Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

A. Obecná část

B. Zvláštní část

Hlava I – Portál NÚKIB

K § 1 – Přístup do Portálu NÚKIB a úkony v něm

Toto ustanovení v odst. 1 a 2 specifikuje jakým způsobem se relevantní osoby mají přihlašovat do prostředí Portálu NÚKIB a jaké standardizované formuláře, resp. úkony, jsou jeho prostřednictvím zpřístupněny uživatelům.

Preferovaná metoda přihlašování je přitom zcela záměrně pouze pomocí přidělených přihlašovacích údajů, tedy bez použití prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace. Běžní uživatelé (viz dále), kterým založí účty oprávněná či pověřená osoba, budou oprávněni pouze ke čtení údajů dostupných v Portálu NÚKIB, v takových případech není třeba vyžadovat jejich elektronickou identifikaci či autentizaci, jelikož nejsou vůči Úřadu prováděny žádné závazné právní úkony. Dalším důvodem preference tohoto typu přihlašování je skutečnost, že by nedostupnost kvalifikovaného systému elektronické identifikace mohla způsobovat nemožnost přihlášení do Portálu NÚKIB, a tedy jeho faktickou nedostupnost.

Dle odst. 3 lze vybrané úkony dle zákona o kybernetické bezpečnosti provést pouze „kvalifikovaným“ způsobem, tedy pouze ze strany oprávněné či pověřené osoby, které se identifikují a autentizují prostřednictvím prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace alespoň s úrovní záruky značná. Toto ustanovení navazuje na § X odst. 2 a 3 zákona a pouze upravuje organizační podmínky používání Portálu. Tímto způsobem je zaručeno provedení nezbytných úkonů právně aprobovaným způsobem ze strany k tomu oprávněných osob. Předmětnou úpravou a odpovídajícím technickým nastavením systému není žádný regulovaný subjekt jakkoli znevýhodněn či omezen na svých právech a je zachován princip technologické neutrality, jelikož není vyžadováno využití konkrétního prostředku elektronické identifikace.

Odst. 4 pouze reaguje na situace, kdy by oprávněná či pověřená osoba nebyla občanem České republiky a nebylo by tak možné použít výše popsaný způsob přihlášení, resp. ověření vůči základním registrům. V takových případech bude muset dojít k individuálnímu posouzení oprávnění jednat za poskytovatele regulované služby.

K § 2 – Osoby přistupující do Portálu NÚKIB

V tomto ustanovení jsou vymezeny tři základní role osob přistupujících do Portálu NÚKIB, a sice oprávněná osoba, pověřená osoba a uživatel.

Definice oprávněné osoby vychází z technických možností automatizované elektronické identifikace a autentizace při využití údajů dostupných v základních registrech dle § 26 zákona o základních registrech, a rámcově také z § 30 správního řádu (SŘ) a § 21 občanského soudního řadu (OSŘ). Pokud by oprávnění osob jednat za poskytovatele regulované služby muselo být vždy posuzováno individuálně, přesně v souladu s výše citovanými ustanoveními SŘ a OSŘ, znamenalo by to pro Úřad enormní administrativní zátěž vyžadující významné personální kapacity schopné zvládnout prvotní vlnu registrací tisíců nově regulovaných subjektů. Vyhláška počítá i se situací, kdy konkrétní osoba nebude občanem České republiky, a využití základních registrů tak nebude možné (viz předcházející ustanovení). V případě orgánů veřejné

moci je předpokládáno využití tzv. Jednotného identitního prostoru a Katalogu autentizačních a autorizačních služeb (JIP-KAAS), který je v § 56a zákona o základních registrech označován jako autentizační informační systém.

Oprávněná osoba je způsobilá činit skrze Portál NÚKIB veškeré dostupné úkony, oproti pověřené osobě také pověřovat další osoby a potvrdit registraci organizace, za kterou je oprávněna jednat.

Pověřená osoba je v zásadě „kvalifikovaným“ uživatelem, který byl pověřen ze strany oprávněné osoby vykonávat veškerou agendu související se zákonem o kybernetické bezpečnosti. Pověřenou osobou může být typicky manažer kybernetické bezpečnosti dané organizace, který bude v rámci Portálu NÚKIB spravovat nahlášené údaje a provádět nezbytné úkony. Vzhledem k tomu, že se u těchto osob předpokládá určitá úroveň expertízy v oblasti informačních technologií, nelze jejich povinnou elektronickou identifikaci a autentizaci považovat za jakkoli nepřiměřený, zatěžují či diskriminující požadavek. Naopak jde o zcela nezbytnou funkcionalitu umožňující fungování Portálu NÚKIB v souladu s právními předpisy.

Uživatelem je osoba, které byl zřízen účet ze strany oprávněné či pověřené osoby. Není vyžadována její elektronická identifikace a autentizace, jelikož není oprávněna za poskytovatele regulované služby činit žádné formalizované úkony s výjimkou nahlášení kybernetického bezpečnostního incidentu. Je tedy oprávněna pouze ke čtení informací obsažených v Portálu NÚKIB a k nahlášení incidentu. Řízení přístupů, resp. správa uživatelských účtů, je odpovědností poskytovatele regulované služby, který tyto uživatelské účty zřídil.

K § 3 – Druhy hlášených údajů

Toto ustanovení specifikuje v návaznosti na § X odst. 1 a 2 zákona různé kategorie hlášených údajů a zavádí nezbytné legislativní zkratky využívané v navazujících ustanoveních této vyhlášky, zejména v těch stanovujících obsahové náležitosti jednotlivých úkonů.

Hlava II - Náležitosti vybraných úkonů

K § 4 – Registrace poskytovatele regulované služby

V rámci tohoto ustanovení je blíže specifikován způsob provedení a obsahové náležitosti registrace poskytovatele regulovaných služeb, která musí pobíhat prostřednictvím Portálu NÚKIB.

Registraci určitého subjektu může po své identifikaci a autentizaci iniciovat v zásadě kdokoliv, nicméně registrace musí být v konečném důsledku potvrzena oprávněnou osobou, tak aby bylo zajištěno, že jde skutečně o úkon osoby oprávněné za poskytovatele regulované služby jednat.

Typickým scénářem může být vyplnění registračního formuláře ze strany osoby, která bude v budoucnu pověřenou osobou, například manažerem kybernetické bezpečnosti dané organizace. Oprávněná osoba následně v rámci Portálu NÚKIB provede potvrzení tohoto úkonu v rámci něhož může rovnou pověřit osobu, která zpracovala registrační formulář.

Takové nastavení registrace umožňuje minimální administrativní zatížení poskytovatelů regulovaných služeb a zároveň automatizaci registrace na straně Úřadu.

K § 5 – Změna registrace poskytovatele regulované služby

Ke změně registrace dochází v případech, kdy již registrovaný poskytovatel regulované služby začne poskytovat jakoukoliv další regulovanou službu nebo u něj dojde ke změně režimu v tom smyslu, že se přesune typicky z nižšího režimu do vyššího z důvodu navýšení počtu zaměstnanců či obratu, nebo naplnění jiných relevantních kritérií. V těchto situacích může u poskytovatele regulované služby dojít ke změně rozsahu jeho práv a povinností včetně běhu

některých lhůt, pročež je změna registrace specifickým úkonem lišícím se od běžné změny hlášených údajů. Je samozřejmě možné, že vedle změny registrace bude nezbytné provést také „běžnou“ změnu některých nahlášených údajů. Účelem je mimo jiné, aby měl poskytovatel regulované služby jasnou informaci o tom, jaký je rozsah zejména povinností a od jakého okamžiku plynou lhůty k jejich plnění.

K § 6 – Pověření osoby

Pověření osoby je proces přidělení oprávnění konkrétní fyzické osobě činit skrze Portál NÚKIB jménem poskytovatele regulované služby nezbytné úkony, u kterých je vyžadováno provedení ze strany pověřené osoby. Drobným specifikem pověření je, že ho může provést pouze oprávněná osoba, přičemž musí jednoznačně identifikovat pověřenou fyzickou osobu, tak aby byla následně možná její elektronická identifikace a autentizace skrze výše popsané procesy.

K jednomu poskytovateli regulovaných služeb může být přiřazeno více pověřených osob, jejichž rozsah oprávnění je totožný. Poskytovatel regulovaných služeb je přitom povinen zajistit dostatečnou zastupitelnost těchto osob (srov. § X odst. 5 *[Hlášení údajů]* zákona).

K § 7 – Hlášení kybernetického bezpečnostního incidentu

V rámci tohoto ustanovení je blíže specifikován způsob provedení a obsahové náležitosti jednotlivých hlášení prováděných v souvislosti s kybernetickým bezpečnostním incidentem. Výčet veškerých možných hlášení je obsažen v odst. 2 tohoto ustanovení, přičemž formulář pro hlášení incidentu umožní kontinuální doplňování relevantních informací, právě od prvotního varování až po závěrečnou zprávu.

Jak bylo řečeno výše, zákon i vyhláška počítají se situacemi, kdy kybernetický bezpečnostní incident z objektivních důvodů nebude možné nahlásit skrze Portál NÚKIB, pročež zavádějí náhradní způsoby hlášení skrze e-mail, datovou schránku a přinejhorším telefonicky. Pro tyto náhradní způsoby hlášení se přitom obsahové náležitosti uplatní obdobně.

Zákon počítá s možností nahlášení kybernetického bezpečnostního incidentu také ze strany dobrovolných ohlašovatelů, a to skrze formulář dostupný na webu Úřadu. Pro tyto případy jsou taktéž vymezeny obsahové náležitosti daného formuláře, tak aby bylo ze strany Úřadu možné automatizované efektivní zpracování těchto podání.

K § 8 – Obsahové náležitosti dalších úkonů

Toto ustanovení vymezuje obsahové náležitosti jednotlivých formulářových podání, která nebyla řešena v jiných ustanoveních vyhlášky. Toto ustanovení je nezbytné pro vyhovění požadavkům nálezu Ústavního soudu ze dne 12. listopadu 2019, sp.zn. Pl. ÚS 19/17, na dostatečně určité vymezení obsahu standardizovaných formulářových podání.

Návrh vyhláška má obdobnou strukturu jako vyhláška č. 180/2021 Sb., o náležitostech formulářů k evidenci skutečných majitelů a o změně souvisejících vyhlášek, a obdobně jako tato vyhláška neobsahuje konkrétní šablony jednotlivých formulářů, jelikož o jejich konkrétní grafické a funkční podobě nebylo dosud rozhodnuto. Vzhledem k tomu, že se předpokládá jejich interaktivita, by publikace statických šablon mohla činit problémy při možných aktualizacích.

K § 9 – Účinnost

Protože podstatnou část návrhu zákona, resp. z něj odvozeného návrhu této vyhlášky tvoří transpozice směrnice NIS2, je také stanovení účinnosti nové právní úpravy s požadavky této směrnice úzce spojeno. V souladu s obsahem čl. 41 odst. 1 jsou členské státy povinny přijmout a zveřejnit opatření nezbytná pro dosažení souladu s touto směrnicí do 17. října 2024, přičemž od 18. října 2024 se tato opatření použijí. Z tohoto důvodu je také nutné, aby byla právní úprava

podle tohoto návrhu zákona a jeho prováděcích právních předpisů přijata nejpozději k 18. říjnu 2024 a zároveň ještě předtím byla zajištěná dostatečná legisvakanční lhůta, aby se povinné orgány a osoby stihly připravit na veškeré povinnosti.