28. 1. 2026

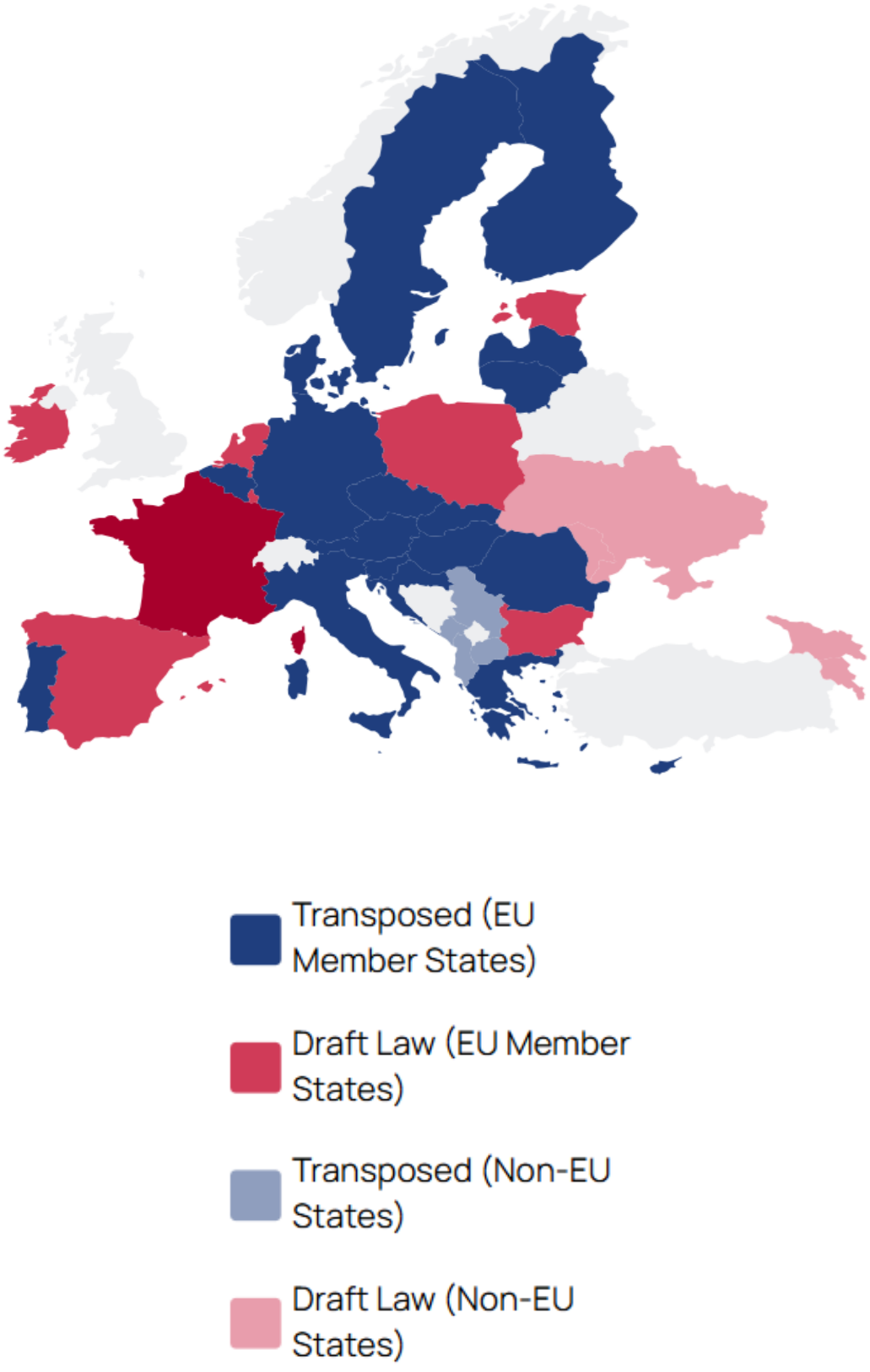
Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Aktuality z práva internetu: kybernetická bezpečnost a online řešení sporů

V závěru minulého roku byla kybernetická bezpečnost určitě nejčastěji vyslovovaným výrazem v oblasti internetového práva v České republice i v mnoha dalších státech EU. V ČR dne 1. listopadu vstoupil v platnost nový zákon o kybernetické bezpečnosti (NZKB), který převedl do českého práva Směrnici EU č. 2022/2555 o opatřeních k zajištění vysoké úrovně kybernetické bezpečnosti v Unii, známé jako NIS 2. Česká republika je jedním z posledních států, které NIS 2 implementovaly několik velkých států se však opozdily ještě víc, např. Francie, Polsko a Španělsko. Nicméně i v těchto zbývajících státech je národní legislativa přijímána, a tedy v několika týdnech budou pravděpodobně všechny členské státy EU již mít NIS 2 implementovanou. Rovněž některé státy mimo EU přijaly zákony velmi podobné NIS 2, např. Velká Británie.

Nyní tedy nastává doba zvýšeného úsilí při plnění povinností předepsaných NIS 2 a související národní legislativou. Nové povinnosti v oblasti kybernetické bezpečnosti se dotýkají velkého množství jak soukromých subjektů, tak veřejných institucí. Náš „domácí“ NZKB stanoví termín 12 měsíců od doručení rozhodnutí o registraci subjektu u NÚKIB, přičemž termín pro provedení „samoregistrace“ na portálu NÚKIB uplynul 31.12. 2025.

U každé významné nové legislativy nastávají situace, kdy některá ustanovení nejsou zcela jasná a jejichž význam a dopady se vyjasňují až po jejich vstupu v platnost. Nejinak je tomu s NZKB a NIS 2. V tomto článku se chci dotknout dvou takových otázek, které se již objevily a jejichž dopady nejsou zatím úplně zřejmé.



Zdroj: The European Cyber Security Organisation (ECSO)
https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

Regulované služby a implementace povinností v nadnárodních skupinách firem

V ČR působí mnoho firem, které jsou součástí firemních skupin, zahrnujících firmy působící v jiných zemích, včetně zemí EU. Pro zjednodušení se budu dále zabývat pouze zeměmi EU. V každé z těchto

zemí buď již je, nebo velmi brzy bude, národní zákon implementující směrnici NIS 2. Jednotlivé národní implementace se do určité míry liší, přestože předpokládám, že NIS 2 je v nich implementována v podstatě správně. Tyto odlišnosti mezi národními legislativci nicméně ztěžují úkoly implementace v rámci firemních skupin a kladou otázky, na které je nyní někdy obtížné odpovědět.

Jednou z odlišností českého přístupu je podrobnost povinností, kdy NZKB a prováděcí vyhlášky obsahují několikanásobně víc (na počet) povinností než obsahuje NIS 2, přestože faktický rozsah povinností odpovídá. Evropská Komise tento český přístup chválí, protože dává větší právní jistotu subjektům, které nyní musí tyto povinnosti uvést do života.

Státy EU kladou různý důraz na různé aspekty kybernetické bezpečnosti. NZKB zjevně klade velký důraz na řízení řetězce dodavatelů, protože rozsah povinností v NZKB a v prováděcích vyhláškách je opět výrazně podrobnější, než je tomu v NIS 2.

Rozdíly, které již způsobují významné dopady, se týkají národních priorit v určování toho, jaké služby by měly spadat pod regulaci a zejména na jaké služby by se měl vztahovat vyšší režim povinností. Jak asi čtenáři vědí, NIS 2 a národní zákony včetně NZKB rozlišují dva režimy, vyšší a nižší. Služby a činnosti na které se vztahuje režim vyšších povinností jsou pod výrazně vyššími požadavky, jejich splnění a následné dodržování si vyžádá mnohem víc nákladů a času než splnění povinností v rámci nižší úrovně regulačních povinností.

Vezměme si následující hypotetickou situaci: regulovaná služba „vesmírné technologie“ v oblasti výzkumu a vývoje je zařazena podle vyhlášky č. 408/2025 Sb. k NZKB (Vyhláška o regulovaných službách) do režimu nižších povinností, bez ohledu na velikost výzkumné instituce. Jeden z velkých členských států EU tuto stejnou službu zařadil do režimu vyšších povinností, opět bez ohledu na velikost subjektu, provádějícího výzkumnou činnost v této oblasti. Existuje pravděpodobně alespoň jedna firma s pobočkami v ČR a v této jiné členské zemi EU, tyto pobočky spolu určitě komunikují, sdílejí data aj. Pokud nejsou jejich technická aktiva zcela oddělená, což v dnešní době spíše nepředpokládám, pak tuzemská firma velmi pravděpodobně proto stejně „spadne“ do režimu vyšších povinností díky sesterské firmě v jiném členském státě EU.

Nebo jiná hypotéza: jiný obor výzkumné činnosti je prováděný významnou nadnárodní firmou, působící v řadě členských zemí EU. Ve všech zemích až na ČR je tento obor považovaný za činnost s nižším režimem povinností, pouze v ČR je považovaný za obor klíčový, tedy s vyšším režimem. Nadnárodní skupina má v ČR jen velmi malou pobočku, která se účastní výzkumu v rámci skupiny. Tato malá pobočka, v podstatě jeden malý tým několika výzkumníků, tak může teoreticky ovlivnit režim povinností pro celou velkou nadnárodní skupinu s tisíci pracovníky. Což vzhledem k této skutečnosti bude mít za následek poměrně vysoké náklady na zajištění všech opatření ve vyšším režimu povinností.

Existuje řada souvisejících otázek: jestliže část skupiny je v režimu vyšších povinností kvůli jedné ze služeb a jiná část skupiny v jiných zemích je ve stejném režimu kvůli jiné službě, jak zajistit efektivní implementaci rozsáhlých povinností v rámci skupiny a současně splnit požadavky národních zákonů? Lze např. řídit implementaci z jednoho centra? Lze pořizovat a udržovat jednu sadu bezpečnostní dokumentace, s místními rozdíly? V jakých jazycích? Je možné a vhodné monitorovat (řízení detekce a prevence kybernetických hrozeb a incidentů) z jednoho centra ve všech zemích? Lze vytvářet virtuální skupinové týmy expertů na kybernetickou bezpečnost, které budou působit pro všechny firmy v rámci jedné nadnárodní skupiny? Lze takto plnit předepsané personální role dle NIS 2 a národních zákonů zemí, v nichž působí členské firmy nadnárodní skupiny?

Velmi bude záležet na požadavcích národních regulátorů. V ČR máme podle mého názoru dobrý

příklad – NÚKIB myslím zatím plní svou funkci výborně, portál NÚKIB obsahuje rostoucí počet návodů, pomocných popisů a výkladových stanovisek a prezentací. Doufejme, že NÚKIB ve svém důrazu na srozumitelnost a transparentnost bude pokračovat.

Evidence „průřezových“ aktiv, popisujících různé regulované služby

Další otevřenou otázkou, která souvisí s implementací povinností dle NIS 2 v nadnárodních firmách, ale nejen v nich, je to, jak správně v souladu s národními zákony evidovat aktiva. Předpokládám, že čtenáři se již setkali s termíny primární a podpůrná aktiva. Primární a podpůrná aktiva je možné vhodným způsobem agregovat podle metodiky, kterou si může stanovit každá regulovaná organizace podle svých potřeb a faktického stavu – a musí si ji obhájit před potenciálními kontrolory z NÚKIB. Míra agregace je důležitá kvůli další práci na zavádění zákonných povinností. Příliš detailní evidence aktiv ztěžuje jejich evidenci a údržbu této evidence, příliš velká agregace zase způsobuje problémy s kontrolou splnění požadavku na popis/obsáhnutí každé regulované služby prostřednictvím evidence aktiv.

V rámci poradenské činnosti jsme se setkali také s aktivy – svou povahou primárními, které jako by prostupovaly tyto dvě kategorie dané legislativou a prostupovaly i napříč více než jednou regulovanou službou. Příkladem jsou IT služby a bezpečnostní služby, které jsou často v rámci firemních struktur poskytovány jak interně pro zajištění služeb poskytovatele, tak externě pro jiné subjekty v rámci stejné skupiny. Takových příkladů přitom může být víc. Poskytování IT služeb a bezpečnostních služeb v rámci skupiny patří obvykle pod regulovanou službu „poskytování řízené služby“, resp. „poskytování řízené bezpečnostní služby“, nicméně fakticky jsou primární aktiva v obou případech využívána také na přímou podporu služeb vlastního poskytovatele, přičemž tyto služby jsou také předmětem regulace podle NZKB. Tato primární aktiva tedy nelze dost dobře „rozdělit“, respektive by to neodpovídalo faktickému stavu.

Je tedy možné, aby organizace evidovaly jedno primární aktivum napříč všemi, nebo některými regulovanými službami? Těmto primárním aktivům říkám „průřezová“. Myslím si, že to možné je, pokud lze v dalších úrovních evidence aktiv popsat či vydělit části, které patří pouze jedné určité regulované službě, tedy aby byl splněn požadavek na popis každé jednotlivé regulované služby zvlášť. Mělo by to být možné na úrovni informací jako dalšího typu primárních aktiv, anebo na úrovni souvisejících podpůrných aktiv.

Online řešení sporů jako budoucí bezpečnostní opatření v oblasti kybernetické bezpečnosti u služeb zaměřených na spotřebitele

Kromě národních zákonů ve vztahu k NIS 2 byl konec roku a začátek nového roku zajímavý také z jiné oblasti – online řešení sporů. Domnívám se přitom, že tyto dvě oblasti zdánlivě nesouvisející se v blízké budoucnosti úžeji přiblíží a snad i protnou. Proto se u této problematiky také krátce zastavíme.

V listopadu 2025 Rada EU odsouhlasila návrh změn Směrnice EU č. 2013/11 o alternativním řešení spotřebitelských sporů (tzv. ADR Směrnice). Jakmile tento finální návrh odsouhlasí Evropský Parlament a vstoupí v platnost (což se předpokládá v prvním pololetí tohoto roku), budou mít členské státy 26 měsíců na to přijmout národní legislativu, upravující národní zákony do souladu s ADR Směrnicí, a nová pravidla začnou platit 32 měsíců od zveřejnění Směrnice v Official Journal. V tomto

článku nechci uvádět podrobnosti, jen to, že ADR Směrnice obsahuje zatím nejvýznamnější podporu alternativního řešení sporů a zejména online řešení sporů pro spotřebitelské spory. Délka lhůty na implementaci nových ustanovení je značná, což je dáno rozsahem úkolů, které musí členské státy zajistit. Jen pro ilustraci: akreditovaná ADR centra pro spotřebitelské spory budou muset podporovat přístup osob s různými druhy digitálních znevýhodnění, což je velmi správný úkol, který však bude v praxi dost obtížné splnit. Státy EU tak budou světovými průkopníky.

Současně již na konci ledna bude v New Yorku představen nový standard mezinárodní standardizační organizace IEEE označovaný P7012 nebo také „My Terms“. Tento standard obsahuje možnost spotřebitelů nebo šířeji občanů navrhovat své požadavky na nakládání se svými daty ve vztahu k třetím stranám, poskytujícím služby a produkty na internetu, tak, aby tyto vlastní podmínky byly čitelné digitálními systémy. Tedy aby zařízení uživatelů-lidí mohlo komunikovat se zařízeními prodejců anebo poskytovatelů služeb a aby lidé mohli prostřednictvím těchto zařízení uzavírat platné smlouvy se svými navrženými podmínkami, nikoliv s typovými podmínkami prodejců. Po vyhlášení v lednu nastane období uvádění tohoto standardu do praxe.

Jedním z předpokládaných úspěchů My Terms bude vynutitelnost uzavřených podmínek, na které prodejci přistoupí a následně je poruší. V tomto ohledu se předpokládá klíčový význam standardizovaného online řešení sporů, kdy by spory o porušení My Terms měly být snadno a rychle řešeny buď přímo mezi zúčastněnými stranami, nebo nezávislými ADR centry. Zde je souvislost s ADR Směrnicí. Jakmile by došlo k porušení My Terms, spor bude možno řešit ADR centry zřízenými podle ADR Směrnice. Relativně dlouhá doba daná na implementaci ADR Směrnice nemusí být nutně dlouhá, protože prosazování nového standardu do praxe trvá obvykle delší dobu a navíc požadavky ADR Směrnice jsou již známé a mohou se projevit v praxi před vypršením lhůty v ADR Směrnici.

Jak to souvisí s kybernetickou bezpečností? Argumentuji, že obě nedávné události dokládají rostoucí význam online řešení sporů pro internet. Jsem přesvědčený o tom, že v časovém rámci tří let se stane online řešení sporů dalším bezpečnostním opatřením nejprve v oblasti služeb a produktů pro spotřebitele. Jsem velmi rád, že naše práce na standardizaci online řešení sporů k této situaci přispívá a že budu na konci ledna mezi těmi, kdo se (byť na dálku) zúčastní uvedení standardu My Terms do života.

Na závěr bych chtěl uvést, že plánujeme po roce zorganizovat další **sérii** několika seminářů o **implementaci NZKB v praxi**. Předběžný termín je **březen** a bližší informace budou k dispozici na **webu** PRK Partners a v jiných médiích.

Mgr. Ing. Zbyněk Loebl, LL.M.
Of counsel

P / R / K

ADVOKÁTNÍ KANCELÁŘ

PRK Partners s.r.o. advokátní kancelář

Jáchymova 2
110 00 Praha 1

Tel.: +420 221 430 111
Fax: +420 224 235 450
e-mail: prague@prkpartners.com

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona