DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Pravidla pro Národní identitní autoritu

Zásadním požadavkem bezpečnosti a transparentnosti pro informační systémy veřejné správy je požadavek na jednotnou elektronickou identifikaci externích uživatelů. Pro každou operaci je nutná znalost osoby, která tuto operaci provádí zvláště z hlediska nepopiratelné zodpovědnosti osoby. Externí uživatelé (klienti) informačních systémů veřejné správy musí být jednoznačně identifikováni zvláště z důvodů ochrany osobních údajů a dále z procesního hlediska, jak předpokládá správní řád (jednoznačné prokázání totožnosti účastníků řízení).

Úloha správy přístupů se pro každý informační systém veřejné správy skládá z následujících kroků:

- **Identifikace –** jednoznačné a nepopiratelné určení fyzické osoby, která přistupuje k informačnímu systému veřejné správy
- **Autentizace** – prokázání, že přistupující osoba je tou osobou, za kterou se vydává. Autentizace probíhá předložením **autentizačních prostředků** (například uživatelské jméno a heslo, autentizační certifikát), které osobě přidělil správce informačního systému
- **Autorizace** – na základě údajů o identifikované a autentizované osobě a dalších údajů o této osobě (například zařazení na pracovní pozici) zařazení osoby do odpovídající role a z toho vyplývající vyhodnocení oprávnění na úkony a data v rámci informačního systému.

NAP v této oblasti vyžaduje naplnění následujících principů pro všechny informační systémy veřejné správy:

1. Každý úřad, který poskytuje své služby elektronicky, potřebuje svého klienta ověřit (ztotožnit) s využitím kvalifikovaného systému elektronické identifikace, jehož služby jsou poskytovány Národní identitní autoritě. Ověření totožnosti vyžaduje právní předpis nebo výkon působnosti.
2. Pro využití Národní identitní autority se musí organizace stát tzv. kvalifikovaným poskytovatelem služeb (Service provider; SeP), dle postupu popsaném níže.
3. Každý úřad musí akceptovat nejen identitu českého občana, ale kteréhokoliv občana Evropské Unie dle eIDAS.
4. Jakýkoliv nový identitní prostor musí být budován tak, aby byl federovaný v rámci Národní identitní autority.
    1. Před tvorbou nového identitního prostoru je potřeba si prvně udělat analýzu, zda nepostačuje některý z federovaných identitních prostředků v rámci Národní identitní autority.
5. Prostředky pro identifikaci a autentizaci jsou vždy vydány bezpečnou a jednoznačnou cestou identifikované osobě tak, aby byla zajištěna minimální úroveň důvěry. O vydání prostředků existuje trvalý záznam spolu s údaji, jak byla ověřena identita osoby.
6. Osoba, jíž byly prostředky vydány, zachází s prostředkem s náležitou péčí tak , aby nedošlo k jeho zneužití či odcizení.
7. Osoba, jíž byly prostředky vydány, nese nedílnou zodpovědnost za všechny úkony, které byly v informačním systému provedeny při použití těchto prostředků.
8. Věcný správce agend, které jsou vykonávány v rámci informačního systému, zodpovídá za obsazení osob do rolí (technicky vykonává technický správce informačního systému, vždy však na základě podkladů věcných správců). Tuto svoji zodpovědnost může delegovat v rámci organizační struktury na více zodpovědných osob.

Postup ohlášení kvalifikovaného poskytovatele služby (Service provider; SeP)

Následující kroky popisují jednotlivé části procesu, který je naznačen níže, na základě ověření přes ISDS. Aktuálně je registrace organizace prostřednictvím portálu národního bodu přístupná pouze pro orgány veřejné moci, ostatní subjekty musí provést registraci přímo u Správy základních registrů (viz krok 8). Kompletní příručka je dostupná zde.

1. Uživatel jako zástupce organizace požaduje po portálu národního bodu, který je Service Providerem,

službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů.
2. Portál národního bodu kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).
3. Pro ověření uživatele pro registraci organizace či konfigurací jednotlivých Service Providerů je jako Identity Provider určen Informační systém datových schránek (ISDS). Národní identitní autorita provede přesměrování na přihlášení prostřednictvím datových schránek.
4. Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci na portálu národního bodu, musí být přihlášen prostřednictvím ISDS (v definované roli a typem schránky OVM). V případě, že organizace není OVM, je potřeba provést registraci u Správy základních registrů.
5. V případě, kdy je uživatel úspěšně ověřen, Informační systém datových schránek předá Národní identitní autoritě jako výsledek ověření autentizační token obsahující IČO a název subjektu, roli přihlašovaného uživatele a další atributy.
6. Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR) na jehož základě následně provede kontrolu existence IČO.
7. Národní identitní autorita předává portálu národního bodu potřebné atributy z Informačního systému základních registrů a atributy přijaté v autentizačním tokenu z Informačního systému datových schránek, které jsou nutné ke zpracování formuláře pro registraci.
8. Na základě úspěšného splnění předchozích kroků umožní portál národního bodu uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci. Toto platí pouze pro organizace, které jsou OVM. Není-li organizace OVM, jsou místo registračního formuláře zobrazeny podrobné informace o tom, jakým způsobem provést registraci přímo u Správy základních registrů.
9. Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).
10. Portál národního bodu zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci (seznam konfigurací kvalifikovaných poskytovatelů).
11. Uživatel provede konfiguraci Service Providera zahrnující následující údaje:
    - IČO subjektu
    - Název kvalifikovaného poskytovatele
    - Popis kvalifikovaného poskytovatele
    - URL adresa odkazující na úvodní webové stránky kvalifikovaného poskytovatele
    - URL adresa pro odeslání požadavků
    - Adresa pro příjem vydaného tokenu
    - URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu
    - Načtení certifikátu
    - Adresa pro načtení veřejné části šifrovacího certifikátu z metadat
    - Zpřístupnění autentizace prostřednictvím brány eIDAS
    - Logo kvalifikovaného poskytovatele

Příklad pro poskytovatele zdravotních služeb

Poskytovatel zdravotních služeb není orgán veřejné moci, a proto je třeba zajistit kromě výše uvedeného postupu i následující kroky:

1. Požádat Ministerstvo zdravotnictví o zavedení do registru práv a povinností jako SPUÚ dle povinností vyplývající ze zákonů č. 250/2017 Sb. a č. 372/2011 Sb., ideálně pod agendou A1086
2. Na adrese https://www.identitaobcana.cz/Home/Ovm se přihlásit jako oprávněný uživatel datovou schránkou poskytovatele zdravotních služeb
    - Nově by se mělo nabídnout ruční zadání údajů s dalším postupem
    - Pokud se neobjeví, postupovat dle obecných bodů výše – poslání datové zprávy obsahující potřebné údaje (URL, logo….)
3. Upravit si svůj profil na https://www.identitaobcana.cz/Home/Ovm pro přístup jiných osob (IT oddělení např.) a správu svého profilu, konfigurovat pro Portál pacienta poskytovatele zdravotních služeb.

Podmínky pro nevizuální přihlašování

Přihlašování z mobilních aplikací je založeno na následujících předpokladech:

Poskytovatel služby musí

- vytvořit svoji mobilní aplikaci
- vytvořit svoje API
- zabezpečit komunikace mezi svým API a mobilní aplikaci
- provést registraci svého API a mobilní aplikace v NIA
- definovat a zaregistrovat sadu atributů, které budou obsahem JWT (JSON Web Token)
- zajistit komunikaci mezi API a NIA pro vyzvedávání JWT

NIA poskytuje

- rozhraní pro interaktivní přihlášení
- rozhraní pro registraci mobilní aplikace
- rozhraní pro přihlášení mobilní aplikace
- rozhraní pro API, které si z NIA vyzvedne JWT

Uživatel

- musí mít platný a funkční profil NIA a musí mít k dispozici, alespoň jeden platný přihlašovací prostředek, např. mobilní klíč eGovernmentu anebo bankovní identitu,
- nainstaluje si mobilní aplikaci od poskytovatele služby,
- po prvním spuštění aplikace provede interaktivní přihlášení přes NIA, které zajistí registraci aplikace v NIA,
- podle potřeby bude opakovat interaktivní přihlášení z aplikace, pokud z nějakého důvodu bude registrace v NIA zrušena/zneplatněna (změna konfigurace SePa anebo každých 6 měsíců).

Po registraci mobilní aplikace může provést přihlášení k NIA. Výsledkem přihlášení je tzv. access token, který mobilní aplikace předá komponentě (API) poskytovatele služeb. Tato komponenta (API) následně zavolá definované rozhraní NIA, kde předá access token a své přihlašovací údaje. Na základě tohoto volání NAI provede vydání JWT.

Pravidla určení úrovně záruky pro poskytované služby (LoA)

Každý poskytovatel služby si sám určuje, jakou úroveň záruky (LoA) po uživateli vyžaduje[1)]), pokud neexistuje právní předpis, který by výslovně stanovoval úroveň záruky. Ideální stav je, že toto určení je provedeno pro každou jednotlivou službu, která se na portále poskytuje. Protože se však typicky uživatel předem nehlásí k jedné jednotlivé službě, ale k portálu jakožto agregaci více služeb, má poskytovatel služeb následující možnost:

1. Nastaví úroveň záruky podle nejčastěji využívaných služeb nebo dle nejčetnější úrovně záruky u nabízených služeb. Tato možnost zajistí, že uživateli bude po autentizaci dostupná většina služeb a zároveň se po uživateli nepožaduje prostředek s vysokou úrovní záruky. Pokud však uživatel chce využít služby s vyšší úrovní záruky, než použil při původní autentizaci, měl by být uživatel vyzván k autentizaci prostředkem s vyšší úrovní záruky.
2. Nenastaví žádnou vstupní úroveň záruky. Tato možnost zajistí, že se uživatel autentizuje na daný portál jakýmkoliv identitním prostředkem NIA a až následně se při výběru služby uživatelem kontroluje, zda je pro ni splněna minimální úroveň záruky. Pokud není, měl by být uživatel vyzván k autentizaci prostředkem s vyšší úrovní záruky.
3. Potřebnou úroveň záruky nastaví podle nejpřísnější služby. Tato možnost zajistí, že uživatel bude moci vždy využít všechny služby, které jsou na portále dostupné k vyřízení. Nevýhodou je, že se po uživateli může vyžadovat zbytečně vysoká úroveň záruky, kterou nemusí disponovat prostředky, které vlastní.

Pro jakoukoliv zvolenou variantu z pohledu poskytovatele služeb však platí několik povinností:

1. Požadovaná úroveň záruky u jednotlivých služeb odpovídá informacím uvedených v katalogu služeb a v případném právním předpise, který výslovně stanovuje úroveň záruky.
2. Uživateli autentizovaném s nižší úrovní záruky se neskrývá nabídka služeb vyžadující vyšší úroveň záruky.

Podstatné otázky a odpovědi na využívání NIA

Otázky týkající se Centrálního registru životního prostředí

Otázky týkající se přihlašování uživatelů do systémů Centrální registr životního prostředí, potažmo Integrovaného systému ohlašovacích povinností. Předání proběhlo přípisy Ministerstva životního prostředí:

1. ze dne 19. ledna 2024, sp. zn. ZN/MZP/2024/280/6, odpověď DIA byla poskytnuta pod sp. zn. DIA-2188-2/OPL-2024
2. ze dne 21. listopadu 2023, sp. zn. MZP/2023/110/787, odpověď DIA byla poskytnuta pod sp. zn. DIA-16244-2/OHA-2023

Žádám o doložení právního předpisu nebo o doložení faktu, že výkon působnosti vyžaduje prokázání totožnosti fyzické osoby. Zákon č. 250/2017 Sb., §2 říká, že pokud je nutné prokázání totožnosti, lze to pouze prostřednictvím kvalifikovaného systému. Neříká však, že ISPOP má právo vyžadovat identifikaci fyzické osoby. Roční hlášení je prováděno za právnickou osobu, nikoli za fyzickou.

Jak je vysvětleno výše, pokud agendový zákon neomezí způsob činit podání, je nutné se řídit obecnou úpravou podání uvedenou ve správním řádu, která je pro elektronické podání upravena zejména v ZoPDS a dalších speciálních předpisech. Informační systém veřejné správy je pouze jednou z možností, jak činit podání vůči orgánu veřejné správy. Pokud je agendovým zákonem stanoveno, že se podání vůči orgánu veřejné správy činí prostřednictvím informačního systému veřejné správy dle § 4 odst. (1) písm. d) ZoPDS, je nutné, aby se fyzická osoba, která za povinný subjekt jedná, přihlásila do informačního systému veřejné správy prostřednictvím identity občana, jak ostatně vyplývá také z § 2 ZoEI. V takovém případě pak není nutné podání ani podepisovat, jelikož se uplatní fikce podpisu dle § 8 zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Identitu občana nemám a nebudu si ji zřizovat, takovou povinnost jako občan nemám, jak se mám nadále přihlašovat?

V případě, kdy agendový zákon omezí způsob činit podání vůči orgánu veřejné správy pouze na elektronickou podobu (a agendový zákona nijak blíže neurčuje závaznou podobu úkonu a jeho podání), je možné úkon činit nejen za použití informačního systému, ale dále též např. prostřednictvím datové schránky či sítě elektronických komunikací za použití uznávaného elektronického podpisu dle §4 odst. (1) ZoPDS. Fyzická osoba jednající jménem PO není povinna si pořizovat identitu občana. Identita občana, resp. elektronická identifikace, je obecně pouze jednou z možností, jak učinit podání vůči orgánům veřejné moci.

Nebudu identitu občana využívat v rámci plnění pracovních povinností. Z jakého důvodu by řadoví zaměstnanci měli používat svoji Identitu občana pro plnění zákonných povinností svého zaměstnavatele? Proč není dostačující současný způsob přihlašování do systémů CRŽP? Proč je zásadní znát totožnost ohlašovatele/zaměstnance právnické osoby při takových úkonech jako je ohlášení produkce odpadů?

Využití identity občana je pouze jednou z možností, jak činit úkony vůči orgánům veřejné správy. Zajištění potřebných nástrojů pro plnění povinností povinného subjektu vyplývajících z agendových zákonů by mělo být primárně povinností konkrétního subjektu, na který plnění zákonných povinností dopadá. Pokud zaměstnanci povinného subjektu odmítají využívat či si pořídit identitu občana, měl by jim subjekt, za který mají jednat, umožnit užití datové schránky či zprostředkovat vydání certifikátu pro uznávaný elektronický podpis.

Pokud si propojím Identitu občana ke svému účtu v ISPOP, jak to pak funguje ohledně pokut atp.? Nemůže se stát, že firma bude po mě vymáhat zaplacení pokuty nebo nějakého poplatku, kterou obdrží, na základě podaného hlášení, když tam teď bude moje identita? Předtím to byl účet firemní a bral jsem to jako hlášení za firmu, teď to bude hlášení s mojí identitou.

Odpovědnost fyzické osoby (FO) za digitální úkony činěné v zastoupení právnické osoby (PO) je shodná, jako v případě úkonů činěných v listinné, nedigitální formě. Pokud FO činí úkon vůči orgánu veřejné moci svým jménem, ale v zastoupení a při plnění povinnosti stanovené PO, tak její odpovědnost za toto právní jednání není neomezená, ale odvíjí se od právního titulu, kterým je FO oprávněna za PO jednat. Ať už se jedná například o jednatele uvedeného v Obchodním rejstříku, zaměstnance pověřeného k určitým úkolům nebo zmocněnce na základě plné moci, odvíjí se odpovědnost této FO od konkrétního právního titulu a způsobené škody.

Do SEPNO ohlašuji automatizovaně ze SW přes účet, který jsme si zřídili jako systémový (tzn. pro komunikaci systém-systém), vztahuje se povinnost i na tyto účty? Lze i nadále využívat přihlašování přes Jméno + Heslo + 2. faktor?

Není-li nutné prokazovat totožnost, tak není povinnost využívat identitu občana. Komunikace mezi systémy nevyžaduje prokazování totožnosti, ovšem když je potřeba například zřídit danou komunikaci (vystavení či evidence systémového certifikátu) je nutné tuto službu obsloužit s prokázanou totožností, a tedy i využitím identity občana.

Jakým způsobem je zajištěna bezpečnost úniku dat z identity občana, může zaměstnavatel přikázat zaměstnancům, ať poskytnou svoje osobní údaje? Nedojde tím k porušení zákona GDPR?

Při přihlášení do informačního systému veřejné správy za použití identity občana uživatele přesměruje na Národní bod pro identifikaci a autentizaci (NIA), kde jsou popsány předávané osobní údaje, způsob jejich předání, důvod jejich zpracování, a osoba je vyzvána k udělení trvalého nebo jednorázového souhlasu s jejich zpracováním. Toto řešení je v souladu s právními předpisy upravujícími zpracování osobních údajů. Více informací k této věci konec konců uvádí i MŽP v dokumentu k CRŽP dostupném na tomto odkazu.

Dle jakého konkrétního ustanovení právního předpisu je dovozována povinnost užívat Identity občana, popř. Bankovní identitu k přihlašování do systému ISPOP?

Pokud jde o předmětné ustanovení § 2 zákona č. 250/2017 Sb., o elektronické identifikaci, platí, že „Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace *pouze* prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).“ Elektronickou identifikací se podle čl. 3 odst. 1 Nařízení Evropského parlamentu a Rady č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (nařízen eIDAS) rozumí mj. postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují fyzickou osobu zastupující právnickou osobu.

Ministerstvo životního prostředí, jak sám uvádíte, je správcem obou zmíněných informačních systémů veřejné správy, správa zmíněných informačních systémů je tedy součástí výkonu jeho působnosti. Ke správě informačních systémů veřejné správy nepochybně patří též řízení přístupu k informačním systémům, které probíhá mj. požadavkem na prokázání totožnosti osob, které k těmto informačním systémům přistupují. Prokázání totožnosti je tedy vyžadováno v rámci výkonu působnosti Ministerstva životního prostředí jakožto orgánu veřejné moci a není nutné, aby bylo uvedeno v právním předpisu explicitně. Postup zjišťování totožnosti v rámci přístupu ke zmíněným informačním systémům odpovídá výše uvedené definici elektronické identifikace uvedené v nařízen eIDAS, toto nařízení zároveň počítá s tím, že svou totožnost prokazuje fyzická osoba mj. při zastupování právnické osoby.

Shrnuji, že pokud požadavek na prokázání totožnosti vyplývá z výkonu působnosti a je činěn s využitím

elektronické identifikace, lze jej umožnit pouze prostřednictvím kvalifikovaného systému elektronické identifikace (označovaný též jako NIA, identita občana, atd.), nikoliv jiným způsobem, jak uvádí závěrečná část výše zmíněného zákonného ustanovení.

S ohledem na uvedené považuje Digitální a informační agentura postup Ministerstva životního prostředí za souladný s právní předpisy upravujícími elektronickou identifikaci.

Z jakého důvodu není při přihlašování zaměstnance postupováno stejně jako v případě přihlašování úřední osoby, když se vždy rovněž jedná de facto o zaměstnance?

Pokud jde o jednání při zastupování právnické osoby, je vhodné zmínit, že pokud jde fyzické prokazování totožnosti při jednání za právnickou osobu, je používání fyzických dokladů, které nepochybně nejsou vydány jen pro jednání za právnickou osobu, naprosto běžné. Např. pokud jednatel společnosti s ručením omezeným nebo jiný její zástupce jedná vůči orgánu veřejné moci za tuto společnost osobně nebo činí za tuto společnost písemné právní jednání vyžadující úředně ověřený podpis, prokáže vůči orgánu veřejné moci svou totožnost občanským průkazem nebo např. cestovním pasem, nikoliv dokladem vydaným jen pro kontext zastupování právnické osoby. Digitální a informační agentura neshledává používání kvalifikovaných prostředků elektronické identifikace v těchto situacích od používání fyzických dokladů totožnosti zásadně odlišným. V této souvislosti lze pro úplnost poukázat na to, že je rovněž běžné, že osoby, které nejsou statutárními orgány právnické osoby, ale jde o zmocněné zaměstnance či jiné zmocněné osoby, sdělují v rámci svého zastupování právnické osoby řadu osobních údajů, které se následně objevují např. ve sbírce listin obchodního rejstříku, např. datum narození nebo adresu trvalého pobytu takového zmocněnce.

Pokud jde o autentizaci, tedy o spojení totožnosti určité fyzické osoby s jejím oprávněním jednat za právnickou osobu, a s rozsahem tohoto oprávnění, je toto záležitostí nastavení předmětných informačních systémů a legislativy je upravující. Lze v tomto směru odkázat na analogii např. s nastavením přihlašování k informačnímu systému datových schránek, kdy relevantní právní úprava odlišuje osoby mající primární oprávnění přihlašovat se do datové schránky, tj. v případě právnické osoby její statutární orgán nebo členy statutárního orgánu (srov. § 8 odst. 3 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů) od osob majících odvozené oprávnění přihlašovat se do datové schránky, tj. tzv. pověřených osob (srov. § 8 odst. 6 písm. b) zákona o elektronických úkonech a autorizované konverzi dokumentů). Rovněž právní úprava přihlašování k informačním systémům v působnosti orgánů Finanční správy rozlišuje mezi primárně oprávněnými přihlašujícími se osobami a odvozeně oprávněnými přihlašujícími se osobami (zde např. daňový poradce). Používání kvalifikovaných prostředků elektronické identifikace tedy nebrání společnosti ORLEN Unipetrol RPA s.r.o., aby oprávnění k přístupu k předmětným informačním systémům udělovala a odnímala sama.

Pokud jde o vyjádření pověřence pro ochranu osobních údajů Ministerstva životního prostředí, k tomu uvádíme, že přechod z tzv. proprietární (tj. jen pro konkrétní informační systém vytvořené) elektronické identifikace je procesem postupným a nelze tedy vyloučit, že proprietární identifikace je k přístupu k některým informačním systémům stále využívána do doby zavedení přístupu výlučně prostřednictvím kvalifikovaného systému elektronické identifikace. Vyjádření pověřence pro ochranu osobních údajů Ministerstva životního prostředí je tedy vyjádřením popisu praktické implementace již účinné právní úpravy, nikoliv popis právní úpravy účinné v budoucnu.

Pokud jde o důvody, proč není postupováno stejně jako v případě úřední osoby, platí, že autentizační informační systém (JIP/KAAS) podle § 56a zákona č. 111/2009 Sb., o základních registrech, je zřízen pro ztotožnění fyzických osob, které vykonávají činnosti v agendách jako tzv. nositelé rolí. Cílem je nejen řádná autentizace těchto fyzických osob, ale též vedení řádných záznamů o využívání údajů obsažených v informačních systémech veřejné správy, a to až na úroveň konkrétní fyzické osoby, která údaje využila. Na rozdíl od elektronické identifikace určuje konkrétní fyzické osoby jakožto nositelé rolí přímo orgán veřejné moci, tyto údaje se zapisují do základního registru práv a povinností. S ohledem na výše uvedené je JIP/KAAS určen pro ztotožnění úředníků, kteří jménem orgánu veřejné moci jednají, tj. pro státní zaměstnance, zaměstnance nebo jiné osoby v podobném vztahu k orgánu. Pro úplnost dodávám, že právnická osoba nemůže být nositelem role.

Jakým způsobem se bude postupovat, pokud nastane technická porucha na straně provozovatele systému Identity občana popř. Bankovní identity a systém bude nedostupný a proto nebude možno ověřit ohlašovatele a přihlásit se zejména do systému SEPNO, kde je nutno v krátkých časových intervalech provádět ohlášení? Zákon o odpadech řeší v §79 odst. 3 pouze náhradní postup ohlašování přepravy nebezpečných odpadů při přerušení provozu ISPOP. Nedostupnost systému Identity občana popř. Bankovní identity není nikde řešena, Toto ve svém důsledku znemožní odvoz nebezpečných odpadů a způsobí provozovatelům zvýšenou administrativní i finanční zátěž.

Právní úprava postupu pro případy technických poruch není ve vztahu k elektronické identifikaci zavedena, je nicméně vhodné doplnit, že právní úprava postupu pro případy technických poruch není zavedena ve valné většině případů ani např. ve vztahu např. k technické poruše informačních systémů veřejné správy nebo datových schránek a není mi známo, že by úprava postupu pro případy technických poruch byla zavedena ve vztahu k technické poruše dosud používaných identifikačních nástrojů vůči informačním systémům zmíněným v přípisu. Právní úprava počítá s tím, že tyto nástroje budou dostupné. V případě potřeby je možné využít zmírňujících institutů podle příslušných právních předpisů, v tomto doporučujeme konzultaci s Ministerstvem životního prostředí. Upozorňuje, že v případě využití prostředku elektronické identifikace, jejichž vydavatelem je banka (tzv. bankovní identita nebo bankID), může nastat technická porucha též na straně konkrétní vydávající banky.

Jak bude řešeno neohlášení ve smyslu odmítání požadovaného přihlášení za právnickou osobu prostřednictvím individuálních možností fyzické osoby dle výše uvedených argumentací?

V tomto doporučujeme konzultaci s Ministerstvem životního prostředí.

1)
Přehled prostředků s jejich úrovní záruky seznam_poskytovatelu_identity_identity_provideridp