho s IKT, a predchádzanie ďalším škodám, ako aj prispôsobené postupy reakcie a obnovy, **(iv)** odhad predbežných vplyvov, škôd a strát, **(v)** stanovenie opatrení v oblasti komunikácie a krízového riadenia, ktorými sa zabezpečí, aby sa aktualizované informácie zasielali všetkým príslušným interným zamestnancom a externým zainteresovaným stranám a aby sa o nich podávali správy príslušným orgánom.

Finančné subjekty v nadväznosti na všetky uvedené povinnosti musia tiež v zmysle nariadenia DORA zriadiť **dostatočné záložné systémy**, postupy a politiky zálohovania **a metódy obnovy**, a to po prípadnom kybernetickom útoku.

Nemožno tiež opomenúť **povinnosť finančného subjektu disponovať spôsobilosťami a spôsobilými personálnymi kapacitami** na zhromažďovanie informácií o zraniteľných miestach a kybernetických hrozbách, incidentoch súvisiacich s IKT, najmä kybernetických útokoch, a analyzovanie vplyvu, ktorý pravdepodobne majú na ich digitálnu prevádzkovú odolnosť.

Vedúci pracovníci v oblasti IKT musia podať **aspoň raz ročne riadiacemu orgánu finančného subjektu správu o zisteniach** na úseku kybernetickej bezpečnosti a predkladajú odporúčania.

Samozrejme, je tu tiež povinnosť priebežne monitorovať technologický vývoj na úseku kybernetickej bezpečnosti.

6. ZHRNUTIE

Z uvedeného, ako aj z podrobného znenia nariadenia DORA vyplýva, že nariadenie DORA skutočne podrobne určuje prvky tzv. risk manažmentu IKT pre finančné subjekty, ktoré možno do aplikačnej praxe zhrnúť nasledovne:

Nariadenie **DORA od finančných subjektov vyžaduje, aby vytvorili komplexný rámec riadenia rizík IKT, ktorý zahŕňa (i)** vytvorenie a udržiavanie odolných systémov a nástrojov IKT, ktoré minimalizujú vplyv IKT rizika, **(ii)** identifikovanie, klasifikovanie a dokumentovanie kritických funkcií a aktív, **(iii)** neustály monitoring všetkých zdrojov rizík IKT s cieľom nastaviť vhodné ochranné a preventívne opatrenia, **(iv)** zabezpečenie rýchlej detekcie anomálnych činností, **(v)** zavedenie špecializovaných a komplexných politík kontinuity podnikania a plánov po havárii a obnovu vrátane ročného testovania plánov pokrývajúceho všetky podporné funkcie, **(vi)** vytvorenie mechanizmov na učenie sa z externých udalostí, ako aj z vlastných incidentov.

Hĺbkové procesy a skutočne aj tie najmenšie **detaily postupov vo veci riadenia IKT rizík, sú súčasťou DELEGOVANÉHO NARIADENIA KOMISIE (EÚ) 2024/1774 z 13. marca 2024**, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa spresňujú nástroje, metódy, postupy a politiky riadenia IKT rizika a zjednodušený rámec riadenia IKT rizika.

Toto delegované nariadenie je dostupné online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202401774

Publikované dňa 04.09.2025.

RIADENIE, KLASIFIKÁCIA A NAHLASOVANIE INCIDENTOV SÚVISIACICH S IKT

1. ABSTRAKT

Finančné subjekty sú povinné podľa nariadenia DORA vymedziť, zaviesť a vykonávať proces riadenia incidentov súvisiacich s IKT s cieľom odhaľovať, riadiť a oznamovať incidenty súvisiace s IKT. Finančné subjekty sú povinné zaznamenávať všetky incidenty súvisiace s IKT a významné kybernetické hrozby. S tým súvisí, aby finančné subjekty stanovili vhodné postupy a procesy na zaistenie konzistentného a integrovaného monitorovania, riešenia a následných opatrení v prípade incidentov súvisiacich s IKT s cieľom zabezpečiť, aby sa hlavné príčiny identifikovali, zdokumentovali a riešili s cieľom zabrániť výskytu takýchto incidentov. Podrobnosti v nasledovnom príspevku.

2. POVINNOSTI NA ÚSEKU REPORTOVANIA INDICENTOV

Povinnosti finančných subjektov z nariadenia DORA na úseku incidentov možno zosumarizovať a konštatovať, že **finančné subjekty sú povinné (i) vyvinúť zrozumiteľný proces** na zaznamenávanie/klasifikáciu všetkých incidentov v oblasti IKT a určovanie závažných incidentov podľa kritérií podrobne opísaných v nariadení a bližšie špecifikovaných európskymi orgánmi dohľadu (EBA, EIOPA a ESMA), **(ii) predložiť úvodnú, priebežnú a záverečnú správu** o incidentoch súvisiacich s IKT, **(iii) harmonizovať oznamovanie incidentov** súvisiacich s IKT prostredníctvom štandardizovaných vzorov, ktoré vypracovali ESA.

Finančné subjekty sú tiež povinné klasifikovať incidenty súvisiace s IKT a kybernetickými hrozbami.

3. KLASIFIKÁCIA INDICENTOV SÚVISIACICH S IKT A KYBERNETICKÝCH HROZIEB

Finančné subjekty klasifikujú incidenty súvisiace s IKT a určujú ich vplyv na základe týchto kritérií: (i) počet a/alebo relevantnosť klientov alebo finančných protistrán a prípadne výška alebo počet transakcií, ktoré sú ovplyvnené incidentom súvisiacim s IKT, a to, či incident súvisiaci s IKT mal vplyv na dobré meno, **(ii)** trvanie incidentu súvisiaceho s IKT vrátane výpadku služby, **(iii)** geografické rozloženie, pokiaľ ide o oblasti postihnuté incidentom súvisiacim s IKT, najmä ak sa týka viac ako dvoch členských štátov, **(iv)** straty údajov, ktoré incident súvisiaci s IKT prináša v súvislosti s dostupnosťou, pravosťou, integritou alebo dôvernosťou údajov, **(v)** kritickosť zasiahnutých služieb vrátane transakcií a operácií finančného subjektu, **(vi)** hospodársky vplyv, najmä priame a nepriame náklady a straty, incidentu súvisiaceho s IKT v absolútnom aj relatívnom vyjadrení.

Finančné subjekty **klasifikujú kybernetické hrozby ako významné na základe kritickosti služieb vystavených riziku** vrátane transakcií a operácií finančného subjektu, **počtu a/alebo relevantnosti cieľových klientov alebo finančných protistrán a geografického rozloženia** rizikových oblastí.

Finančné subjekty nesmú pri posudzovaní incidentov opomenúť aj ďalšie nariadenie.

Ide o **DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2024/1772 z 13. marca 2024**, ktorým sa dopĺňa nariadenie DORA, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch (ďalej len „delegované nariadenie“).

4. KLASIFIKAČNÉ KRITÉRIÁ

Predmetné delegované nariadenie určuje **klasifikačné kritériá pre určenie závažnosti incidentu** na úseku kybernetickej bezpečnosti.

Ide o **kritérium (i)** klientov, finančných protistrán a transakcií ovplyvnených incidentom, **(ii)** vplyvu na dobré meno, **(iii)** trvanie incidentu súvisiaceho s IKT a výpadok služby, **(iv)** geografického rozloženia, **(v)** straty údajov, **(vi)** kritickosti zasiahnutých služieb **a (vii)** hospodárskeho vplyvu.

4.1 Klienti, finančné protistrany a transakcie ovplyvnené incidentom

Počet klientov ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, odráža **počet všetkých ovplyvnených klientov**, či už fyzických alebo právnických osôb, ktorí **počas incidentu nemôžu alebo nemohli využívať službu** poskytovanú finančným subjektom, alebo ktorých incident nepriaznivo ovplyvnil. Tento počet zahŕňa aj tretie strany, na ktoré sa výslovne vzťahuje zmluvná dohoda medzi finančným subjektom a klientom, ako príjemcov ovplyvnenej služby.

Počet finančných protistrán ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, odráža počet všetkých ovplyvnených finančných protistrán, ktoré s finančným subjektom uzavreli zmluvnú dohodu.

Pokiaľ ide o relevantnosť klientov a finančných protistrán ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, finančný subjekt zohľadňuje rozsah, v akom vplyv na klienta alebo finančnú protistranu **ovplyvní plnenie obchodných cieľov** finančného subjektu, ako aj potenciálny vplyv incidentu na efektívnosť trhu.

Pokiaľ ide o výšku alebo počet transakcií ovplyvnených incidentom, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, finančný subjekt zohľadňuje **všetky ovplyvnené transakcie zahŕňajúce peňažnú sumu**, ak sa aspoň jedna časť transakcie vykonáva v Únii.

Ak nemožno určiť skutočný počet ovplyvnených klientov alebo finančných protistrán alebo skutočný počet alebo sumu ovplyvnených transakcií, finančný subjekt odhadne uvedené počty alebo sumy na základe dostupných údajov z porovnateľných referenčných období.

4.2 Vplyv na dobré meno

Na účely určenia vplyvu incidentu na dobré meno, ako sa uvádza v článku 18 ods. 1 písm. a) nariadenia (EÚ) 2022/2554, došlo podľa finančných subjektov k vplyvu na dobré meno, **ak je splnené aspoň jedno z týchto kritérií: (i)** incident bol predmetom mediálneho spravodajstva, **(ii)** incident viedol k opakovaným sťažnostiam rôznych klientov alebo finančných protistrán, ktoré sa týkali služieb vyžadujúcich si priamy kontakt so zákazníkom alebo kritických obchodných vzťahov, **(iii)** finančný subjekt si v dôsledku incidentu nebude môcť alebo pravdepodobne nebude môcť splniť regulačné požiadavky, **(iv)** finančný subjekt v dôsledku incidentu stratí alebo pravdepodobne stratí klientov alebo finančné protistrany, čo môže mať významný vplyv na jeho obchodnú činnosť.

4.3 Trvanie incidentu súvisiaceho s IKT a výpadok služby

Finančné subjekty **merajú trvanie** incidentu súvisiaceho s IKT, ako sa uvádza v článku 18 ods. 1 písm. b) nariadenia (EÚ) 2022/2554, **od momentu, keď incident nastane, až do momentu jeho vyriešenia**. Ak finančné subjekty nedokážu určiť moment, keď k incidentu došlo, merajú trvanie incidentu od momentu, keď sa zistil. Ak sa finančné subjekty dozvedia, že incident sa vyskytol pred jeho odhalením, merajú jeho trvanie od momentu zaznamenania incidentu v záznamových protokoloch siete alebo systému alebo v iných zdrojoch údajov. Ak finančné subjekty ešte nevedia, kedy sa incident vyrieši, alebo nedokážu overiť záznamy v záznamových protokoloch alebo iných zdrojoch údajov, uplatňujú odhady.

Finančné subjekty merajú výpadok služby v dôsledku incidentu, ako sa uvádza v článku 18 ods. 1 písm. b) nariadenia (EÚ) 2022/2554, **od**

momentu, keď je služba pre klientov, finančné protistrany alebo iných interných či externých používateľov **úplne alebo čiastočne nedostupná**, až do momentu, keď sa bežné činnosti alebo operácie obnovili na úroveň služby, ktorá bola poskytovaná pred incidentom. Ak výpadok služby spôsobí omeškanie pri poskytovaní služby po obnovení bežných činností alebo operácií, výpadok sa meria od začiatku incidentu do momentu, keď sa uvedená meškajúca služba plne poskytuje. Ak finančné subjekty nedokážu určiť moment, keď sa začal výpadok služby, merajú trvanie výpadku služby od momentu, keď sa výpadok zistil.

4.4 Geografické rozloženie

Na účely určenia geografického rozloženia, pokiaľ ide o oblasti postihnuté incidentom, ako sa uvádza v článku 18 ods. 1 písm. c) nariadenia (EÚ) 2022/2554, finančné subjekty **posúdia, či incident má alebo mal vplyv v iných členských štátoch, a najmä význam vplyvu vo vzťahu ku ktorémukoľvek z týchto subjektov: (i)** klienti a finančné protistrany v iných členských štátoch, **(ii)** pobočky alebo iné finančné subjekty v rámci skupiny vykonávajúce činnosti v iných členských štátoch, **(iii)** infraštruktúry finančného trhu alebo externí poskytovatelia, ktoré/ktorí môžu mať vplyv na finančné subjekty v iných členských štátoch, ktorým poskytujú služby, a to v rozsahu, v akom sú takéto informácie k dispozícii.

4.5 Straty údajov

Na účely určenia strát údajov, ktoré incident so sebou prináša, ako sa uvádza v článku 18 ods. 1 písm. d) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú tieto aspekty: **(i)** v súvislosti s dostupnosťou údajov, či sa v dôsledku incidentu stali údaje poskytované na požiadanie finančného subjektu, jeho klientov alebo jeho protistrán dočasne alebo trvalo nedostupné alebo nepoužiteľné, **(ii)** v súvislosti s pravosťou údajov, či incident ohrozil dôveryhodnosť zdroja údajov, **(iii)** v súvislosti s integritou údajov, či incident viedol k nepovolenej zmene údajov, v dôsledku ktorej sa údaje stali znehodnotenými alebo neúplnými, **(iv)** v súvislosti s dôvernosťou údajov, či incident viedol k prístupu k údajom alebo k ich sprístupneniu neoprávnenej strane alebo systému.

4.6 Kritickosť zasiahnutých služieb

Na účely určenia kritickosti zasiahnutých služieb, ako sa uvádza v článku 18 ods. 1 písm. e) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú, či incident: **(i)** ovplyvňuje alebo ovplyvnil IKT služby alebo sieť a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu; **(ii)** ovplyvňuje alebo ovplyvnil finančné služby, ktoré poskytuje finančný subjekt a ktoré si vyžadujú povolenie, registráciu alebo ktoré podliehajú dohľadu príslušných orgánov; **(iii)** predstavuje alebo predstavoval úspešný, škodlivý a neoprávnený prístup do siete a informačných systémov finančného subjektu.

4.7 Hospodársky vplyv

Na účely určenia hospodárskeho vplyvu incidentu, ako sa uvádza v článku 18 ods. 1 písm. f) nariadenia (EÚ) 2022/2554, finančné subjekty zohľadňujú, bez zohľadnenia spätne získaných finančných prostriedkov, **tieto druhy priamych a nepriamych nákladov a strát, ktoré im vznikli v dôsledku incidentu: (i)** vyvlastnené finančné prostriedky alebo finančné aktíva, za ktoré zodpovedajú, vrátane aktív stratených v dôsledku krádeže, **(ii)** náklady na výmenu alebo premiestnenie softvéru, hardvéru alebo infraštruktúry, **(iii)** náklady na zamestnancov vrátane nákladov spojených s nahradením alebo premiestnením zamestnancov, prijímaním ďalších zamestnancov, odmeňovaním nadčasov a obnovením stratených alebo zhoršených zručností, **(iv)** poplatky z dôvodu nedodržania zmluvných záväzkov, **(v)** náklady na nápravu a odškodnenie zákazníkov, **(vi)** straty v dôsledku ušlých príjmov, **(vii)** náklady spojené s vnútornou a vonkajšou komunikáciou, **(viii)** náklady na poradenstvo vrátane nákladov spojených s právnym poradenstvom, forenznými službami a sanačnými službami.

5. PRAHOVÉ HODNOTY POSUDZOVANIA ZÁVAŽNÝCH INCIDENTOV

Delegované nariadenie určuje prahové hodnoty pre učenie závažnosti incidentov.

Prahová hodnota významnosti pre kritérium „klienti, finančné protistrany a transakcie ovplyvnené incidentom“ je splnená, ak je splnená ktorákoľvek z týchto podmienok: (i) počet ovplyvnených klientov je **vyšší ako 10 % všetkých klientov** využívajúcich ovplyvnenú službu, **(ii)** počet ovplyvnených klientov využívajúcich ovplyvnenú službu je **vyšší ako 100 000, (iii)** počet ovplyvnených finančných protistrán je **vyšší ako 30 % všetkých finančných protistrán** vykonávajúcich činnosti súvisiace s poskytovaním ovplyvnenej služby, **(iv) počet ovplyvnených transakcií je vyšší ako 10 % denného priemerného počtu** transakcií vykonávaných finančným subjektom v súvislosti s ovplyvnenou službou, **(v) suma ovplyvnených transakcií je vyššia ako 10 % dennej priemernej hodnoty** transakcií vykonávaných finančným subjektom v súvislosti s ovplyvnenou službou, **(vi) ovplyvnení boli klienti alebo finančné protistrany, ktorí/ktoré boli identifikované ako dôležití/dôležité**.

Ak nemožno určiť skutočný počet ovplyvnených klientov alebo finančných protistrán alebo skutočný počet alebo sumu ovplyvnených transakcií, finančný subjekt odhadne uvedené počty alebo sumy na základe dostupných údajov z porovnateľných referenčných období.

Prahová hodnota významnosti pre kritérium „vplyv na dobré meno“ je splnená, ak je splnená ktorákoľvek z podmienok uvedených v bode 4.2 vyššie.

Prahová hodnota významnosti pre kritérium „trvanie incidentu súvisiaceho s IKT a výpadok služby“ je splnená, ak je splnená ktorákoľvek z týchto podmienok: **(i) incident trvá dlhšie ako 24 hodín, (ii)** v prípade služieb IKT, ktoré podporujú kritické alebo dôležité funkcie, je **výpadok služby dlhší ako 2 hodiny**.

Prahová hodnota významnosti pre kritérium „geografické rozloženie“ je splnená, ak má incident **vplyv v dvoch alebo viacerých členských štátoch**.

Prahová hodnota významnosti pre kritérium **„straty údajov“ je splnená, ak je splnená ktorákoľvek z týchto podmienok: (i)** každý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov má alebo bude mať nepriaznivý vplyv na plnenie obchodných cieľov finančného subjektu alebo na jeho schopnosť spĺňať regulačné požiadavky, **(ii)** sieť a informačné systémy sú zasiahnuté úspešným, škodlivým a neoprávneným prístupom, na ktorý sa nevzťahuje na prvý bod, ak takýto prístup môže viesť k stratám údajov.

Prahová hodnota významnosti pre kritérium **„hospodársky vplyv“ je splnená, ak náklady a straty**, ktoré vznikli finančnému subjektu v dôsledku incidentu, **prekročili alebo pravdepodobne prekročia 100 000 EUR**.

6. PRAHOVÉ HODNOTY NA URČENIE VÝZNAMNÝCH KYBERNETICKÝCH HROZIEB

Na účely nariadenia DORA sa kybernetická hrozba považuje za významnú, ak sú splnené všetky tieto podmienky:

(A) kybernetická hrozba, ak by k nej došlo, mohla ovplyvniť alebo by mohla ovplyvniť kritické alebo dôležité funkcie finančného subjektu alebo iné finančné subjekty, externých poskytovateľov, klientov alebo finančné protistrany, a to na základe informácií, ktoré má finančný subjekt k dispozícii,

(B) existuje vysoká pravdepodobnosť naplnenia kybernetickej hrozby vo finančnom subjekte alebo v iných finančných subjektoch, pričom sa **zohľadňujú aspoň tieto prvky**:

- **i)** uplatniteľné riziká súvisiace s kybernetickou hrozbou uvedenou v prvom bode vrátane potenciálnych zraniteľných miest systémov finančného subjektu, ktoré možno zneužiť,
- **ii)** spôsobilosti a úmysel aktérov hrozby v rozsahu, ktorý je finančnému subjektu známy,

iii) pretrvávanie hrozby a všetky získané poznatky o incidentoch, ktoré ovplyvnili finančný subjekt alebo jeho externého poskytovateľa, klientov alebo finančné protistrany,

(C) ak by došlo ku kybernetickej hrozbe, mohla by spĺňať ktorúkoľvek z týchto podmienok:

(i) kritérium týkajúce sa kritickosti zasiahnutých služieb,

(ii) prahovú hodnotu významnosti, ktorú uvádzame vyššie v odseku 5 pre kritérium klienti, finančné protistrany a transakcie ovplyvnené incidentom,

(iii) prahovú hodnotu významnosti, ktorú uvádzame vyššie v odseku 6 pre kritérium geografického rozloženia.

7. REPORTING ZÁVAŽNÝCH IKT INCIDENTOV

Finančné subjekty nahlasujú závažné incidenty súvisiace s IKT relevantnému príslušnému orgánu uvedenému v článku 46 v súlade s odsekom 4 tohto článku. Ak finančný subjekt podlieha dohľadu viac ako jedného príslušného vnútroštátneho orgánu uvedeného v článku 46, členské štáty určia jediný príslušný orgán ako relevantný príslušný orgán zodpovedný za vykonávanie funkcií a povinností stanovených v tomto článku.

Úverové inštitúcie klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013 oznamujú závažné incidenty súvisiace s IKT relevantnému vnútroštátnemu príslušnému orgánu určenému v súlade s článkom 4 smernice 2013/36/EÚ, ktorý uvedenú správu bezodkladne zašle ECB.

Finančné subjekty môžu dobrovoľne oznamovať významné kybernetické hrozby relevantnému príslušnému orgánu, ak sa domnievajú, že hrozba je relevantná pre finančný systém, používateľov služieb alebo klientov. Relevantný príslušný orgán môže poskytnúť takéto informácie iným relevantným orgánom.

Úverové inštitúcie klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013 môžu dobrovoľne oznamovať významné kybernetické hrozby relevantnému vnútroštátnemu príslušnému orgánu určenému v súlade s článkom 4 smernice 2013/36/EÚ, ktorý oznámenie bezodkladne zašle ECB.

Členské štáty môžu určiť, že tie finančné subjekty, ktoré dobrovoľne oznamujú, môžu uvedené oznámenie zaslať aj jednotkám CSIRT určeným alebo zriadeným v súlade so smernicou NIS 2.

Ak dôjde k závažnému incidentu súvisiacemu s IKT, ktorý má vplyv na finančné záujmy klientov, finančné subjekty bez zbytočného odkladu a čo najskôr po tom, ako o ňom nadobudli vedomosť, informujú svojich klientov o závažnom incidente súvisiacom s IKT a o opatreniach, ktoré boli prijaté na zmiernenie nepriaznivých účinkov takéhoto incidentu.

V prípade významnej kybernetickej hrozby finančné subjekty v náležitých prípadoch informujú svojich klientov, ktorí sú potenciálne dotknutí, o akýchkoľvek vhodných ochranných opatreniach, ktorých prijatie títo klienti môžu zvážiť.

Finančné subjekty v lehotách, ktoré sa stanovia v súlade s článkom 20 nariadenia DORA, predložia relevantnému príslušnému orgánu (i) počiatočné oznámenie, **(ii)** priebežnú správu po počiatočnom oznámení uvedenom v písmene a), hneď ako sa výrazne zmení stav pôvodného incidentu alebo po zmene riešenia závažného incidentu súvisiaceho s IKT na základe nových dostupných informácií, po ktorej v náležitých prípadoch nasledujú aktualizované oznámenia vždy, keď je k dispozícii príslušná aktualizácia stavu, ako aj na základe osobitnej žiadosti príslušného orgánu, **(iii)** záverečnú správu po dokončení analýzy hlavných príčin, bez ohľadu na to, či už boli vykonané zmierňujúce opatrenia, a keď sú k dispozícii skutočné údaje o vplyve, aby sa nahradili odhady.

Finančné subjekty môžu v súlade s odvetvovým právom Únie a vnútroštátnym odvetvovým právom **zveriť nahlasovacie povinnosti podľa tohto článku externému poskytovateľovi služieb formou outsourcingu**. V prípade takéhoto

outsourcingu je finančný subjekt naďalej plne zodpovedný za plnenie požiadaviek na nahlasovanie incidentov.

Po prijatí počiatočného oznámenia a každej správy uvedenej v odseku 4 príslušný orgán včas poskytne podrobné údaje o závažnom incidente súvisiacom s IKT, a to náležite na základe ich príslušných právomocí, teda orgánom EBA, ESMA alebo EIOPA, Európskej centrálnej banke, príslušným orgánom, jednotným kontaktným miestam alebo jednotkám CSIRT určeným alebo zriadeným v súlade so smernicou NIS 2, orgánom pre riešenie krízových situácií uvedeným v článku 3 smernice 2014/59/EÚ a Jednotnej rade pre riešenie krízových situácií (SRB).

Po prijatí informácií **EBA, ESMA alebo EIOPA a ECB po konzultácii s agentúrou ENISA a v spolupráci s relevantným príslušným orgánom posúdia, či je závažný incident súvisiaci s IKT relevantný pre príslušné orgány v iných členských štátoch**. Po tomto posúdení EBA, ESMA alebo EIOPA čo najskôr náležite informujú relevantné príslušné orgány v iných členských štátoch. ECB informuje členov Európskeho systému centrálnych bánk o otázkach relevantných pre platobné systémy. Na základe uvedeného oznámenia príslušné orgány v relevantných prípadoch prijmú všetky nevyhnutné opatrenia s cieľom ochrániť bezprostrednú stabilitu finančného systému.

Harmonizácia **obsahu a postupov nahlasovania incidentov, vzory nahlasovania**, sú súčasťou ďalšieho nariadenia, a to **DELEGOVANÉHO NARIADENIA KOMISIE (EÚ) 2025/301 z 23. októbra 2024**, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb.

Nariadenie je dostupné online a obsahuje skutočne podrobný a vyčerpávajúci popis postupov nahlasovania incidentov, vrátane lehôt: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202500301

Vzory na nahlasovanie incidentov IKT sú dostupné rovnako tak online, a to prostredníctvom VYKONÁVACIEHO NARIADENIA KOMISIE (EÚ) 2025/302 z 23. októbra 2024, ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a na oznamovanie významných kybernetických hrozieb: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202500302

Publikované dňa 04.09.2025.

TESTOVANIE DIGITÁLNEJ PREVÁDZKOVEJ ODOLNOSTI

1. ABSTRAKT

Nariadenie DORA vyžaduje, aby poskytovatelia finančných služieb testovali svoje systémy na základe súvisiacich rizík. Testovanie digitálnej prevádzkovej odolnosti je povinné a jeho cieľom je posúdiť pripravenosť na riešenie incidentov **súvi**siacich **s** IKT, identifikovať slabé stránky, nedostatky a medzery v digitálnej prevádzkovej odolnosti a urýchlene zaviesť nápravné opatrenia. V našom článku sa podrobnejšie dočítate aj o takzvaných penetračných testoch.

2. VŠEOBECNÉ POŽIADAVKY NA TESTOVANIE

Na účely posúdenia pripravenosti riešiť incidenty súvisiace s IKT, identifikácie slabých miest, nedostatkov a medzier digitálnej prevádzkovej odolnosti a urýchleného vykonania nápravných opatrení finančné subjekty iné ako mikropodniky zriadia, udržiavajú a preskúmavajú spoľahlivý a komplexný program testovania digitálnej prevádzkovej odolnosti ako integrálnu súčasť rámca riadenia IKT rizika.

Program na testovanie digitálnej prevádzkovej odolnosti zahŕňa celý rad posúdení, testov, metodík, postupov a nástrojov.

Pri vykonávaní programu testovania digitálnej prevádzkovej odolnosti sa finančné subjekty iné ako mikropodniky riadia prístupom založeným na riziku, pričom náležite prihliadajú na vyvíjajúce sa prostredie IKT rizika, všetky špecifické riziká, ktorým je alebo by mohol byť dotknutý finančný subjekt vystavený, kritickosť informačných aktív a poskytovaných služieb, ako aj akýkoľvek iný faktor, ktorý finančný subjekt považuje za vhodný.

Finančné subjekty iné ako mikropodniky zabezpečia, aby **testy vykonávali nezávislé strany, či už interné alebo externé**. Ak testy vykonáva interný testovací subjekt, finančné subjekty vyčlenia dostatočné zdroje a zabezpečia, aby sa vo fáze navrhovania a vykonávania testu zabránilo konfliktom záujmov.

Finančné subjekty iné ako mikropodniky stanovia postupy a politiky na určenie priorít, klasifikáciu a nápravu všetkých problémov odhalených počas vykonávania testov a zavedú interné metodiky validácie s cieľom zabezpečiť úplné riešenie všetkých zistených slabých miest, nedostatkov a medzier.

Finančné subjekty iné ako mikropodniky zabezpečia, aby sa aspoň raz ročne vykonávali vhodné testy všetkých IKT systémov a aplikácií podporujúcich kritické alebo dôležité funkcie.

3. TESTOVANIE IKT NÁSTROJOV A SYSTÉMOV

V rámci programu testovania digitálnej prevádzkovej odolnosti **finančný subjekt zabezpečí vykonanie vhodných testov, ako sú (i)** posúdenia a vyhľadávania zraniteľnosti, **(ii)** analýzy otvorených zdrojov (analýzy open-source riešení), **(iii)** posúdenia bezpečnosti sietí, **(iv)** analýzy nedostatkov, **(v)** preskúmania fyzickej bezpečnosti, **(vi)** dotazníky a skenovacie softvérové riešenia, preskúmania zdrojových kódov, **(vii)** ak je to možné, testy založené na konkrétnych scenároch, **(viii)** testovania kompatibility, **(ix)** testovania výkonnosti, **(x)** testovania medzi koncovými bodmi (end-to-end testovania) **a (xi)** penetračné testovania.

4. POKROČILÉ TESTOVANIE IKT NÁSTROJOV, SYSTÉMOV A PROCESOV

Veľké a prepojené finančné subjekty, vykonávajú **aspoň každé tri roky pokročilé testovanie prostredníctvom penetračného testovania**. Na základe rizikového profilu finančného subjektu a s prihliadnutím na prevádzkové okolnosti môže príslušný orgán v prípade potreby požiadať finančný subjekt o zníženie alebo zvýšenie tejto frekvencie.

TLPT je skratka pre tzv. **Threat-Led Penetration Test**.

Ide o formu bezpečnostného testovania, ktoré **simuluje reálne kybernetické útoky** za účelom vyhodnotenia účinnosti bezpečnostných opatrení finančného subjektu. Je založené na skutočných alebo predpokladaných hrozbách alebo zraniteľnosti.

Penetračné testovanie je jedným z pilierov nariadenia DORA.

Každý penetračný test na základe konkrétnej hrozby zahŕňa viaceré alebo všetky kritické alebo dôležité funkcie finančného subjektu a vykonáva sa na živých produkčných systémoch podporujúcich takéto funkcie.

Finančné subjekty identifikujú všetky relevantné podkladové IKT systémy, procesy a technológie podporujúce kritické alebo dôležité funkcie a všetky relevantné IKT služby vrátane tých, ktoré podporujú kritické alebo dôležité funkcie, ktoré sú externe zabezpečované formou outsourcingu alebo zmluvne dohodnuté s externým poskytovateľom IKT služieb.

Finančné subjekty posúdia, na ktoré kritické alebo dôležité funkcie, sa TLPT musí vzťahovať. Výsledok tohto posúdenia určí presný rozsah TLPT a validujú ho príslušné orgány.

Ak sú externí poskytovatelia IKT služieb zahrnutí do rozsahu pôsobnosti TLPT, finančný subjekt prijme potrebné opatrenia a záruky na zabezpečenie účasti takýchto externých poskytovateľov IKT služieb na TLPT a vždy si ponechá plnú zodpovednosť za zabezpečenie súladu s týmto nariadením.

Finančné subjekty uzatvárajú zmluvy s testovacími subjektmi na účely vykonávania TLPT v súlade s článkom 27 nariadenia DORA. Ak finančné subjekty využívajú interné testovacie subjekty na účely vykonávania TLPT, uzatvoria zmluvu s externými testovacími subjektmi po každom treťom testovaní.

Príslušné orgány určia finančné subjekty, od ktorých sa vyžaduje vykonávanie TLPT, pričom zohľadnia kritériá stanovené v článku 4 ods. 2, a to **na základe posúdenia (i)** faktorov súvisiacich s vplyvom, najmä rozsahom, v akom služby poskytované a činnosti vykonávané finančným subjektom majú vplyv na finančný sektor, **(ii)** prípadných obáv o finančnú stabilitu vrátane systémového charakteru finančného subjektu na úrovni Únie alebo na vnútroštátnej úrovni, podľa toho, čo je uplatniteľné **(iii)** konkrétneho IKT rizikového profilu, úrovne IKT vyspelosti finančného subjektu alebo súvisiacich technologických prvkov.

4.1 Testovacie subjekty

V súlade s nariadením DORA **finančné subjekty využívajú na vykonávanie TLPT iba testovacie subjekty, ktoré (i)** sú najvhodnejšie a najuznávanejšie, **(ii)** disponujú technickými a organizačnými spôsobilosťami a preukazujú osobitné odborné znalosti v oblasti spravodajských informácií o hrozbách, penetračného testovania a testovania prostredníctvom červeného tímu, **(iii)** sú certifikované akreditačným orgánom v členskom štáte alebo dodržiavajú formálne kódexy správania alebo etické rámce, **(iv)** poskytujú nezávislé uistenie alebo audítorskú správu v súvislosti so správnym riadením rizík spojených s vykonávaním TLPT vrátane náležitej ochrany dôverných informácií finančného subjektu a nápravy obchodných rizík finančného subjektu, **(v)** sú riadne a v plnom rozsahu kryté príslušnými poisteniami zodpovednosti za škodu spôsobenú pri výkone povolania, a to aj pre prípad pochybenia a nedbanlivosti.

Ak využívajú interné testovacie subjekty, finančné subjekty musia zabezpečiť, aby okrem uvedených požiadaviek, **boli splnené aj tieto podmienky: (vi)** takéto využitie schválil relevantný príslušný orgán alebo jeden verejný orgán určený v súlade s článkom 26 ods. 9 a 10 nariadenia, **(vii)** relevantný príslušný orgán overil, že finančný subjekt má dostatočné vyčlenené zdroje a zabezpečil, aby sa vo fáze navrhovania a vykonávania testu zabránilo konfliktom záujmov **a (viii)** poskytovateľ spravodajských informácií o

hrozbách je vo vzťahu k finančnému subjektu externým subjektom.

Finančné subjekty zabezpečia, aby sa **v zmluvách uzavretých s externými testovacími subjektmi vyžadovalo správne riadenie výsledkov** TLPT a aby akékoľvek spracúvanie z toho vyplývajúcich údajov vrátane akéhokoľvek generovania, uchovávania, agregácie, navrhovania, podávania správ, komunikácie alebo likvidácie nevytváralo pre finančný subjekt riziká.

4.2 Detaily penetračného testovania

Účelom tohto špeciálneho vydania Pro Bona nie je predstaviť kompletné technické detaily penetračného testovania, iba právny rámec.

Tak, ako aj nahlasovanie incidentov a riadenie IKT rizík má svoje delegované nariadenia, aj **penetračné testovanie je detailne upravené v ďalšom delegovanom nariadení**.

Ide o **DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2025/1190 z 13. februára 2025**, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie špecifikujú kritériá používané na identifikáciu finančných subjektov povinných vykonať penetračné testovanie na základe konkrétnej hrozby, požiadavky a normy, ktorými sa riadi využívanie interných testovacích subjektov, požiadavky týkajúce sa rozsahu pôsobnosti, metodiky testovania a prístupu pre každú fázu testovania, výsledkov, záverečného a nápravného štádia a druh spolupráce v oblasti dohľadu a v iných relevantných oblastiach potrebnej na vykonávanie TLPT a na uľahčenie vzájomného uznávania.

Je dostupné online:
https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202501190.

Toto delegované nariadenie odzrkadľuje **metodiku, proces a štruktúru penetračného testovania** na základe konkrétnej hrozby.

Vzhľadom na zložitosť TLPT a s ním súvisiace riziká by sa jeho používanie malo obmedziť na tie finančné subjekty, pre ktoré je odôvodnené. Orgány zodpovedné za záležitosti TLPT (orgány TLPT buď na úrovni Únie alebo na vnútroštátnej úrovni) by preto mali z rozsahu pôsobnosti TLPT vylúčiť tie finančné subjekty, ktoré pôsobia v hlavných pododvetviach finančných služieb, pre ktoré TLPT nie je odôvodnené. To znamená, že aj keď úverové inštitúcie, platobné inštitúcie a inštitúcie elektronického peňažníctva, centrálne depozitáre cenných papierov, centrálne protistrany, obchodné miesta, poisťovne a zaisťovne spĺňajú kvantitatívne kritériá, mohli by byť oslobodené od požiadavky TLPT vzhľadom na celkové posúdenie ich rizikového profilu a vyspelosti v oblasti IKT, vplyvu na finančný sektor a súvisiacich obáv týkajúcich sa finančnej stability.

Metodika penetračného testovania zabezpečuje zapojenie týchto hlavných účastníkov: (i) finančného subjektu s kontrolným tímom (tzv. „kontrolný tím“) a modrým tímom **a (ii)** orgánu TLPT vo forme kybernetického tímu TLPT, **(iii)** poskytovateľa spravodajských informácií o hrozbách **a (iv)** testovacích subjektov (tzv. červený tím).

Pre zaujímavosť uvádzame jednotlivú definíciu pojmov do aplikačnej praxe penetračného testovania.

„Kontrolný tím“ je tím zložený zo zamestnancov testovaného finančného subjektu a, ak je to relevantné vzhľadom na rozsah pôsobnosti TLPT, zo zamestnancov jeho externých poskytovateľov služieb a akejkoľvek inej strany, ktorá test riadi.

„Vedúci kontrolného tímu“ je zamestnanec finančného subjektu zodpovedný za vykonávanie všetkých činností súvisiacich s TLPT pre finančný subjekt v kontexte daného testu.

„Modrý tím“ sú zamestnanci finančného subjektu a prípadne zamestnanci externých poskytovateľov služieb finančného subjektu a akejkoľvek inej strany považovanej za relevantnú z hľadiska rozsahu pôsobnosti TLPT, externých poskytovateľov služieb finančného subjektu, ktorí bránia používanie sietí a informačných systémov finančného subjektu, a to udržiavaním stavu

bezpečnosti pred simulovanými alebo skutočnými útokmi a ktorí nemajú vedomosť o TLPT.

„Úlohy modrého tímu“ sú úlohy, ktoré zvyčajne vykonáva modrý tím, ako sú centrum bezpečnostných operácií (CBO), služby infraštruktúry IKT, služby helpdesku, služby riadenia incidentov na operačnej úrovni.

„Červený tím“ sú interné alebo externé testovacie subjekty, ktoré sú zazmluvnené alebo pridelené na TLPT.

„Poskytovatelia TLPT“ sú testovacie subjekty a poskytovatelia spravodajských informácií o hrozbách.

„Opora“ je pomoc alebo informácie, ktoré kontrolný tím poskytuje testovacím subjektom s cieľom umožniť testovacím subjektom pokračovať vo vykonávaní dráhy útoku, ak nie sú schopní napredovať samostatne a ak neexistuje žiadna iná primeraná alternatíva, a to aj vzhľadom na nedostatočný čas alebo zdroje v danom TLPT.

„Dráha útoku“ je trasa, ktorú nasledujú testovacie subjekty počas fázy aktívneho testovania prostredníctvom červeného tímu TLPT, aby dosiahli vlajky špecifikované pre dané TLPT.

„Vlajky“ sú kľúčové ciele IKT systémov podporujúcich kritické alebo dôležité funkcie finančného subjektu, ktoré sa testovacie subjekty snažia dosiahnuť cez test.

„Citlivé informácie“ sú informácie, ktoré možno ľahko využiť na vykonanie útokov na IKT systémy finančného subjektu, duševné vlastníctvo, dôverné obchodné údaje alebo osobné údaje, ktoré môžu priamo alebo nepriamo poškodiť finančný subjekt a jeho ekosystém, ak by boli v rukách aktérov s nekalými úmyslami.

4.3 Identifikácia finančných subjektov povinných vykonať TLPT

Identifikáciu subjektov pre povinné penetračné testovanie nájdeme v spomínanom delegovanom nariadení.

Orgány TLPT posudzujú, či je akýkoľvek finančný subjekt povinný vykonať TLPT, pričom zohľadňujú vplyv týchto finančných subjektov, ich systémový charakter a ich rizikový profil v oblasti IKT, a to na základe všetkých týchto kritérií:

A) faktory súvisiace s vplyvom a systémovým charakterom:
i) veľkosť finančného subjektu určená na základe toho, či finančný subjekt poskytuje finančné služby v jednom alebo viacerých členských štátoch, a porovnaním činností finančného subjektu s činnosťami iných finančných subjektov poskytujúcich podobné služby;
ii) rozsah a povaha prepojenia finančného subjektu s inými finančnými subjektmi vo finančnom sektore v jednom alebo viacerých členských štátoch;
iii) kritickosť alebo význam služieb, ktoré finančný subjekt poskytuje finančnému sektoru;
iv) nahraditeľnosť služieb, ktoré finančný subjekt poskytuje;
v) zložitosť obchodného modelu finančného subjektu a súvisiacich služieb a procesov;
vi) či je finančný subjekt súčasťou skupiny systémového charakteru na úrovni Únie alebo na vnútroštátnej úrovni vo finančnom sektore a zdieľa IKT systémy;

B) faktory súvisiace s IKT rizikom:
i) rizikový profil finančného subjektu;
ii) panoráma hrozieb finančného subjektu;
iii) stupeň závislosti kritických alebo dôležitých funkcií alebo ich podporných funkcií finančného subjektu od IKT systémov a procesov;
iv) zložitosť architektúry IKT finančného subjektu;
v) IKT služby a funkcie podporované externými poskytovateľmi IKT služieb a množstvo a typ zmluvných dojednaní s externými poskytovateľmi IKT služieb alebo vnútroskupinovými poskytovateľmi IKT služieb;
vi) výsledky všetkých preskúmaní orgánmi dohľadu, ktoré sú relevantné pre posúdenie vyspelosti finančného subjektu v oblasti IKT;
vii) vyspelosť plánov kontinuity činností v oblasti IKT a plánov reakcie a obnovy v oblasti IKT;
viii) vyspelosť operačných bezpečnostných opatrení v oblasti IKT na odhaľovanie a zmierňovanie vrátane schopnosti: 1. neustále

monitorovať infraštruktúru IKT finančného subjektu; 2. v reálnom čase odhaľovať udalosti súvisiace s IKT; 3. analyzovať udalosti uvedené v bode 2; 4. včas a účinne reagovať na udalosti uvedené v bode 2;
ix) či je finančný subjekt súčasťou skupiny pôsobiacej vo finančnom sektore na úrovni Únie alebo na vnútroštátnej úrovni, v rámci ktorej sa zdieľajú IKT systémy.

Bez ohľadu na splnenie alebo nesplnenie uvedených faktorov, orgány TLPT vyžadujú, aby TLPT vykonávali všetky nasledujúce finančné subjekty:

A) úverové inštitúcie, ktoré spĺňajú ktorúkoľvek z týchto podmienok:
i) boli identifikované ako globálne systémovo významné inštitúcie (G-SII) v súlade s článkom 131 smernice Európskeho parlamentu a Rady 2013/36/EÚ (7);
ii) boli identifikované ako inak systémovo významné inštitúcie (O-SII) v súlade s článkom 131 smernice 2013/36/EÚ; iii) sú súčasťou G-SII alebo O-SII;

B) platobné inštitúcie, ktoré v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT prekročili celkovú hodnotu platobných transakcií vo výške 150 miliárd EUR v zmysle vymedzenia v článku 4 bode 5 smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 (8);

C) inštitúcie elektronického peňažníctva, ktoré v každom z dvoch kalendárnych rokov predchádzajúcich posúdeniu orgánom TLPT prekročili buď celkovú hodnotu platobných transakcií vo výške 150 miliárd EUR v zmysle vymedzenia v článku 4 bode 5 smernice (EÚ) 2015/2366 alebo celkovú hodnotu 40 miliárd EUR sumy vydaných elektronických peňazí;

D) centrálne depozitáre cenných papierov;

E) centrálne protistrany;

F) obchodné miesta s elektronickým systémom obchodovania, ktoré spĺňajú ktorékoľvek z podrobných kritérií určených delegovaným nariadením;

G) poisťovne a zaisťovne, ktoré spĺňajú všetky tieto kritériá:
i) majú hrubé predpísané poistné, ktoré presahuje 1 500 000 000 EUR;
ii) majú technické rezervy, ktoré presahujú 10 000 000 000 EUR;
iii) poisťovne, ktoré vykonávajú len činnosti životného poistenia alebo činnosti životného aj neživotného poistenia a ktorých celkové aktíva presahujú 3,5 % súčtu celkových aktív poisťovní a zaisťovní usadených v členskom štáte ocenených v súlade s článkom 75 smernice Európskeho parlamentu a Rady (11) 2009/138/ES.

Na podrobnosti v posudzovaní opätovne odkazujeme na delegované nariadenie a najmä na jeho článok 2: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202501190.

Jednotlivé fázy penetračného testovania, výber externého subjektu penetračného testovania a všetky podrobné postupy sú obsiahnuté v delegovanom nariadení, na ktoré odkazujeme online.

5. OSVEDČENIE O PENETRAČNOM TESTE A LEHOTY

O realizácií penetračného testu u slovenského finančného subjektu podliehajúcemu povinnosti penetračného testovania, vydáva **osvedčenie v zmysle § 36a zákona o dohľade nad finančným trhom** č. 747/2004 Z. z. v platnom znení, **Národná banka Slovenska**. Národná banka Slovenska vydáva na účely vzájomného uznávania podľa osobitného predpisu osvedčenia o vykonaní penetračného testu na základe konkrétnej hrozby. Keďže nariadenie DORA bolo zverejnené v Úradnom vestníku Európskej únie dňa 27. decembra 2022 a nadobudlo platnosť od 16. januára 2023 a od tohto dátumu mali inštitúcie 24 mesiacov na začlenenie nových pravidiel do svojich procesov, tak z uvedeného vyplýva, že **penetračné testovanie, vzhľadom na jeho povinnosť realizácie každé 3 roky, by malo začať koncom roka 2025.**

Publikované dňa 04.09.2025.

RIADENIE EXTERNÉHO RIZIKA INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ

1. ABSTRAKT

Finančné subjekty sú podľa nariadenia DORA povinné zabezpečiť dôkladné monitorovanie rizík, ktoré plynú od poskytovateľov IKT tretích strán, nahlásiť svoj kompletný register outsourcovaných činností vrátane vnútroskupinových služieb a akékoľvek zmeny v zadávaní kritických služieb externým poskytovateľom služieb IKT, zabezpečiť, aby zmluvy s poskytovateľmi IKT tretích strán obsahovali všetky potrebné podrobnosti. Tieto a ďalšie podrobnosti ohľadom riadenia externého rizika v našom článku.

2. VŠEOBECNÉ ZÁSADY

Finančné subjekty riadia externé IKT riziko ako integrálnu súčasť IKT rizika v medziach svojho rámca riadenia IKT rizika, ako je uvedené v článku 6 ods. 1, a **v súlade s týmito zásadami:**

(A) finančné subjekty, ktoré majú uzavreté zmluvné dojednania o využívaní IKT služieb na vykonávanie svojich obchodných činností, sú vždy plne zodpovedné za dodržiavanie a plnenie všetkých povinností vyplývajúcich z tohto nariadenia a uplatniteľného práva v oblasti finančných službách;

(B) riadenie externého IKT rizika finančnými subjektmi sa vykonáva so zreteľom na zásadu proporcionality, pričom sa **zohľadňujú tieto aspekty: (i)** povaha, rozsah, zložitosť a význam závislostí súvisiacich s IKT, **(ii)** riziká vyplývajúce zo zmluvných dojednaní o využívaní IKT služieb uzavretých s externými poskytovateľmi IKT služieb, pričom sa zohľadňuje kritickosť alebo dôležitosť príslušnej služby, procesu alebo funkcie, ako aj potenciálny vplyv na kontinuitu a dostupnosť finančných služieb a činností na individuálnej úrovni a na úrovni skupiny.

Finančné subjekty **aspoň raz ročne nahlasujú príslušným orgánom (i)** počet nových dojednaní o využívaní IKT služieb, **(ii)** kategórie externých poskytovateľov IKT služieb, **(iii)** druh zmluvných dojednaní **a (iv)** poskytované IKT služby a funkcie. Finančné subjekty sprístupnia príslušnému orgánu na jeho žiadosť úplný register informácií alebo na požiadanie jeho konkrétne oddiely spolu so všetkými informáciami, ktoré sa považujú za potrebné na umožnenie účinného dohľadu nad finančným subjektom. Finančné subjekty včas **informujú príslušný orgán o každom plánovanom zmluvnom dojednaní o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie**, ako aj o tom, kedy sa funkcia stala kritickou alebo dôležitou.

Pred uzavretím zmluvného dojednania o využívaní IKT služieb finančné subjekty (i) posúdia, či sa zmluvné dojednanie vzťahuje na využívanie IKT služieb podporujúcich kritickú alebo dôležitú funkciu, **(ii)** posúdia, či sú splnené podmienky dohľadu pre uzatváranie zmlúv, **(iii)** identifikujú a posúdia všetky relevantné riziká v súvislosti so zmluvným dojednaním vrátane možnosti, že takéto zmluvné dojednania môžu prispieť k posilneniu rizika koncentrácie IKT, ako sa uvádza v článku 29, **(iv)** vykonajú všetku náležitú starostlivosť v súvislosti s potenciálnymi externými poskytovateľmi IKT služieb a zabezpečia vhodnosť externého poskytovateľa IKT služieb počas celého procesu výberu a posudzovania, **(v)** identifikujú a posúdia konflikty záujmu, ktoré môže zmluvné dojednanie spôsobiť.

Finančné subjekty **môžu uzatvárať zmluvné dojednania len s externými poskytovateľmi IKT služieb, ktorí spĺňajú primerané normy v oblasti informačnej bezpečnosti.** V prípade, že sa uvedené zmluvné dojednania týkajú kritických alebo dôležitých funkcií, finančné subjekty pred uzatvorením dojednaní náležite zohľadnia, ako externí poskytovatelia IKT služieb využívajú

najaktuálnejšie a najprísnejšie normy kvality v oblasti informačnej bezpečnosti.

Finančné subjekty **zabezpečia, aby sa zmluvné dojednania o využívaní IKT služieb mohli ukončiť za ktorýchkoľvek z týchto okolností: (i)** významné porušenie príslušných zákonov, iných právnych predpisov alebo zmluvných podmienok zo strany externého poskytovateľa IKT služieb, **(ii)** okolnosti zistené počas monitorovania externého IKT rizika, ktoré sa považujú za schopné zmeniť výkon funkcií poskytovaných prostredníctvom zmluvného dojednania vrátane závažných zmien, ktoré majú vplyv na dojednanie alebo situáciu externého poskytovateľa IKT služieb, **(iii)** preukázané slabé stránky externého poskytovateľa IKT služieb, týkajúce sa jeho celkového riadenia IKT rizika, a najmä spôsobu, akým zaisťuje dostupnosť, pravosť, integritu a dôvernosť údajov, či už osobných alebo inak citlivých údajov, alebo iných ako osobných údajov, **(iv)** ak príslušný orgán už nemôže účinne vykonávať dohľad nad finančným subjektom v dôsledku podmienok alebo okolností súvisiacich s príslušným zmluvným dojednaním.

Finančné subjekty zabezpečia, **aby mohli ukončiť zmluvné dojednania bez (i) narušenia svojej obchodnej činnosti, (ii) obmedzenia dodržiavania regulačných požiadaviek, (iii) ohrozenia kontinuity a kvality služieb** poskytovaných klientom.

3. KĽÚČOVÉ ZMLUVNÉ USTANOVENIA

Práva a povinnosti finančného subjektu a externého poskytovateľa IKT služieb sa jasne pridelia a stanovia **písomne**.
Úplná zmluva zahŕňa dohody o úrovni poskytovaných služieb a zdokumentuje sa **v jednom písomnom dokumente, ktorý majú zmluvné strany k dispozícii v papierovej forme, alebo v dokumente v inom stiahnuteľnom, trvalom a prístupnom formáte.**

Zmluvné dojednania o využívaní IKT služieb zahŕňajú aspoň (i) jasný a úplný **opis všetkých funkcií a IKT služieb**, ktoré má externý poskytovateľ IKT služieb poskytovať, pričom sa uvedie, či je povolené zadávanie IKT služieb podporujúcich kritickú alebo dôležitú funkciu alebo jej závažných častí subdodávateľovi, a ak áno, podmienky vzťahujúce sa na takéto využívanie subdodávateľa, **(ii)** miesta, konkrétne regióny alebo krajiny, **kde sa majú poskytovať zmluvne dohodnuté alebo subdodávateľsky zabezpečované funkcie a IKT služby** a kde sa majú údaje spracúvať vrátane miesta uchovávania, ako aj požiadavka, aby externý poskytovateľ IKT služieb vopred informoval finančný subjekt, ak plánuje zmeniť takéto miesto, **(iii)** ustanovenia o **dostupnosti, pravosti, integrite alebo dôvernosti v súvislosti s ochranou údajov** vrátane osobných údajov, **(iv)** ustanovenia o zabezpečení obnovy a návratu osobných údajov a iných ako osobných údajov spracúvaných finančným subjektom v ľahko prístupnom formáte v prípade platobnej neschopnosti, riešenia krízových situácií alebo ukončenia obchodných operácií externého poskytovateľa IKT služieb, alebo v prípade ukončenia zmluvných dojednaní, a prístupu k takýmto údajom, **(v)** opis **úrovne poskytovaných služieb** vrátane ich aktualizácií a revízií, **(vi)** povinnosť externého poskytovateľa IKT služieb poskytovať pomoc finančnému subjektu bez dodatočných nákladov alebo za náklady stanovené ex ante, keď dôjde k IKT incidentu, ktorý súvisí s IKT službou poskytnutou finančnému subjektu, **(vii)** povinnosť externého poskytovateľa IKT služieb **plne spolupracovať s príslušnými orgánmi** a orgánmi pre riešenie krízových situácií finančného subjektu, vrátane osôb nimi vymenovanými, **(viii)** právo ukončiť zmluvný vzťah a súvisiaca **minimálna výpovedná lehota na ukončenie** zmluvných dojednaní v súlade s očakávaniami príslušných orgánov a orgánov pre riešenie krízových situácií, **(ix)** podmienky účasti externých poskytovateľov IKT služieb na programoch zvyšovania informovanosti finančných subjektov v oblasti bezpečnosti IKT a na školení v oblasti digitálnej prevádzkovej odolnosti.

Zmluvné dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie zahŕňajú okrem uvedených prvkov aj (x) úplné opisy úrovne služieb vrátane ich aktualizácií a revízií, ako aj presné kvantitatívne a kvalitatívne výkonnostné ciele v rámci dohodnutých úrovní služieb, aby finančný subjekt mohol účinne

monitorovať IKT služby a mal možnosť bez zbytočného odkladu vykonať primerané nápravné opatrenia v prípade nesplnenia dohodnutých úrovní služieb, **(xi)** výpovedné lehoty a nahlasovacie povinnosti externého poskytovateľa IKT služieb voči finančnému subjektu vrátane oznamovania akéhokoľvek vývoja, ktorý by mohol mať významný vplyv na schopnosť externého poskytovateľa IKT služieb účinne poskytovať IKT služby podporujúce kritické alebo dôležité funkcie v súlade s dohodnutými úrovňami služieb, **(xii)** požiadavky na externého poskytovateľa IKT služieb na vykonávanie a testovanie obchodných krízových plánov a na zavedenie bezpečnostných opatrení, nástrojov a politík v oblasti IKT, ktoré poskytujú primeranú úroveň bezpečnosti na poskytovanie služieb zo strany finančného subjektu v súlade s jeho regulačným rámcom, **(xiii)** povinnosť externého poskytovateľa IKT služieb zúčastňovať sa a plne spolupracovať na TLPT finančného subjektu, ako sa uvádza v článkoch 26 a 27, **(xiv)** právo priebežne monitorovať výkonnosť externého poskytovateľa IKT služieb, ktoré zahŕňa:

neobmedzené práva na prístup, inšpekciu a audit vykonávané finančným subjektom alebo vymenovanou treťou stranou a príslušným orgánom, ako aj právo vyhotovovať kópie príslušnej dokumentácie na mieste, ak je kritická pre operácie externého poskytovateľa IKT služieb, ktorého účinnému vykonávaniu nebránia ani ho neobmedzujú iné zmluvné dojednania alebo vykonávacie politiky, **právo dohodnúť sa na alternatívnych úrovniach zabezpečenia**, ak sú dotknuté práva iných klientov, **povinnosť externého poskytovateľa IKT služieb plne spolupracovať počas inšpekcií** na mieste a auditov vykonávaných príslušnými orgánmi, hlavným orgánom dozoru, finančným subjektom alebo vymenovanou treťou stranou; a **povinnosť poskytnúť podrobnosti** o rozsahu, postupoch, ktoré sa majú dodržiavať, a frekvencii takýchto inšpekcií a auditov.

Zmluvné dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie zahŕňajú ďalej okrem uvedených prvkov vyššie tiež (xv) stratégie ukončenia angažovanosti, najmä zavedenie primeraného povinného **prechodného obdobia, počas ktorého bude externý poskytovateľ IKT služieb naďalej poskytovať** príslušné funkcie alebo IKT služby s cieľom znížiť riziko narušenia na úrovni finančného subjektu alebo zabezpečiť efektívne riešenie jeho krízovej situácie a reštrukturalizáciu **a ktoré umožňuje finančnému subjektu prejsť k inému externému poskytovateľovi IKT služieb alebo začať využívať vlastné riešenia** v závislosti od zložitosti poskytovanej služby.

Odchylne sa externý poskytovateľ IKT služieb a **finančný subjekt, ktorý je mikropodnikom, môžu dohodnúť, že práva** finančného subjektu na prístup, inšpekciu a audit **možno delegovať na nezávislú tretiu stranu**, ktorú určí externý poskytovateľ IKT služieb, a že finančný subjekt môže kedykoľvek od tretej strany požadovať informácie a uistenie o výkonnosti externého poskytovateľa IKT služieb.

Pri rokovaniach o zmluvných dojednaniach finančné subjekty a externí poskytovatelia IKT služieb zvážia **použitie štandardných zmluvných doložiek vypracovaných verejnými orgánmi** pre konkrétne služby.

4. URČENIE KRITICKÝCH EXTERNÝCH POSKYTOVATEĽOV IKT SLUŽIEB

Európske orgány dohľadu prostredníctvom spoločného výboru a na základe **odporúčania fóra pre dozor** zriadeného **podľa článku 32 ods. 1 nariadenia DORA** **(i) určia externých poskytovateľov IKT služieb, ktorí sú pre finančné subjekty kritickí**, a to na základe posúdenia, **(ii) vymenujú za hlavný orgán dozoru** pre každého kritického externého poskytovateľa IKT služieb **európsky orgán dohľadu**, ktorý je v súlade s nariadením (EÚ) č. 1093/2010 (EÚ), (EÚ) č. 1094/2010 alebo (EÚ) č. 1095/2010 **zodpovedný za finančné subjekty**, ktoré majú spolu najväčší podiel celkových aktív na hodnote celkových aktív všetkých finančných subjektov využívajúcich služby príslušného kritického externého poskytovateľa IKT služieb, ako to dokazuje suma individuálnych súvah uvedených finančných subjektov.

Určenie uvedené v prvom bode (i) sa nevzťahuje na finančné subjekty poskytujúce IKT služby iným finančným subjektom; externých poskytovateľov IKT služieb, ktorí podliehajú rámcom dozoru zriadeným na účely podpory úloh uvedených v článku 127 ods. 2 Zmluvy o fungovaní Európskej únie, vnútroskupinových poskytovateľov IKT služieb, externých poskytovateľov IKT služieb, ktorí poskytujú IKT služby výhradne v jednom členskom štáte finančným subjektom, ktoré pôsobia len v danom členskom štáte.

Určenie uvedené vyššie v prvom bode vychádza v súvislosti s IKT službami poskytovanými externým poskytovateľom IKT služieb zo všetkých týchto kritérií:

(A) systémový vplyv na stabilitu, kontinuitu alebo kvalitu poskytovania finančných služieb, ak by príslušný externý poskytovateľ IKT služieb čelil rozsiahlemu prevádzkovému zlyhaniu v poskytovaní svojich služieb, so zohľadnením počtu finančných subjektov a celkovej hodnoty aktív finančných subjektov, ktorým príslušný externý poskytovateľ IKT služieb poskytuje služby;

(B) systémový charakter alebo význam finančných subjektov, ktoré závisia od príslušného externého poskytovateľa IKT služieb, posudzovaný v súlade s týmito parametrami: **i) počet globálne systémovo významných inštitúcií** (ďalej len „G-SII“) alebo inak systémovo významných inštitúcií (ďalej len „O-SII“), ktoré závisia od príslušného externého poskytovateľa IKT služieb, **ii) vzájomná závislosť medzi G-SII alebo O-SII** uvedenými v bode i) a inými finančnými subjektmi vrátane situácií, keď G-SII alebo O-SII poskytujú služby finančnej infraštruktúry iným finančným subjektom;

(C) závislosť finančných subjektov od služieb, ktoré poskytuje príslušný externý poskytovateľ IKT služieb v súvislosti s kritickými alebo dôležitými funkciami finančných subjektov, ktoré v konečnom dôsledku zahŕňajú toho istého externého poskytovateľa IKT služieb, a to bez ohľadu na to, či finančné subjekty závisia od uvedených služieb priamo alebo nepriamo prostredníctvom subdodávateľských dojednaní;

(D) stupeň nahraditeľnosti externého poskytovateľa IKT služieb pri zohľadnení týchto parametrov: **i) neexistencia skutočných, hoci len čiastočných, alternatív** z dôvodu obmedzeného počtu externých poskytovateľov IKT služieb na konkrétnom trhu, alebo trhový podiel príslušného externého poskytovateľa IKT služieb, alebo súvisiaca technická zložitosť či prepracovanosť, a to aj vo vzťahu k akejkoľvek proprietárnej technológii, alebo osobitosti organizácie alebo činnosti daného externého poskytovateľa IKT služieb; **ii) ťažkosti v súvislosti s čiastočným alebo úplným presunom** príslušných údajov a pracovného zaťaženia z príslušného externého poskytovateľa IKT služieb na iného externého poskytovateľa IKT služieb, a to buď z dôvodu značných finančných nákladov, času alebo iných zdrojov, ktoré môže takýto presun predstavovať, alebo z dôvodu zvýšeného IKT rizika alebo iných prevádzkových rizík, ktorým môže byť finančný subjekt vystavený pri takomto presune.

Po určení externého poskytovateľa IKT služieb za kritického európske orgány dohľadu prostredníctvom spoločného výboru **oznámia externému poskytovateľovi IKT služieb takéto určenie a dátum, od ktorého bude skutočne podliehať činnostiam dozoru.** Uvedený počiatočný dátum nesmie byť neskôr ako jeden mesiac po oznámení. Externý poskytovateľ IKT služieb oznámi finančným subjektom, ktorým poskytuje služby, že bol určený ako kritický.

Európske orgány dohľadu prostredníctvom spoločného výboru vypracujú, uverejnia a každoročne aktualizujú zoznam kritických externých poskytovateľov IKT služieb na úrovni Únie.

5. ÚLOHY HLAVNÉHO ORGÁNU DOZORU

Hlavný orgán dozoru určený článkom 32 nariadenia DORA **vykonáva dozor nad pridelenými kritickými externými poskytovateľmi IKT služieb a na účely všetkých záležitostí týkajúcich sa dozoru je hlavným kontaktným miestom** pre týchto kritických externých poskytovateľov IKT služieb.
Hlavný orgán dozoru posudzuje, či každý kritický externý poskytovateľ IKT služieb zaviedol

komplexné, riadne a účinné pravidlá, postupy, mechanizmy a opatrenia na riadenie IKT rizika, ktoré kritický externý poskytovateľ IKT služieb môže predstavovať pre finančné subjekty.

Posúdenie zahŕňa (i) požiadavky na IKT s cieľom zaistiť najmä bezpečnosť, dostupnosť, kontinuitu, škálovateľnosť a kvalitu služieb, ktoré kritický externý poskytovateľ IKT služieb poskytuje finančným subjektom, ako aj schopnosť neustále zachovávať vysokú úroveň dostupnosti, pravosti, integrity alebo dôvernosti údajov, **(ii)** fyzickú bezpečnosť prispievajúcu k zaisteniu bezpečnosti IKT vrátane bezpečnosti priestorov, zariadení a dátových centier, **(iii)** procesy riadenia rizika vrátane politík riadenia IKT rizika, politík kontinuity činností v oblasti IKT a plánov reakcie a obnovy v oblasti IKT, **(iv)** mechanizmy správy a riadenia vrátane organizačnej štruktúry s jasnými, transparentnými a konzistentnými líniami zodpovednosti a pravidlami zodpovednosti umožňujúcimi účinné riadenie IKT rizika, **(v)** identifikáciu, monitorovanie a okamžité nahlasovanie významných incidentov súvisiacich s IKT finančným subjektom, riadenie a riešenie týchto incidentov, najmä kybernetických útokov, **(vi)** mechanizmy prenosnosti údajov, prenosnosti a interoperability aplikácií, ktoré zabezpečujú účinný výkon práv na ukončenie zmluvy finančnými subjektmi, **(vii)** testovanie IKT systémov, infraštruktúry a kontrol, **(viii)** audity IKT, **(ix)** používanie príslušných vnútroštátnych a medzinárodných noriem uplatniteľných na poskytovanie IKT služieb kritického externého poskytovateľa IKT služieb finančným subjektom.

Plnenie uvedených požiadaviek bude súčasťou kontroly hlavného orgánu dozoru u externého poskytovateľa IKT služieb na základe individuálneho ročného plánu dozoru.

Hlavný orgán dozoru má v zmysle článku 35 mnohé právomoci od požadovania informácií, cez vykonávanie všeobecných inšpekcií a vydávania odporúčaní, až po zákaz uzatvárania subdodávateľských dohôd.

Všetky detailné podrobnosti ohľadom dozoru nad externými poskytovateľmi IKT služieb, sú súčasťou článku 32 až článku 43 nariadenia DORA, samozrejme dostupného online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32022R2554&qid=1672669681316&from=SK.

Zjednodušene povedané, je skutočne potrebné zdôrazniť, že na základe nariadenia DORA má Európska únia oprávnenie kontrolovať a vykonávať inšpekcie a z toho vyplývajúcim určitým spôsobom mať vplyv na IT firmy na trhu externého dodávania IKT služieb.

6. POSÚDENIE SUBDODÁVATEĽOV ZO STRANY FINANČNÉHO SUBJEKTU

Poskytovanie IKT služieb finančným subjektom často závisí od komplexného reťazca subdodávateľov IKT, pričom externí poskytovatelia IKT služieb môžu uzavrieť jednu alebo viacero subdodávateľských dojednaní s inými externými poskytovateľmi IKT služieb. Nepriame spoliehanie sa na subdodávateľov IKT môže mať vplyv na schopnosť finančného subjektu identifikovať, posudzovať a riadiť svoje riziká.

Finančné subjekty sa značne líšia veľkosťou, štruktúrou a vnútornou organizáciou, ako aj povahou a zložitosťou svojich činností. V záujme zabezpečenia proporcionality by sa táto **rozmanitosť mala zohľadňovať pri špecifikovaní toho, ktoré prvky by mal finančný subjekt určovať a posudzovať pri využívaní subdodávateľov v prípade IKT služieb podporujúcich kritické alebo dôležité funkcie.**
S cieľom umožniť finančným subjektom posudzovať riziká spojené so subdodávateľskými dojednaniami alebo s ich závažnými zmenami by externí poskytovatelia IKT služieb mali informovať finančné subjekty, ktorým poskytujú IKT služby, o všetkých takýchto nových dojednaniach alebo zmenách v dostatočnom predstihu pred tým, ako sa takéto dojednania alebo zmeny začnú uplatňovať.

Za účelom posudzovania uvedeného, existuje ďalšie delegované nariadenie, a to DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2025/532 z 24. marca 2025, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o

regulačné technické predpisy, v ktorých sa bližšie špecifikujú prvky, ktoré musí finančný subjekt určiť a posúdiť pri využívaní subdodávateľov v prípade IKT služieb podporujúcich kritické alebo dôležité funkcie.

Na základe uvedeného delegovaného nariadenia, **finančný subjekt pred uzavretím zmluvného dojednania s externým poskytovateľom IKT služieb rozhodne**, či tento externý poskytovateľ IKT služieb môže IKT službu, ktorá podporuje kritické alebo dôležité funkcie alebo ich závažné časti, **zabezpečovať s využitím subdodávateľov**.

Finančný subjekt uzatvára takéto zmluvné dojednanie len vtedy, ak usúdil, že boli splnené všetky tieto podmienky: (i) postupy náležitej starostlivosti týkajúce sa externého poskytovateľa IKT služieb zabezpečujú, že môže vyberať a posudzovať prevádzkové a finančné schopnosti potenciálnych subdodávateľov IKT poskytovať IKT služby, ktoré podporujú kritické alebo dôležité funkcie alebo ich závažné časti, a v prípade, že to finančný subjekt vyžaduje, aj účasťou externého poskytovateľa IKT služieb na testovaní digitálnej prevádzkovej odolnosti, ako sa uvádza v kapitole IV nariadenia (EÚ) 2022/2554, **(ii)** externý poskytovateľ IKT služieb dokáže identifikovať všetkých subdodávateľov, ktorí poskytujú IKT služby podporujúce kritické alebo dôležité funkcie alebo ich závažné časti, ako aj informovať finančný subjekt o uvedených subdodávateľoch a poskytovať finančnému subjektu všetky informácie, ktoré môžu byť potrebné na posudzovanie podmienok podľa tohto článku, **(iii)** externý poskytovateľ IKT služieb zabezpečuje, aby zmluvné dojednania so subdodávateľmi, ktorí poskytujú IKT služby podporujúce kritické alebo dôležité funkcie alebo ich závažné časti, umožňovali finančnému subjektu plniť si svoje vlastné povinnosti vyplývajúce z nariadenia (EÚ) 2022/2554 a dodržiavať uplatniteľné právne predpisy Únie a vnútroštátne právne predpisy, **(iv)** subdodávateľ udelí finančnému subjektu a príslušným orgánom a orgánom pre riešenie krízových situácií rovnaké zmluvné práva na prístup a inšpekciu, ako sú tie, ktoré mu udelil externý poskytovateľ IKT služieb, **(v)** bez toho, aby bola dotknutá konečná zodpovednosť finančného subjektu za plnenie svojich právnych a regulačných povinností, samotný externý poskytovateľ IKT služieb má dostatočné schopnosti, odborné znalosti a primerané finančné, ľudské a technické zdroje na monitorovanie IKT rizík na úrovni subdodávateľov, a to aj uplatňovaním primeraných noriem v oblasti informačnej bezpečnosti a zavedením primeranej organizačnej štruktúry, riadenia rizík a vnútorných kontrol, ako aj nahlasovania incidentov a reakcií na ne, **(vi)** finančný subjekt má dostatočné schopnosti, odborné znalosti a primerané finančné, ľudské a technické zdroje na monitorovanie IKT rizík vo vzťahu k službe podporujúcej kritické alebo dôležité funkcie alebo ich závažné časti, ktorá bola zabezpečovaná s využitím subdodávateľov, a to aj uplatňovaním primeraných noriem v oblasti informačnej bezpečnosti a zavedením primeranej organizačnej štruktúry a riadenia rizík, reakcie na incidenty, riadenia kontinuity činností a vnútorných kontrol, **(vii)** finančný subjekt posúdil vplyv možného zlyhania subdodávateľa, ktorý poskytuje IKT služby podporujúce kritické alebo dôležité funkcie alebo ich závažnú časť, na digitálnu prevádzkovú odolnosť a finančnú situáciu finančného subjektu, **(viii)** finančný subjekt posúdil riziká spojené s miestom poskytovania IKT služieb potenciálnych subdodávateľov v súvislosti s IKT službami podporujúcimi kritické alebo dôležité funkcie alebo ich závažnú časť, ktoré poskytuje externý poskytovateľ IKT služieb, **(ix)** finančný subjekt posúdil riziká koncentrácie IKT na úrovni subjektu v súlade s článkom 29 nariadenia (EÚ) 2022/2554, **(x)** finančný subjekt posúdil, či existujú prekážky pri uplatňovaní auditu, inšpekcie a prístupových práv príslušnými orgánmi, orgánmi pre riešenie krízových situácií alebo finančným subjektom vrátane osôb, ktoré tieto orgány vymenovali.

Podmienky, za ktorých môžu byť IKT služby, ktoré podporujú kritické alebo dôležité funkcie alebo ich závažnú časť, **zabezpečované s využitím subdodávateľov**, ako aj **závažné zmeny subdodávateľských dojednaní** týkajúcich sa IKT služieb, ktoré podporujú kritické alebo dôležité funkcie alebo ich závažné časti, to všetko je **podrobnou súčasťou predmetného delegovaného nariadenia, dostupného rovnako tak online**: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202500532.

7. UKONČENIE ZMLUVNÉHO DOJEDNANIA MEDZI FINANČNÝM SUBJEKTOM A EXTERNÝM POSKTOVATEĽOM IKT SLUŽIEB

Finančný subjekt má právo stanoviť v zmluvnom dojednaní s externým poskytovateľom IKT služieb, že zmluvné dojednanie sa má ukončiť v každom z týchto prípadov: (i) finančný subjekt namietal voči závažným zmenám subdodávateľských dojednaní podporujúcich kritické alebo dôležité funkcie a požiadal o úpravy uvedených zmien, ale externý poskytovateľ IKT služieb napriek tomu tieto závažné zmeny vykonal, **(ii)** externý poskytovateľ IKT služieb vykonal závažné zmeny subdodávateľských dojednaní podporujúcich kritické alebo dôležité funkcie alebo ich závažné časti pred uplynutím lehoty na oznámenie bez súhlasu finančného subjektu, **(iii)** externý poskytovateľ IKT služieb IKT službu, ktorá podporuje kritickú alebo dôležitú funkciu alebo jej závažnú časť, zabezpečoval s využitím subdodávateľov pričom zmluvné dojednanie medzi finančným subjektom a externým poskytovateľom IKT služieb výslovne nepovoľuje, aby bola zabezpečovaná s využitím subdodávateľov.

Publikované dňa 04.09.2025.

Informácie uvedené v bulletine ULC Čarnogurský PRO BONO nie sú poskytovaním právnych rád. Nemožno z neho odvodzovať žiadne práva ani povinnosti. Materiál obsiahnutý v tomto dokumente je informatívnej povahy a aplikácia vyššie uvedených informácií bude vždy špecifická v závislosti od konkrétnych okolností prípadu. Z uvedených dôvodov pri konkrétnych právnych riešeniach preto vždy odporúčame konzultácie. I keď bulletin nepreberá zodpovednosť za prípadné chyby či nepresnosti, ani za akékoľvek škody vzniknuté z aktivít konaných na základe informácií uvedených v tomto dokumente.

Obsah bulletinu ULC Čarnogurský PRO BONO nie je možné využívať pre účely zisku, ponúkať svojim klientom ako svoj vlastný alebo publikovať bez predchádzajúceho písomného súhlasu spoločnosti ULC Čarnogurský s.r.o. V prípade záujmu o ďalšie informácie alebo o poskytnutie individuálneho poradenstva či konzultácií nás neváhajte kontaktovať.

V prípade, že naďalej nechcete byť adresátom tejto služby, kontaktujte nás na e-mailovej adrese probono@ulclegal.com. Ďakujeme.

V prípade akýchkoľvek otázok nás, prosím, kontaktujte prostredníctvom emailovej adresy office@ulclegal.com.