



C1V2 – shrnutí projektových výstupů

Analýza legislativy upravující informační systémy veřejné správy a další způsoby poskytování informací

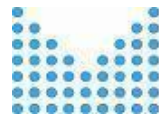
Vytvořeno v rámci projektu

Rozvoj datových politik v oblasti zlepšování kvality
a interoperability dat veřejné správy
CZ.03.4.74/0.0/0.0/15_025/0013983

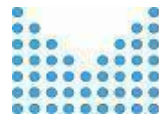
Klíčová aktivita: 01 Zvýšení počtu orgánů veřejné moci poskytujících otevřená data

Indikátor: 8 05 00 Počet napsaných a zveřejněných analytických a strategických dokumentů (vč. evaluačních)

Verze výstupu: 01



Popis výstupu C1V2	3
I. Analytické texty	4
1. Dokumenty k DEPO2 – Zákon č. 111/2009 Sb. – Veřejný datový fond	4
1.1 Odůvodnění navrhovaných změn v rámci novely DEPO2	4
1.2 Poznámky k novele DEPO – reakce na OLG	5
2. Vyhodnocení open data wishlist – březen 2021	9
3. Věcný záměr zákona o správě dat veřejného sektoru	12
II. Odpovědi na dotazy povinných subjektů	49
1. Odpověď pro Národní knihovnu: Vyjádření k možnosti publikovat databáze Národní knihovny jako otevřená data (2019)	49
2. Komunikace s Parlamentním institutem – K povinnostem vyplývajícím z § 4b odst. 2 (2019)	53
3. Vysvětlení pro OLEG: Otevřené formální normy na obsahy úředních desek (2020)	55
4. Reakce na Estonský <i>white paper</i> k možnosti publikovat jako otevřená data osobní údaje na základě jejich zařazení od HVDs (2020)	56
5. Vyjádření OHA MVČR k otázce poskytnutí dat z webové stránky www.kudyznudy.cz společnosti SmartGuide s.r.o. (IČ: 07254890) (2020)	57
6. Doporučení k vyhodnocování povinnosti vyplývajících z § 5a odst. 2 zákona č. 106/1999 Sb. (2021)	59
7. Dotazy zaslané od společnosti Databox po provedeném školení na téma právní úprava otevřených dat (2021)	61
8. Vyjádření pro Národní knihovnu ohledně možnosti publikace jejich databází jako otevřená data (2021)	64



Popis výstupu C1V2

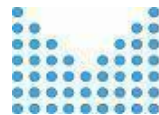
V rámci výstupu C1V2 měla být provedena analýza existující právní úpravy, která se dotýká otevřených dat, přičemž rozsah byl nadefinován tak, že měla být provedena analýza předpisů zejména č. 123/1998 Sb., 365/2000 Sb. a 111/2009 Sb. Průběh práce na projektu KODI a požadavky ze strany MVČR nakonec vedly k drobnému formálnímu posunu, kdy analýza zákona č. 123/1998 Sb. z hlediska možnosti publikace otevřených dat vztahujících se k informacím o životním prostředí byla provedena v rámci práce na novele zákonů č. 106/1999 Sb., a č. 123/1999 Sb., připravované za účelem implementace směrnice EU č. 2019/1024 (Open data směrnice). Analýza zákona č. 123/1998 Sb. byla tak věcně zpracována v rámci výstupu C1V3, který byl uzavřen již na počátku roku 2021.

V případě zákona č. 111/2009 Sb. byla analýza vhodné možnosti posílení principů otevřených dat v rámci předávání údajů mezi orgány veřejného sektoru provedena v rámci prací na velké změnové novele tzv. DEPO 2, která vešla v platnost jako zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci. Výsledkem je tzv. propojený datový fond a veřejný datový fond. Tento dokument je součástí této shrnující zprávy.

Z hlediska zákona č. 365/2000 Sb. došlo k primárně k identifikaci nedostatečné úpravy principů řízení dat. Výstupem této části je návrh věcného záměru zákona o správě dat veřejného sektoru, který tento problém detailně rozebírá a adresuje jej možným řešením.

Tento shrnující zpráva je rozdělena do dvou základních částí. První část tvoří jádro tohoto výstupu. Obsahuje plný text návrhu věcného záměru zákona o správě dat veřejného sektoru ve verzi, v jaké byl odeslán do vnitrorezortního připomínkového řízení na konci května 2022. Dále obsahuje vyhodnocený open data wish-list uzavřený k březnu 2021. Konečně obsahuje rovněž argumentační podklady pro novelu zákona č. 111/2009 Sb. Tyto dokumenty v rámci první části řazeny v chronologickém pořadí.

Druhá část tohoto dokumentu obsahuje texty dílčích analýz konkrétních praktických problémů a odpovědi na otázky související s publikováním otevřených dat, se kterými se na OHA obracely jiné orgány veřejné správy a další zapojené subjekty. Byť tyto dílčí výstupy z hlediska zadání výstupu C1V2 plní doplňkovou roli, byla jejich prostřednictvím naplněna důležitá role OHA jakožto konzultačního pracoviště podporujícího ekosystém otevřených dat v ČR. Jednotlivé dílčí části jsou řazeny v chronologickém pořadí, jak postupně vznikaly.



I. Analytické texty

1. Dokumenty k DEPO2 – Zákon č. 111/2009 Sb. – Veřejný datový fond

1.1 Odůvodnění navrhovaných změn v rámci novely DEPO2

Návrh na rozšíření o Veřejný datový fond–číselníkový

Gestor agendy při ohlášení agendy uvede ve výčtu údajů vedených nebo vytvářených v rámci agendy informaci o tom, zda je daný údaj kódován číselníkem. Údaj kódovaný číselníkem je údaj, který může nabývat pouze předem daných hodnot definovaných číselníkem. Číselníky kódující údaje musí být publikovány jako otevřená data. Primárně jsou pro kódování údajů používány již existující číselníky publikované jako otevřená data jinými ústředními správními úřady. Až v případě, že potřebný číselník ještě neexistuje jako otevřená data, publikuje gestor agendy svůj vlastní číselník jako otevřená data sám. Nutnou součástí publikace číselníku jako otevřená data je také jeho katalogizace v národním katalogu otevřených dat. K analýze, zda potřebný číselník již existuje jako otevřená data, používá gestor agendy národní katalog otevřených dat. Ve výčtu údajů je potom pro údaj kódovaný číselníkem uveden odkaz na katalogizační záznam číselníku v národním katalogu otevřených dat. Gestor agendy zajistí, že informační systémy veřejné správy používané pro výkon agendy skutečně využívají tento číselník v aktuální verzi zaznamenané v registru práv a povinností a v národním katalogu otevřených dat.

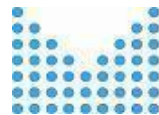
V případě údajů z jiných agend, které jsou kódovány číselníky a využívány v rámci agendy, musí správce informačního systému veřejné správy využívajícího tyto údaje zajistit použití příslušných číselníků v aktuální verzi dle národního katalogu otevřených dat. Protože jsou číselníky publikovány jako otevřená data, neprobíhá za účelem zajištění přístupu k číselníkům proces schvalování čerpání číselníků. Tím je redukována administrativa spojená s výměnou údajů mezi informačními systémy veřejné správy.

Pro zajištění aktuálnosti číselníků přijímají informační systémy veřejné správy notifikace o změnách ve využívaných číselnících prostřednictvím centrální notifikační služby. Informační systém veřejné správy využívá číselník, pokud agenda, pro jejíž výkon informační systém slouží, čerpá údaj, který je tímto číselníkem kódován. Oprávnění čerpání je zaznamenáno v registru práv a povinností a z tohoto záznamu vyplývá také využívání číselníku.

Tato varianta je přítomná v minimalistické podobě přiloženém návrhu (změny vyznačené žlutě).

Plán do budoucna: Návrh na rozšíření o Veřejný datový fond -obecný

Gestor agendy při ohlášení agendy uvede ve výčtu údajů vedených nebo vytvářených v rámci agendy pro každý údaj informaci o tom, zda je údaj veřejný nebo neveřejný. Údaj je neveřejný, pokud existuje legislativní ustanovení, ze kterého neveřejnost údaje vyplývá. V opačném případě je veřejný. Pro neveřejný údaj uvede gestor agendy odkaz na legislativní ustanovení, ze kterého neveřejnost vyplývá. Správce informačního systému veřejné správy, který vede údaje označené jako veřejné, publikuje části dat spravované tímto informačním systémem veřejné správy a odpovídající těmto údajům jako otevřená data a katalogizuje je v národním katalogu otevřených dat. Ostatní části dat spravované tímto informačním systémem veřejné správy, tj. ty odpovídající neveřejným údajům, publikuje také jako otevřená data včetně katalogizace v národním katalogu otevřených dat, avšak po odpovídající anonymizaci nebo agregaci. Při agregacích může dojít k potřebě využití číselníku. Potom se postupuje stejně,



jako v případě číselníků kódujících údaje. Gestor agendy uvede v ohlášení agendy pro každý veřejný i neveřejný údaj datové sady, prostřednictvím kterých jsou části dat odpovídající tomuto údaji publikovány jako otevřená data. Datové sady jsou uvedeny v hlášení agendy ve formě odkazů na katalogizační záznamy datových sad v národním katalogu otevřených dat.

Pokud gestor agendy při vyhodnocování, jaké údaje, z jakých informačních systémů veřejné správy bude potřeba pro výkon jím ohlašované agendy využívat, zjistí, že některé potřebné údaje jsou dle evidence v registru práv a povinností veřejné, uvede je v ohlášení agendy, ale schválení využívání těchto údajů bude automaticky vyřízeno kladně. Tím je redukována administrativa spojená se schvalováním. V případě posuzování požadavku k přístupu k neveřejným údajům může Ministerstvo vnitra navrhnout správci agendového informačního systému, ve kterém jsou neveřejné údaje vedeny, jejich označení za veřejné. V případě nesouhlasného stanoviska správce k návrhu na označení údajů za veřejné rozhodne v případě těch správců, kteří jsou podřízeni vládě, o konečném označení údajů za veřejné vláda jako vrcholný orgán moci výkonné a subjekt odpovědný Poslanecké sněmovně mj. za výkon veřejné správy, a to s využitím stanoviska Úřadu pro ochranu osobních údajů. V případě ostatních správců je stanovisko správců konečné. V případě označení původně neveřejných údajů za veřejné zajistí správce příslušného informačního systému veřejné správy publikaci příslušné části dat jako otevřená data a gestor agendy zajistí označení údajů v evidenci v registru práv a povinností jako veřejné.

Pokud gestor agendy při vyhodnocování, jaké údaje, z jakých informačních systémů veřejné správy bude potřeba pro výkon jím ohlašované agendy využívat, zjistí, že některé potřebné údaje jsou dle evidence v registru práv a povinností neveřejné, ale potřebuje využívat pouze anonymizovanou nebo agregovanou podobu údajů zveřejněnou jako otevřená data, uvede v ohlášení agendy i tuto potřebu. Ke schválení využívání těchto údajů bude automaticky vyřízeno kladně. Účelem tohoto kroku je zaznamenat v registru práv a povinností i využívání těchto údajů, aby bylo možné notifikovat uživatele dat o změnách v datech a také vytvářet kompletní atlas dat a datových toků ve veřejné správě ČR.

Tato varianta zatím zahrnuta v textu předpisu není. Jde nicméně o dlouhodobý cíl, který je v souladu s Informační koncepcí ČR.

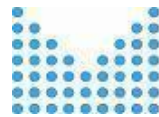
Obecný text pro obě varianty

Publikace dat z informačních systémů veřejné správy se musí řídit obecnými pravidly pro publikaci otevřených dat vydaných Ministerstvem vnitra, včetně dodržování otevřených formálních norem stanovených Ministerstvem vnitra.

1.2 Poznámky k novele DEPO – reakce na OLG

Číselníky

- Oceňujeme, že zmínka o číselnících zůstala v návrhu přítomná, bohužel v této podobě míří zcela mimo účel, který jsme zamýšleli.
- Cílem je takový stav, kdy se v rámci veřejné správy používají sjednocené číselníky. Proto, pokud jsou pro agendu používány údaje, které jsou kódovatelné číselníkem, jsou tyto číselníky zveřejňovány jako otevřená data.
- Číselníky vznikají na principu „první příchozí“ – pokud ohlašovatel agendy bude užívat údaje, které jsou číselníkem kódovatelné, tak nejprve zkontroluje, zda již takový číselník neexistuje a pokud ne, tak vytvoří číselník nový, který zveřejní jako

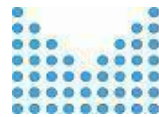


otevřená data. Pokud gestor jiné agendy bude využívat ve své agendě stejné kategorie údajů, musí již použít takto vytvořený číselník.

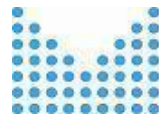
- Více viz dokument – číselníky odůvodnění
- Tvůrcem a zveřejnitelem číselníku je tak první ohlašovatel agendy, která využívá údaje kódované číselníkem.
- Toto je naprosto klíčový režim povinnosti, o kterém jsme měli za to, že je dostatečně vyjádřen v našem návrhu § 54 odst. 1. Pokud to jasné není, určitě souhlasíme s tím, aby se předpis přeformuloval. **Tato povinnost je ale naprosté minimum, které z hlediska efektivní práce s daty veřejné správy musí být zachována.**
- Textace, jak je v současné době navrhovaná v § 54 odst. 1 („správce registru práv a povinností umožňuje údaj uvést s využitím číselníku, ohlašovatel agendy uvede údaj s využitím číselníku“) neodpovídá výše nastíněnému účelu úpravy a v kontextu novely je nadbytečná.

Veřejný datový fond

- K účelu navrhované právní úpravy
 - Novela má za cíl transparentně nastavit režim předávání agendových údajů v rámci výkonu jednotlivých agend různými orgány veřejné správy. Cílem je, aby existující údaje, které jsou potřeba pro výkon většího množství agend, byly přítomné u primárního gestora agendy a ostatní orgány veřejné správy je od něj mohly převzít, pokud je pro výkon svých agend potřebuje. Z toho důvodu se v informační koncepci ČR předpokládá zavedení konceptů veřejného datového fondu (který je tvořený údaji, které jsou veřejně zpřístupnitelné) a propojeného datového fondu (který je tvořený údaji, které nemohou být veřejné a předávají se mezi orgány veřejné správy přímo). Tato koncepce je dlouhodobě schválena a podporována architekturou eGov.
 - Veřejný datový fond je preferovaným způsobem předávání údajů mezi orgány veřejné správy, protože při jeho užití odpadá následná administrativní zátěž při schvalování předávání údajů.
 - Je na diskreci jednotlivých gestorů agend, aby si rozhodly, zda údaje, které v AIS mají jsou veřejné přístupné (ve smyslu publicity veřejné správy), nebo zda nikoli. V tu chvíli je nicméně nezbytné, aby neveřejnost údajů odůvodnili.
 - Primárním cílem návrhu tedy není zveřejnění informací jako takové, to je spíše vedlejší produkt. Cílem je vytvoření infrastruktury předávání údajů mezi jednotlivými orgány veřejné správy. Druhým zásadním cílem pak je přimět garanty agendových systémů, aby si „udělali pořádek v datech“, tedy aby se zamysleli, jaké údaje v systémech mají a roztřídili je. Vzhledem k tomu moc nerozumíme výhradě, že je koncepčním problémem zavedení principu pouze pro AIS a nikoli pro všechny rejstříky. Ze stejného důvodu se nedomníváme, že by byl návrh obcházením principů, které jsou teď přítomné v navrhované implementační novele zákona č. 106/1999 Sb. Pokud toto rozlišení není z materiálu dostatečně jasné, určitě je možné je upřesnit v odůvodnění. Distinkce v účelu normy je však zcela zásadní.



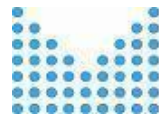
- K zařazení novely do zákona č. 111/2009 Sb.
 - Máme za to, že vzhledem k výše popsanému cíli úpravy je zákon č. 111/2009 Sb. vhodným legislativním nosičem. Umístění do zákona č. 106/1999 Sb. by nebylo vhodné vzhledem k určité bezbřehosti regulovaných subjektů, což je problém, na který jsme několikrát narazili v průběhu příprav různých open data novel zákona č. 106/1999 Sb.
 - Zákon č. 111/2009 Sb. působí a má v kontextu navrhované novely působit jako zvláštní předpis, který jednoznačně vymezuje rozsah povinných subjektů a povinných systémů (proto jde o AIS a nikoli o všechny informační systémy). Díky tomu je možné vyhnout se problému přílišné šíře a nejistoty, který je spojen se zákonem 106/1999 Sb.
- K jednotlivým komentářům:
 - „Z věcného hlediska je úprava nekoncepční v tom, že toto pravidlo zavedeme pro údaje v AIS a nikoliv obecně v rejstřících vedených povinnými subjekty dle stošestky.“
 - Jak je uvedeno výše, není to nekoncepční, protože primární účel návrhu není zveřejňování informací ale vytvoření systému, který umožní efektivní předávání údajů mezi jednotlivými AIS a jejich gestory.
 - „Je riziko, že ex lege zveřejníme údaje, u nichž právní předpis o veřejnosti či neveřejnosti mlčí, ale z povahy věci jde o údaje neveřejné.“
 - Máme za to, že takové údaje nemohou existovat. Zákon 106/1999 Sb. stojí na principu publicity veřejné správy. Pokud není neveřejnost údajů dána zákonem (ať už výslovně, nebo charakterem těch údajů – např. jde o utajované informace) nemůže jejich zveřejnění představovat problém.
 - „Většina AIS není zřízena zákonem (určitě nemáme 4 000 AIS zřízených zákonem). O velkém množství údajů v nich vedených a jejich veřejnosti nemusí být v právním řádu ani zmínka. Pak se mohou stát automaticky veřejnými (nebo se o tom začnou vést spory, bude-li např. agenda, v nichž se povedou, kryta mlčenlivostí).“
 - To opět není problém, viz výše. Navrhovaný princip nezakládá veřejnost údajů obsažených v AIS – ty údaje buď veřejné jsou (a jsou tedy například získatelné žádostí podle z. 106), nebo nejsou.
 - Každopádně toto zhodnocení je na garantovi AIS, který by sám měl nejlépe vědět, jaké údaje v systému má.
 - Pokud je problém ve formulaci, která umožňuje označit údaje jako neveřejné, v tom smyslu, že je moc úzká (a tedy neumožní označit jako neveřejné údaje, které by neveřejné být měly z nějakého důvodu na který jsme zapomněli), určitě si rádi necháme poradit. Námi navrhovaná formulace byla: *„Údaje vedené v agendovém informačním systému jsou veřejné, ledaže je jejich veřejnost vyloučena zvláštním předpisem 57), nebo pokud se jedná o údaje vedené v agendovém informačním systému, které slouží toliko*



k vnitřním procesům správce agendového systému a technickému zajištění fungování agendového informačního systému.“

- „Jestliže se následně ukáže, že došlo k změně veřejnosti nějakých údajů a příslušný ústřední správní úřad se nemohl k změně principu iniciovaného námi, nikoliv poslanci (sic) vyjádřit, bude to problém“
 - Tato situace by neměla nastat, protože princip publicity veřejné správy, viz argumentace výše.
- „Skutečně jsou všechny AIS obsahující veřejně přístupné údaje vytvořeny tak, že umožní dálkový přístup?“
 - V současné době možná ne, ale do budoucna to tak v souladu s principy veřejného datového fondu bude MV prosazováno. I vzhledem k tomu bude vhodné opatřit novelu dostatečně dlouhou legisvakanční lhůtou.
- „Při prosazování stanovování množiny údajů čerpatelných z ISVS v rámci registrace agendy bylo trváno na adekvátním vlivu správce ISVS. Rozpor mezi postoji ohlašovatele agendy a správce ISVS měla řešit vláda jako vrcholný orgán moci výkonné. Zde se předpokládá rozhodování ÚOOÚ. Budou nějaké opravné prostředky?“
 - Další opravné prostředky jsme nepředpokládali, protože již rozhodnutí ÚOOÚ je vlastně opravným prostředkem vůči výzvě MV.
- „Jsou všechny AIS vytvořeny tak, aby umožňovaly zpřístupnit jakémukoliv jinému AIS veřejné údaje? To je důvod, proč v odstavci 1 je užito slovo „může“ (dává prostor pro zohlednění technických možností AIS).“
 - Podobně jako výše, v současné době možná ne, ale do budoucna to tak v souladu s principy veřejného datového fondu bude MV prosazováno. I vzhledem k tomu bude vhodné opatřit novelu dostatečně dlouhou legisvakanční lhůtou.
- Netrváme na neměnnosti našeho návrhu a budeme rádi za pomoc v precizaci. Zakotvení VDF je však zcela zásadní součástí chystané novely, která se na toky dat mezi orgány veřejné správy zaměřuje.

Více odkazujeme na odůvodnění, které jsme zasílali již s minulou verzí návrhu.



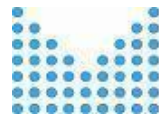
2. Vyhodnocení open data wishlist – březen 2021

V březnu 2021 proběhlo vyhodnocení open data wishlistu, tedy podnětů veřejnosti sbíraných na webových stránce opendata.gov.cz. Zaznamenané podněty byly z rozmezí léto 2019 – březen 2021. I přes relativně dlouhé období se nakonec ve výsledném hodnocení objevilo jen relativně malé množství podnětů (23 unikátních), zřejmě z důvodu nižšího zájmu ze strany veřejnosti. Oproti předchozím iteracím vyhodnocení těchto podnětů proběhlo v mírně zjednodušené podobě, kdy byla opuštěna systematika 5 kategorií,¹ která sloužila hlavně jako prvotní nástroj vyhodnocení vhodnosti a možnosti zařazení požadovaných dat do nařízení vlády č. 425/2016 Sb. Se zrušením tohoto nařízení však tato metodika vyhodnocení podnětů veřejnosti ztratila smysl. Výsledkem vyhodnocení je tak primárně získání základního přehledu o poptávaných datech, jejich právní povaze a zhodnocení, který orgán veřejné správy za ně odpovídá a bylo by ho možné v budoucnu motivovat k jejich zveřejnění.

Vyhodnocení wishlistu je přítomné v následující tabulce:

Označení datové sady	Správce dat	Zákonná úprava	Poskytování dle 106?	Povinnost aktivně poskytovat?	Možnost poskytovat?
Údaje o osobě držitele individuálního oprávnění k využívání rádiových kmitočtů dle ZEK	ČTÚ	127/2005 Sb.; § 15 odst. 5	Obecně ano	Ne	Ne
Záznamy z meteostanic	ČHMÚ	123/1998 Sb.	Ne	Ne	Ano
Anonymizovaná databáze trestných činů a pachatelů evidovaných Policií ČR	Policie ČR	106/1999 Sb.	Ano	Ne	Ano
Data o parkování	Obce	106/1999 Sb.	Ano	Ne	Ano
Průjezdy aut na různých místech včetně typu vozu	Obce	106/1999 Sb.	Ano	Ne	Ano
Počty cestujících v metru z automatických sčítačů	DPP	106/1999 Sb.	Ano	Ne	Ano
Počty nakoupených jízdenek podle místa a způsobu nákupu	Dopravní podniky	106/1999 Sb.	Ano	Ne	Ano

¹ Více viz: <https://opendata.gov.cz/dokumenty:anal%C3%BDza-opendata-wishlist>



Pocty cestujících bus tramvaj lanovka taxi loď přívozy	Dopravní podniky	106/1999 Sb.	Ano	Ne	Ano
Pocty chodců na různých místech	Obce	106/1999 Sb.	Ano	Ne	Ano
Symboly a vlaky obcí	Obce	106/1999 Sb.	Ano	Ne	Ano
Kompletní záznamy z STK od r. 2010	Ministerstvo dopravy	106/1999 Sb.	Ano	Ne	Ano
Aktuální zpoždění vlaků	SŽDC	106/1999 Sb.	Ano	Ne	Ano
Data volné kapacity intenzivní péče	Nemocnice, ÚZIS	106/1999 Sb.	Ano	Ne	Ano
Soupis rybářských revírů	Ministerstvo zemědělství	99/2004 Sb. , o rybářství	Možná	Ne	Ano
Inženýrské sítě					
Rozsudky	Soudy, MSp	106/1999 Sb.	Ano	Ne	Ano
Data leteckého laserového skenování ČR	ČÚZK	123/1998 Sb.	Ne	Ne (Předpokládám, s tou 123/1998 je to místy trochu matoucí)	Ano
Zastávky veřejné dopravy - souřadnice	Obce	106/1999 Sb.	Ano	Ne	Ano
Data z leteckých příruček	Řízení letového provozu	106/1999 Sb.; 49/1997 Sb., o civilním letectví	Ne	Ano	Ano
Ženy a muži ve vedení obcí (+ jejich věk, profese, nominující strana, stranická příslušnost, dále kódy obcí pro rychlé spárování s dalšími daty, např. počty obyvatel)	ČSÚ	106/1999 Sb.	Ano	Ne	Ano
Počet cizinců na úrovni obcí	MV	106/1999 Sb., 111/2009 Sb. (registr obyvatel)	Ano	Ne	Ano - Anonymizované



Silniční databanka (silniční data)	MD, ŘSD (NDIC)	361/2000 Sb., o provozu na pozemních komunikacích	Ne	Ano	Ano
Databáze dopravního značení	MD, ŘSD	106/1999 Sb., 361/2000 Sb., o silničním provozu	Ano	Ne	Ano



3. Věcný záměr zákona o správě dat veřejného sektoru

Úvod

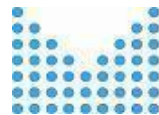
Návrh věcného záměru zákona o správě dat veřejného sektoru je předkládán na základě usnesení vlády č. 332 ze dne 27. dubna 2022, kterým byl stanoven plán legislativních prací na rok 2022.

Důvody pro vytvoření věcného návrhu jsou dva. Prvním z nich je chybějící právní úprava, kdy orgány veřejné správy nejsou dostatečně vedeny k tomu, aby efektivně nakládaly se svými daty. Praxe ukazuje, že existující právní úprava je příliš zaměřena na informační systémy veřejné správy (ISVS) a data jsou chápána pouze jako jejich součást. To vede k situaci, kdy jsou pomíjeny konkrétní aspekty správy dat jako takových. Data uchovávaná v jednotlivých ISVS nejsou popisována a správce ISVS tak často ani přesně neví, s jakými daty disponuje. To následně vede k nedostatečné transparentnosti, protože tuto znalost následně postrádají jak veřejnost, tak hlavně další agendová místa, která by daná data mohla využít v rámci plnění svých agend. Následně tento problém vede k nemožnosti efektivních toků dat v rámci veřejného sektoru, protože jednotlivá agendová místa nemohou bez znalosti existence specifických dat žádat o přístup k nim a jejich využití. Důsledkem je praxe, při které jsou nevhodně pořízována duplicitní data různými orgány veřejné správy pro výkon jejich činností/agend, a při které není naplněn potenciál efektivních datových toků mezi orgány veřejné správy. Znalosti toho, s jakými daty stát nakládá, je nezbytným krokem k dosažení cíle, který je formulován v programovém prohlášení vlády: „*Důsledně budeme vymáhat, aby mezi úřady obíhala data, nikoli občan.*“.² Vyřešení tohoto problému představuje první část z navrhované úpravy.

Druhým důvodem navrhované právní úpravy je absence možnosti tzv. řízeného přístupu k datům, a to zejména za účely vědy a výzkumu. Aktuální právní úprava poskytování informací veřejného sektoru trpí dvěma zásadními problémy. Prvním je nemožnost žádat typově stejné informace od většího množství povinných subjektů najednou, a nemožnost efektivního vyřešení takové žádosti. Důsledkem je nízká efektivita a navyšování nákladů na straně jak žadatele (klienta služeb), tak státu. S tím souvisí nemožnost efektivního a zároveň dostatečně technicky nebo organizačně zabezpečeného přístupu k datům, jejichž poskytnutí je vyloučeno aktuální právní úpravou o poskytování informací. Jedná se zejména o osobní údaje, či informace chráněné právy duševního vlastnictví třetích osob. Kvůli této nedostupnosti přístupu není možné ani následné použití těchto dat, nebo jejich odvozenin, za společensky prospěšnými účely (například vědecký výzkum). Řízený přístup k těmto datům (jejich poskytnutí ve formě, která zároveň naplní cíle žadatele a zároveň působením právních a organizačních záruk zajistí, že riziko jejich zneužití bude minimální) v současné právní úpravě citelně chybí. Řízený přístup k datům pak představuje druhý pilíř navrhované úpravy.

Návrh věcného záměru v první části stanoví povinným subjektům, které budou stejně definovány jako v zákoně 365/2000 Sb., o informačních systémech veřejné správy, povinnost provádět datový přezkum, během kterého budou identifikována data, kterými daný povinný subjekt disponuje. Na základě datového přezkumu pak budou vytvářeny popisy těchto dat, které budou evidovány ve veřejném registru tak, aby byly dohledatelné. Veřejná správa a veřejnost tak budou vědět, s jakými daty stát disponuje a pracuje. Povinné subjekty rovněž

² Programové prohlášení vlády České republiky, 2022, s. 35. Online: <https://www.vlada.cz/assets/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-Petra-Fialy.pdf>



budou formalizovat a garantovat zajištění přístupnosti identifikovaných dat jak pro výkon svých agend, tak pro výkon agend jiných povinných subjektů.

Návrh v druhé části určí jednotný datový úřad, který bude působit jako centrální místo pro vyřizování žádostí o řízený přístup k datům a který bude v případě žádosti o tento přístup, které jsou v gesci většího množství povinných subjektů, propojovat jejich datová rozhraní. Návrh dále obsahuje systém nástrojů (právních, technických i organizačních), které zajišťují ochranu kolidujících práv a zájmů, zejména v podobě práva na ochranu osobních údajů, a minimalizaci rizika, které by bylo s poskytnutím takových dat spojené. Vzhledem k tomu je návrh v souladu s ústavními principy a požadavky, které vyplývají z práva EU.

Druhá část a její konstrukce je inspirována návrhem nařízení EU o správě dat, které v současné době prochází legislativním procesem v Evropském parlamentu. Toto nařízení předpokládá existenci možnosti řízeného přístupu k datům v právních rádech členských států, ale nezakládá ji, ani ji nenařizuje. Základním regulatorním principem předmětné části nařízení o správě dat je zajištění základní úrovně, kterou členské státy mají povinnost splnit, pokud se k poskytování takových dat samy rozhodnou. Návrh věcného záměru zákona o správě dat veřejného sektoru nebude duplicitní právní úpravou správy dat, ale může být nosičem pro harmonizační úpravu vzhledem k evropskému nařízení o správě dat.

V případě částí návrh bude obsah existenci výjimek z uvedených povinností v takových odůvodněných případech, aby byla zajištěna ochrana kolidujících práv a zájmů.

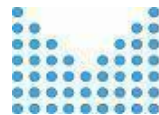
1 Přehled právních předpisů vztahujících se k věcnému záměru zákona

Právní úprava, která se dotýká dat veřejného sektoru³, je v současné podobě velice roztržštěná, a to jak na evropské, tak národní úrovni. Neexistuje žádný jednotný rámec, který by tuto problematiku upravoval komplexně. Na evropské úrovni zajišťuje specifickou ochranu databází práv duševního vlastnictví tzv. databázová směrnice (směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází). Právní úprava dat veřejného sektoru je obecně rámována Evropskou datovou strategií, která byla formulována na začátku roku 2020⁴. Zahrnuje již existující právní předpisy, jako je Obecné nařízení o ochraně osobních údajů (nařízení EU č. 2016/679), Nařízení o volném toku neosobních údajů (nařízení EU č. 2018/1807) a Směrnici o otevřených datech (směrnice EU č. 2019/1024). Do rámce evropské datové strategie pak v blízké době má přibýt Nařízení o správě dat,⁵ jehož cílem je jednak sjednotit pravidla poskytování specifických typů informací, a jednak zajistit bezpečné prostředí pro datové prostředníky a datový altruismus. Dalším chystaným předpisem je tzv. Data Act, který se zaměří na problematiku předávání dat mezi soukromými organizacemi a státními orgány. Krom uvedeného existuje řada specifických

³ V rámci tohoto dokumentu jsou pojmy data, údaje a informace používány ekvivalentně, pokud není uvedeno jinak. Předkladatel si je vědom významového rozdílu mezi těmito pojmy. Navrhovaná právní úprava je věcně rozkročena mezi úpravu informací veřejného sektoru (tedy primárně zákon č. 106/1999 Sb., jak bude uvedeno dále) a úpravu řízení informačních systémů veřejné správy (tedy zákon č. 365/2000 Sb.), přičemž každá z nich pracuje s těmito pojmy odlišně. Není cílem navrhované úpravy sjednocovat rozdílnou terminologii souvisejících právních předpisů. Když se v návrhu hovoří o přístupu k informacím, jsou míněny informace ve smyslu zákona č. 106/1999 Sb., obecně jakýkoli obsah na jakémkoli nosiči, včetně dat.

⁴ Viz online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

⁵ Návrh nařízení zde: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767>



právních režimů, které se zaměřují na konkrétní oblasti úpravy a působí tak jako *lex specialis*. Jde např. o Směrnici INSPIRE (směrnice č. 2007/2/ES), a zvláštní úpravu zveřejňování dat o dopravě (směrnice č. 2010/40/EU).

V českém právním řádu neexistuje jeden zastřešující zákonný rámec, který by komplexně upravoval problematiku dat. Existuje však řada dílčích právních úprav, které se buď věnují specifické oblasti dat a nakládání s nimi (např. zákon č. 111/2009 Sb., o základních registrech a zákon č. 89/1995 Sb., o státní statistické službě), nebo se dat dotýkají nepřímo ať už skrze regulaci informačních systémů dle zákona č. 365/2000 Sb., v nichž se data nacházejí, nebo protože upravují určité kontexty nakládání s nimi.⁶ To je příklad právní úpravy ochrany osobních údajů, ochrany obchodního tajemství, nebo zákona č. 121/2000 Sb., autorský zákon. Specifickou roli zastávají dva zákony zajišťující právo přístupu veřejnosti k informacím v podobě obecného zákona č. 106/1999 Sb. a zvláštního zákona č. 123/1998 Sb.

Níže uvedený seznam obsahuje vybrané nejzásadnější evropské a české právní předpisy, které obsahují regulaci dat a nakládání s nimi. Tento výčet vytváří širší kontext, do kterého navrhovaný věcný záměr směřuje, byť se naprosté většiny z nich přímo nedotýká. Navrhovaný věcný záměr zákona má za cíl doplnit tuto mozaiku v mezích doposud neupravené oblasti. Detailní popis interakce navrhovaného věcného záměru a přímo dotčených existujících předpisů je rozebrán v následujících kapitolách tohoto dokumentu.

1.1 Legislativa EU

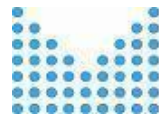
1.1.1 Obecné předpisy

- Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES
- Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii
- Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru

1.1.2 Zvláštní předpisy

- Směrnice Evropského parlamentu a Rady 2007/2/ES ze dne 14. března 2007 o zřízení Infrastruktury pro prostorové informace v Evropském společenství (INSPIRE)
- Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy
- Nařízení 1315/2013, o hlavních směrech Unie pro rozvoj transevropské dopravní sítě a o zrušení rozhodnutí č. 661/2010/EU

⁶ V chápání klasických informačních teorií tak jde o regulaci nakládání s informacemi, jakožto daty v určitém kontextu. Srovnej např. FLORIDI, Luciano, 2010. *Information: a very short introduction*. Oxford ; New York: Oxford University Press. Very short introductions, 225. ISBN 978-0-19-955137-8. a ADRIAANS, Pieter, 2013. Information. In: Edward N. ZALTA, ed. *The Stanford Encyclopedia of Philosophy* [online]. Stanford: Metaphysics Research Lab, Stanford University. Získáno z: <https://plato.stanford.edu/archives/fall2013/entries/information/>



- Nařízení Komise 2015/962, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU

1.1.3 Chystané předpisy

- Nařízení o správě dat
- Tzv. Data Act

1.2 Legislativa ČR

1.2.1 Obecné předpisy

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
 - Podrobně vztah navrhované právní úpravy a tohoto zákona bude rozebrán v kapitole 2.
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- Zákon č. 111/2009 Sb., o základních registrech
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 110/2019 Sb., o zpracování osobních údajů

1.2.2 Zvláštní předpisy

- Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)
- Zákon č. 89/1995 Sb., o státní statistické službě
- Zákon č. 123/1998 Sb., o právu na informace o životním prostředí
- Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování
- Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)

2 Současný právní a faktický stav

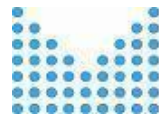
Jak bylo uvedeno v předchozí kapitole, právní úprava datové regulace je nesmírně roztržštěná. To přináší dva hlavní problémy, kterými jsou jednak nepřehlednost právní úpravy a skutečnost, že nepokrývá všechny oblasti, které by regulovat měla. Navrhovaný věcný záměr zákona spadá do oblasti veřejnoprávní regulace a má za cíl postihnout dvě oblasti, jejichž absence úpravy se dlouhodobě ukazuje jako problematická (bude podrobněji popsáno níže). Jsou jimi principy správy dat veřejného sektoru⁷ a úprava regulace řízeného přístupu k datům veřejného sektoru a jejich opětovné užití. První jmenovaná oblast je pak nutným předpokladem pro druhou. Zároveň umožní efektivnější výkon již existujících povinností vyplývajících ze zákona č. 106/1999 Sb., zákona č. 123/1998 Sb., zákona č. 365/2000 Sb. a mnoha dalších.

Navrhovaný věcný záměr zákona o správě dat nemá za cíl být komplexním kodexem, který by vyřešil problém roztržštěnosti právní úpravy nakládání s daty a informacemi ve veřejném sektoru. Naopak, cílem předkládaného tisku je pouze vyplnit dílčí doposud neupravené oblasti.

2.1 Principy správy dat

V českém právním řádu neexistuje úprava, která by se specificky zaměřovala na principy efektivního a korektního nakládání s daty veřejné správy. Na obecné úrovni musí tato činnost

⁷ Pojmem „správa dat“ je použit ve smyslu „data governance“, tedy obecné „řízení nakládání s daty“ a nikoli ve smyslu „data management“. Návrh věcného záměru zákona směřuje na obecné principy nakládání s daty aplikovatelné v celé šíři veřejného sektoru. Není cílem návrhu regulovat přímou správu dat v konkrétních kontextech.



vycházet z principů dobré správy dle správním řádu (zákon č. 500/2004 Sb.). To však, jak praxe ukazuje, není dostatečnou úpravou, neboť orgány veřejné správy nejsou samy o sobě motivovány k tomu, aby si udržovaly o svých datech přehled a pořádek v nich, neboť není jiný právní předpis, který by jim tuto povinnost ukládal. Nejblíže ze současné právní úpravy správy dat dotýká zákon č. 365/2000 Sb., který zavádí pojem informační systém veřejné správy (ISVS) a stanovuje práva a povinnosti, které souvisejí s jejich vytvářením, správou, provozem, užíváním a rozvojem. Informační systém veřejné správy (ISVS) je chápán jako funkční celek zabezpečující informační činnosti. Informační činnosti jsou spojeny s informacemi důležitými pro výkon veřejné správy a zaměřují se na reprezentaci informací daty a na řízení dat prostřednictvím funkcionalit ISVS. Nicméně zákon nestanovuje konkrétní povinnosti spojené s daty, ale pouze s ISVS jako celkem. Datům se věnuje pouze na obecné úrovni, když stanovuje

1. Prostřednictvím ISVS je umožněn přístup k daným datům prostřednictvím referenčního rozhraní i mimo něj více osobám nebo jejich součástí současně.⁸
2. Správce ISVS zajišťuje, aby vazby ISVS na ISVS jiného správce byly uskutečňovány prostřednictvím referenčního rozhraní,⁹ přičemž vazbou se rozumí také sdílení dat.
3. Správce ISVS zajišťuje, aby vazby ISVS na ISVS jiného správce a na IS soukromoprávních uživatelů údajů byly uskutečňovány prostřednictvím centrálního místa služeb.¹⁰
4. Provozovatel ISVS má povinnost předat data uchovávaná v ISVS správci na vyžádání správce a po ukončení provozování ISVS, avšak má právo na úhradu účelně vynaložených nákladů a nejsou dotčena práva k duševnímu vlastnictví.¹¹

Správce ISVS¹² má tedy jen obecné povinnosti týkající se dat, které jej nutí zabývat se daným ISVS pouze jako celkem. Správce nemá určeny povinnosti týkající se správy dat jako takových. Správa dat se tak pouze implicitně předpokládá v rámci povinností spojených se správou ISVS jako celku. To vede k následující praxi, do které jsou správci ISVS nuceni stávající legislativou, s následujícími negativními důsledky:

- **PRAXE neexistující popis dat:** Data uchovávaná v jednotlivých ISVS nejsou popisována, není určen jednotný způsob jejich popisu ani místo, kde by byl popis zveřejněn. Popis by měl zahrnovat popis struktury dat, popis významu dat, popis věcných souvislostí mezi daty a určující legislativou, a popis věcných souvislostí mezi daty napříč různými ISVS jednoho nebo více správců ISVS.
 - **DŮSLEDEK:** Znalosti o datech uchovávaných v jednotlivých ISVS jsou pouze částečné. To znamená, že potenciální uživatelé dat spravovaných v ISVS (např. pracovníci VS ČR, programátoři a další tvůrci služeb s přidanou hodnotou nad daty, novináři, odborníci z veřejnosti, vědecká obec a obecně veřejnost) nemají komplexní přehled o tom, jaká data jsou ve veřejné správě uchovávaná, co znamenají a jak spolu vzájemně souvisí.

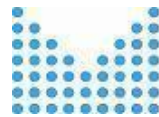
⁸ § 2 písm. p) zákona č. 365/2000 Sb.

⁹ § 5 odst. 2 písm. d) zákona č. 365/2000 Sb.

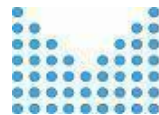
¹⁰ § 6h odst. 4 zákona č. 365/2000 Sb.

¹¹ § 9e zákona č. 365/2000 Sb.

¹² Vymezený v § 2 písm. c) zákona jako „osoba nebo její součást, která poskytuje služby informačního systému veřejné správy a za informační systém veřejné správy odpovídá“.



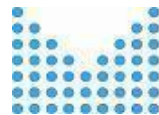
- **DŮSLEDEK:** Pokud někde existují data, která by daný uživatel dokázal smysluplně využít např. pro realizaci/zkvalitnění analýzy, vědeckého výzkumu, aplikační služby pro koncové uživatele, služby veřejné správy pro občany atd., nejsou tato data nalezena a využita a příslušná přidaná hodnota není vytvořena.
- **PRAXE nemožnost přístupu k primárním datům jejich správcem:** K datům uchovávaným v ISVS má správce ISVS zajištěn přístup pouze prostřednictvím uživatelských funkcí ISVS (tj. funkcí dostupných uživatelům prostřednictvím grafického uživatelského rozhraní ISVS, tzv. GUI). Provozovatel či dodavatel ISVS nemá povinnost zajistit přístup ke kompletním datům uchovávaným v ISVS nezávisle na těchto uživatelských funkcích (tzv. primárním datům). Pouze ve specifických případech (explicitní žádost správce ISVS, ukončení provozu) získá jednorázový přístup k datům a často navíc za úplatu. Struktura, v jaké data správce od provozovatele či dodavatele získá, je navíc strukturou databázovou. Databázová reprezentace sice představuje legislativní a doménovou sémantiku dat, ale často používá vlastní technickou terminologii pro pojmenovávání datových prvků a sémantiku rozměňuje díky nutnosti různých technických databázových optimalizací. Podobu, ve které správce data dostane, tak více než legislativní a doménová terminologie, určují databázoví specialisté dodavatele či provozovatele, nikoliv doménoví experti správce.
 - **DŮSLEDEK:** Správce ISVS je v přístupu k datům absolutně závislý na existujících uživatelských funkcích a libovůli provozovatele/dodavatele. Pokud potřebuje přistoupit k datům v jiné podobě, než v jaké jsou nabízeny aplikačními funkcemi, provozovatel/dodavatel si účtuje náklady, které jsou zbytečně vysoké kvůli špatně navržené architektuře systému. To je pak komplikací i pro potenciální uživatele dat, protože správce ISVS není z důvodů špatně nastavených možností přístupu k primárním datům schopen data uživatelům zpřístupnit. Má k dispozici pouze přístup prostřednictvím uživatelských funkcí, které ale uživatelům nabídnout nemůže. I kdyby mohl, nebyly by pro uživatele použitelné, protože se jedná o uživatelské funkce nutné pro plnění zákonných povinností, nikoliv funkce pro další zpracování dat.
 - **DŮSLEDEK:** Protože je podoba získaných dat určena vnitřní databázovou reprezentací a nikoliv legislativní a doménovou terminologií, správce často datům získaným ze systému bez kontextu dodaném uživatelskými funkcemi (a grafickým uživatelským rozhraním) daného ISVS nerozumí. To je pak komplikací i pro potenciální uživatele dat, protože jim správce není schopen data řádně popsat a vysvětlit.
- **PRAXE nejednotný způsob zpřístupňování dat jejich potenciálním uživatelům:** Způsob zpřístupnění dat pro účely jejich sdílení není sjednocen. Není spojen s konkrétní odpovědností a nejsou určeny jasné povinnosti spojené s nutností zajištění, údržby a rozvoje takového způsobu zpřístupnění a s jeho popisem a zveřejněním takového popisu.
 - **DŮSLEDEK:** V organizační struktuře správce ISVS obvykle neexistuje jasné daný útvar s personálními kapacitami a rozpočtem potřebným pro správnou správu dat a jejich sdílení. Datům a jejich zpřístupňování se tak nikdo systematicky nevěnuje a neexistuje v organizační struktuře správce jednotné místo s trvalou a komplexní znalostí o datech a způsobech jejich sdílení.



- **DŮSLEDEK:** Potenciální uživatelé dat nevědí, na koho se mají obrátit v případě, že potřebují zajistit přístup k datům. Nemají jistotu, že ten, s kým komunikují, má potřebné informace, znalosti, schopnosti a kompetence.
- **PRAXE netransparentní způsob zpřístupňování dat jejich potenciálním uživatelům:** Způsoby zpřístupnění nejsou systematicky klasifikovány podle dostupnosti různým skupinám potenciálních uživatelů dat, kterými mohou být ostatní orgány veřejné správy ale i subjekty mimo veřejnou správu (fyzické a právnické osoby), přístup k datům není řešen systematicky, transparentně a není zajištěn na základě jednotných zákonných povinností.
 - **DŮSLEDEK:** Správce neví, jakými způsoby jaká data sdílí a zda je sdílí. Celistvá znalost napříč celou veřejnou správou chybí zcela.
 - **DŮSLEDEK:** Potenciální uživatelé dat nemohou zjistit, zda a jakým způsobem jsou data dostupná a pro jaké skupiny uživatelů jsou data dostupná za splnění jakých podmínek.
 - **DŮSLEDEK:** V případě ad hoc rozhodnutí o zpřístupnění dat správcem danému uživateli na základě splnění ad hoc podmínek nemají ostatní potenciální uživatelé jistotu, že přístup získají také, byť podmínky splňují stejně.
- **PRAXE dobrovolnost zajištění možnosti zpřístupňování dat jejich potenciálním uživatelům:** Zajištění zpřístupnění většiny dat uchovávaných v ISVS není povinností. Výjimku tvoří data, reprezentující údaje, které jsou ze zákona veřejné, případně které jsou poskytnuté na základě žádosti dle zákona č. 106/1999 Sb. U dat, která nejsou povinně zveřejňována, povinnost zajištění zpřístupňování neexistuje a zpřístupňování tak probíhá netransparentně a pouze na základě ad hoc rozhodnutí.
 - **DŮSLEDEK:** Jelikož správce nemá danu povinnost, většinou data ani nezpřístupňuje. Pokud zpřístupňuje, tak ad-hoc a netransparentně.
 - **DŮSLEDEK:** Přístup uživatele k údajům je velice komplikovaný a v praxi často nevede k žádoucímu výsledku.

Popsaná špatná praxe ukazuje, že dosavadní právní úprava není dostatečná k dosažení cílů efektivního a hospodárního eGovernmentu. Správci ISVS v kontextu správy dat nepostupují s péčí řádného hospodáře. **Je nezbytné přijmout právní úpravu, která by přímo adresovala správu dat veřejné správy.** Zvláštní úprava musí vyřešit výše popsanou špatnou praxi a tím zamezit výše popsaným negativním důsledkům. Pro přehlednost ještě jednotlivé příklady špatné praxe shrňme:

- neexistující popis dat
- nemožnost přístupu k primárním datům jejich správcem
- nejednotný způsob zpřístupňování dat jejich potenciálním uživatelům
- netransparentní způsob zpřístupňování dat jejich potenciálním uživatelům
- dobrovolnost zajištění možnosti zpřístupňování dat jejich potenciálním uživatelům



2.2 Řízený přístup k datům veřejného sektoru a jejich opětovné užití

2.2.1 Popis problematiky

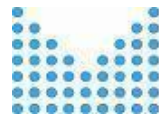
Řízený přístup k datům je vedle otevřených dat, veřejného datového fondu a propojeného datového fondu čtvrtým, doposud obecně právně neupraveným, způsobem předávání dat veřejné správy. Poskytování informací (dat) veřejnou správou v podobě otevřených dat, je obecně upraveno v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím. Veřejný a propojený datový fond je pak zakotven v zákoně č. 111/2009 Sb. a upravuje způsoby předávání dat mezi agendovými místy za účelem výkonu jejich agend. Řízený přístup k datům upravuje datové toky počínající u orgánů veřejné správy a směřující k veřejnosti. Dle současné právní úpravy je obecně možné sdílení dat uchovávaných v ISVS a dalších registrech za jiným účelem, než pro které byly vytvořeny a pro které jsou v ISVS nebo dalších registrech uchovávány, pouze u dat veřejných podle zákona č. 106/1999 Sb. I data, která však nemohou být poskytnuta podle zákona 106/1999 Sb. mají hodnotu spočívající v možnosti jejich sdílení a dalšího užití pro další účely, jako je například vědecký výzkum, datová žurnalistika nebo efektivní výkon veřejné správy.

Základním principem řízeného přístupu k datům je umožnění přístupu k datům, u kterých je regulováno nakládání s nimi, tedy která jsou ze své povahy chráněná zákonem (např. protože jde o osobní údaje, jsou předmětem obchodního tajemství, představují obsah chráněný právy duševního vlastnictví třetích stran atd.). Cílem řízeného přístupu k datům je umožnit přístup k nim nebo jejich odvozeninám a jejich opětovné užití za vybranými zákonem předvídanými účely, které jsou v obecném slova smyslu ve veřejném zájmu, a zároveň zajištění, aby nedošlo k nepřiměřenému zásahu do chráněných práv. Příkladem řízeného přístupu může být zajištění statistických dat z dané datové sady, umožnění přístupu pouze přes zabezpečené počítačové rozhraní nebo jen ve fyzických prostorách správce dat, případně vytvoření právních záruk, které ochranu před zneužitím poskytnutých dat zajišťují. Praktické dopady řízeného přístupu se projevují zejména v oblastech vědeckého výzkumu, vývoje a inovací, získávání statistiky o různých oblastech lidské činnosti pro účely rozšiřování znalostí a výkon svobody projevu v širším slova smyslu, vzdělávání a vhodného nastavování veřejných politik. Klíčovou součástí řízeného přístupu je rovněž možnost získat data od většího množství orgánů veřejné správy najednou a díky tomu pracovat s komplexnějším a celistvějším obrazem.

Řízený přístup k datům se vyskytuje v právní úpravě ve vybraných zahraničních jurisdikcích, jako jsou Spojené státy americké, ale i v právních řádech členských států EU. Příkladem může být Spolková republika Německo. V případě Německa neexistuje centrální orgán, který by řízený přístup k datům zajišťoval, a data pro vědecké účely jsou k dispozici prostřednictvím různých výzkumných datových center. Specifický příklad, který není však hodný následování, nabízí maďarská právní úprava v podobě zákona č. 101 z roku 2007, který umožňuje žádat o anonymizovaná data veřejné správy další orgány veřejné správy za účelem zajištění rozhodování a nastavování politik na základě datových podkladů. Jedná se o nevhodný příklad, protože předpokládá přístup jen ze strany orgánů veřejné správy, nikoli už veřejnosti. Dá se předpokládat, že i vzhledem k tomu v něm není řešená otázka proporcionality a možnost předání se presumuje, zřejmě i proto že stále probíhá v rámci státních institucí. I tento způsob volného předávání by však byl v kontextu českého práva problematický, protože české právo výrazně dbá na dělbu moci a zásadu zákonnosti a přiměřenosti).

Ukázkovým příkladem dobré praxe fungujícího řízeného přístupu v určité oblasti je pak specifická právní úprava ve Finsku, která umožňuje přístup a opětovné užití osobních údajů z oblasti zdravotnictví a sociálních služeb.

V ČR se principy řízeného přístupu k datům objevují v zákoně č. 89/1995 Sb., o státní statistické službě a v zákoně č. 272/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Zákon č. 89/1995 Sb. uvádí v § 17 odst. 1 písm. f) umožňuje předání důvěrných



statistických údajů na základě smlouvy za účelem vědeckého výzkumu.¹³ Dále zákon č. 89/1995 Sb. uvádí v § 18 odst. 1 písm. c), že Český statistický úřad může vypracovat a poskytnout statistické informace na základě smlouvy za cenu stanovenou dohodou. Zákon č. 272/2011 Sb. v § 73 upravuje omezené poskytování dat ze zdravotnických registrů za zákonem stanovených podmínek. Oba zákony neupravují řízený přístup k datům dostatečně. Druhý uvedený navíc vylučuje přístup široké veřejnosti, a to i pro obecně společensky prospěšné účely. Příkladem komplexní úpravy poskytování informací, která zahrnuje jak volný přístup formou veřejného datového fondu, tak prvky řízeného přístupu je úprava katastru nemovitostí podle zákona č. 256/2013 Sb., o katastru nemovitostí.

Problematikou úpravy, která odpovídá popisovanému konceptu řízeného přístupu k datům, se začala zabývat rovněž evropská legislativa v podobě návrhu nařízení o správě dat (dále "DGA", detailně dále v části 2.2.6).

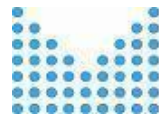
Vzhledem k uvedenému se jeví jako nezbytné připravit takovou obecnou právní úpravu, která komplexní řízený přístup k datům za jasně vymezenými účely umožní.

2.2.2 Vztah k zákonu 106/1999 Sb.

Obecným předpisem pro poskytování informací veřejného sektoru, a to včetně zajištění jejich opětovného užití, je zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Pojem "informace" je v zákoně vymezen v § 3 odst. 3 jako „*jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči*". Tato široká definice zahrnuje i data. Jádrem zákona leží v zajištění základního politického práva na informace ve smyslu čl. 17 odst. 5 Listiny základních práv a svobod. Zákon rovněž obsahuje implementaci PSI Směrnice (směrnice 2003/98/ES) a připravuje se jeho novela, která obsáhne implementaci směrnice o otevřených datech (směrnice EU č. 2019/1024). Jedná se tedy o klíčový předpis upravující opětovné užití informací (a dat) veřejného sektoru. Zákon povinným subjektům ukládá poskytovat informace žadatelům z řad široké veřejnosti, a to s výhradou takových informací, jejichž poskytnutí je zákonem vyloučeno. Zákon dále uděluje povinným subjektům diskreční oprávnění zveřejňovat jakékoli informace opět s výhradou výjimek uvedených v zákoně. Předpokladem pro poskytování informací podle zákona č. 106/1999 Sb. je tzv. princip publicity veřejné správy, dle kterého se informace zásadně poskytují. Žadatel také není nucen prokazovat právní důvod pro jejich poskytnutí, a naopak povinný subjekt musí prokázat v případě odmítnutí žádosti existenci relevantní výjimky, na základě které nejsou informace poskytnuty. Dalším principem zákona č. 106/1999 Sb. je princip neformálnosti. V základu nejsou kladeny žádné formální podmínky na žadatele, resp. na žádost o poskytnutí informace. Ideálním případem je taková situace, kdy žadatel a povinný subjekt spolu vstoupí do konverzace a v případě, že jsou žádány informace, které není možné poskytnout z důvodu existující výjimky, povinný subjekt nabídne žadateli alternativu. To se však děje spíše zřídka (více viz nálezy Ústavního soudu ze dne 1. 7. 2021 sp. zn. III. ÚS 3339/20).

Zákon č. 106/1999 Sb. neupravuje řízený přístup k datům. Základní parametry fungování tohoto předpisu nedávají povinným subjektům na výběr. Pokud informaci poskytnout mohou (tedy pokud neexistuje právní překážka, která by poskytnutí bránila), pak ji poskytnout musí, a to s minimem překážek v souladu s požadavky evropské legislativy (směrnice 2003/98/ES), která byla provedena v § 4a a § 4b zákona. Pokud je informace předmětem některé z výjimek uvedených v zákoně, tak ji povinný subjekt poskytnout nemůže ani přes případné dodatečné zajištění záruk ze strany žadatele. Určitou možnost k poskytnutí představuje anonymizace, kdy výkladová praxe zákona 106/1999 Sb. předpokládá možnost jejího provedení. Dochází

¹³ To se děje v souladu s evropskými předpisy, zejména s nařízením ES č. 223/2009 ze dne 11. března 2009 o evropské statistice.



tak k naplnění požadavku § 8a odst. 1 zákona, dle kterého se informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje poskytují jen v souladu s právními předpisy, upravujícími jejich ochranu (zejména s GDPR a zákonem č. 110/2019 Sb.). Dle výše zmíněného nálezu Ústavního soudu by povinné subjekty měly postupovat tak, aby poskytly požadovanou informaci v její nejširší možné podobě. To se týká rovněž využití procesu anonymizace. Na druhou stranu, praxe ukazuje, že obecně povinné subjekty k anonymizaci přistupují toliko mechanicky v podobě odstranění přímých identifikátorů (např. jméno, příjmení, bydliště, identifikační čísla atd.), ale kreativní anonymizace, která by umožnila bezpečně vytěžit bohatství daného datového zdroje, není ze strany povinných subjektů využívána s odkazem na to, že by šlo o vytváření nové informace dle § 2 odst. 4 zákona.

Obdobná situace vzhledem k umožnění řízeného přístupu k datům pak panuje i v případě zvláštních právních předpisů, které upravují přístup a následné užití specifických informací, např. zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon) a zákon č. 123/1998 Sb., o právu na informace o životním prostředí.

I nadále je vhodné, aby zákon č. 106/1999 Sb. zůstal základním předpisem pro naplňování základního politického práva na informace a obecným předpisem pro poskytování informací a široké zajištění jejich dalšího užití. **Z hlediska zajištění řízeného přístupu k datům však jeho současná podoba není dostatečná. Cílem navrhované právní úpravy není ani z části nahradit zákon č. 106/1999 Sb., ale zajistit řízený přístup k datům, kterou zákon č. 106/1999 Sb. neumožňuje.**

2.2.3 Dotčené subjekty

Aktuální právní úprava v podobě zákona č. 106/1999 Sb., ale i v podobě zvláštních předpisů, předpokládá, že informace poskytuje přímo subjekt, který je dožádán a zároveň je jejich věcným gestorem, resp. který je má v držení.¹⁴ Žadatel nemá možnost získat údaje od většího množství povinných subjektů zároveň, byť spolu věcně souvisí a musí každému subjektu zaslat samostatnou žádost.

Zákon č. 106/1999 Sb. vymezuje povinné subjekty v § 2 následovně:

„(1) Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti, jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.

(2) Povinnými subjekty jsou dále ty subjekty, kterým zákon svěřil rozhodování o právech, právech chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.”

Do působnosti zákona spadá velké množství institucí a orgánů veřejné správy, včetně všech krajů a obcí. Problematický je pak zejména neurčitý právní pojem “veřejná instituce”, jehož výklad se po nálezu Ústavního soudu ve věci ČEZ (sp. zn. IV. ÚS 1146/16) ustálil na takových osobách soukromého práva, které naplní test formulovaný v nálezu Ústavního soudu ve věci Letiště Praha (sp. zn. I. ÚS 260/06) a zároveň jsou 100% vlastněny státem nebo územními samosprávnými celky.

Pro řízený přístup k datům není takto široké vymezení povinných subjektů nezbytné, protože ve většině případů budou z hlediska řízeného přístupu relevantní data v registrech orgánů veřejné správy, případně vyšších územních samosprávných celků. Primárně jde o zajištění bezpečného předávání dat ze strany veřejného sektoru soukromým subjektům za účelem jejich opětovného využití, nikoli nutně jen pro zajištění transparentnosti nakládání s veřejnými

¹⁴ Viz též rozsudek Nejvyššího správního soudu č.j. 6 As 136/2014 – 41.



prostředky, jako je tomu v případě zajištění přístupu k informacím veřejných institucí. Druhým zásadním nedostatkem aktuální právní úpravy je nemožnost žádat o data pocházející od většího množství správců dat najednou, což dále navyšuje náklady žadatelů a fakticky omezuje přístup k datům. Často je navíc dosažení komplexního pohledu na zkoumanou problematiku za využití dat získaných od většího množství povinných subjektů nemožné, kvůli rozdílnému přístupu těchto subjektů k poskytovaným informacím a jejich absencí technické standardizaci.

2.2.4 Podmínky pro přístup a další užití dat

Jelikož je zákon 106/1999 Sb. ovládnut principem publicity veřejné správy, nemusí žadatel prokazovat právní zájem na poskytnutí informace a povinný subjekt informaci musí poskytnout, ledaže by mohl aplikovat jednu z výjimek, které obsahuje zákon 106/1999 Sb. (§ 8a a § 9-11) nebo zvláštní zákony, jako je tomu např. v případě § 73 odst. 7 zákona č. 372/2011 Sb., který uvádí, že „*Statistický ústav poskytne na základě žádosti podle zákona o svobodném přístupu k informacím, pokud se jedná o údaje v Národním zdravotnickém informačním systému, pouze informace o struktuře dat.*”

Z hlediska zajištění řízeného přístupu k datům jsou zásadní výjimky uvedené v zákoně č. 106/1999 Sb. § 9, § 11 odst. 2 písm. c)¹⁵ a zejména pak v § 8a, jehož odst. 1 zní:

“Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu.”

Povinné subjekty odmítnou poskytnout jakoukoli datovou sadu obsahující osobní údaje, pokud není její poskytnutí povinné ze zákona, případně pokud nepřeváží zájmy práva na informace a svobody projevu žadatele a širší veřejnosti nad zájmy ochrany soukromí a osobních údajů dotčených fyzických osob. Pro příklad je možné uvést aplikaci nálezu Ústavního soudu ze dne 17. 10. 2017, sp. zn. IV.ÚS 1378/16 (tzv. Platový nálezh), který je detailně uveden ve zprávě RIA.

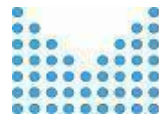
2.2.5 Záruky zákonnosti a zajištění ochrany kolidujících zájmů

Zákon č. 106/1999 Sb. neobsahuje úpravu, která by umožnila vytváření podmínek a záruk pro řízený přístup k datům a jejich následné užití bezpečným způsobem, který by respektoval a nenarušoval kolidující práva a zájmy. S ohledem na zásadu legální licence, co není zákonem zakázáno je povoleno, a principu veřejné správy je aktuální podoba právní úpravy v zásadě duální - informace se buď žadateli poskytne, nebo neposkytne. To však neodpovídá požadavkům na řízený přístup k datům. Ten v základu předpokládá aktivní komunikaci mezi žadatelem a poskytovatelem, jejímž výsledkem je takový způsob poskytnutí dat a v takovém rozsahu, který zároveň naplní potřeby žadatele a zároveň bude zajišťovat vysokou úroveň ochrany kolidujících práv a zájmů.

2.2.6 Propojování různých datových zdrojů

Zákon 106/1999 Sb. je konstruován tak, že povinný subjekt poskytuje pouze takové informace, které již existují a které má ve své dispozici, ať už právní (tj. má povinnost takové informace mít) nebo faktické. Zákon však v současné době neumožňuje poskytovat najednou informace, které jsou v dispozici většího množství povinných subjektů. Žadatel tak musí požádat o informace různé povinné subjekty, což je z hlediska dalšího užití dat a informací časově náročné bez záruky, že všechny povinné subjekty poskytnou informace v požadované a srovnatelné kvalitě. Ve svém důsledku to znemožňuje následnou efektivní práci s těmito daty

¹⁵ Ten zní “Povinný subjekt informaci neposkytne, pokud by tím byla porušena ochrana práv třetích osob k předmětu práva autorského nebo práv souvisejících s právem autorským.”



a informacemi ze strany žadatele zejména pro vědecké a výzkumné účely. Celý problém se pak dále umocňuje tím, že některé informace jsou v podřízeny obecnému předpisu zákona č. 106/1999 Sb., ale celá řada informací je z působnosti tohoto zákona vyňata, příkladem jsou informace spadající do režimu zákona č. 123/1998 Sb.

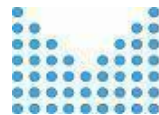
Vedle právní možnosti zajištění řízeného přístupu k datům musí být zajištěna rovněž možnost faktická, která umožní propojování různých souvisejících datových zdrojů (přičemž souvislost nemusí být na první pohled zřejmá a může vycházet z požadavků probíhajícího výzkumu). To současná právní úprava neumožňuje.

2.2.7 Předběžné požadavky vyplývající z návrhu nařízení o správě dat

V listopadu 2020 představila Evropská komise návrh nařízení o správě dat (Data Governance Act, DGA), které navazuje na předchozí datové legislativní iniciativy, jako je např. GDPR (nařízení EU 2016/679), nebo Směrnice o otevřených datech (č. 2019/1024). DGA se věcně zaměřuje na data, která podléhají různým režimům ochrany (zejména ochrana osobních údajů) nebo na data v držení soukromého sektoru. Cílem navrhovaného nařízení je stanovit obecný základ a umožnit vytvoření bezpečného prostředí pro efektivní předávání dat mezi veřejnou správou a soukromým sektorem a v rámci soukromého sektoru. Kapitola II navrhovaného nařízení přímo navazuje na Směrnici o otevřených datech, a upravuje podmínky pro opětovné užití informací veřejného sektoru, které jsou z aplikace Směrnice o otevřených datech vyloučeny z důvodů obchodního tajemství, statistické důvěrnosti, ochrany práv duševního vlastnictví třetích stran a ochrany osobních údajů. Z hlediska rozsahu aplikace se jedná o oblast, které se dotýká navrhovaná úprava řízeného přístupu k datům. Kapitola II DGA nezakládá jakoukoli povinnost poskytování dat, pouze stanoví minimální standard pro případy, kdy je poskytování předmětných dat a jejich opětovné užití umožněno národním právem.

Z aktuální ale dosud neschválené podoby návrhu vyplývají následující okruhy úpravy, které by měly být brány v potaz z hlediska harmonizace a adaptace DGA do právního řádu ČR brány v rámci předkládaného návrhu zákona o správě dat.

- 1) Při poskytování a opětovném užití dat je nezbytné zajistit, aby se tak dělo v souladu s právními předpisy, které zajišťují jejich ochranu. Jedná se zejména o oblast ochrany osobních údajů (zejm. GDPR) a další předpisy zajišťující ochranu informačních práv.
- 2) Poskytovatel dat má zakázáno uzavírat exkluzivní dohody s příjemcem dat, které by znemožnily poskytnutí dat dalším žadatelům.
- 3) Poskytovatel dat může stanovovat podmínky pro poskytování dat tak, aby zajistil, že nedojde k jejich zneužití. Podmínky opakovaného použití musí být nediskriminační, přiměřené a objektivně odůvodněné s ohledem na kategorie dat, účely opakovaného použití a na povahu dat, pro které je opakované použití povoleno. Tyto podmínky nesmějí být použity k omezení hospodářské soutěže. Základní zárukou, která má zajistit zabezpečení předávaných údajů a to, že nedojde k jejich zneužití, je trojstupňový systém:
 - i) poskytnutí agregovaných nebo anonymizovaných údajů, přičemž proces anonymizace probíhá ve spolupráci s žadatelem tak, aby bylo dosaženo výsledků, které potřebuje a zároveň byla chráněna kolidující práva a zájmy.
 - ii) poskytnutí dat prostřednictvím vzdáleného zabezpečeného připojení (např. VPN).
 - iii) poskytnutí dat případně jejich agregovaných nebo anonymizovaných výsledků na místě, přímo v prostorách poskytovatele dat tak, aby bylo minimalizováno riziko úniku.



- 4) Poskytovatel může po příjemci dat požadovat právní záruky, jako je doložka mlčenlivosti, nebo uložení povinnosti neztotožňovat zpětně konkrétní subjekty údajů, aby limitoval možnost zneužití poskytnutých dat ze strany příjemce dat.
- 5) Za poskytnutí dat může poskytovatel požadovat poplatky, které by však v případě opětovného užití za vědeckými účely nebo zpracování dat prováděného SMEs měly být minimální.
- 6) Členské státy mají stanovit seznam institucí, které budou sloužit jako podpora poskytovatelů dat. Tyto instituce mohou být sektorově definované a podpora může být jak technického, tak právního charakteru.
- 7) Členské státy mají stanovit jednotné informační místo, na které se mohou zájemci obracet s žádostmi o poskytnutí dat, a které tyto žádosti pomůže zprostředkovat, včetně např. vyřízení žádostí směřovaných k většímu množství poskytovatelů dat.

3 Návrh věcného řešení – Část I: Správa dat

3.1 Cíl úpravy

Cílem chystané úpravy je zajistit, aby se data uchovávaná v registrech, evidencích, seznamech nebo rejstřících veřejné správy (evidenční systémy) stala samostatným artefaktem s vlastním životním cyklem a s hodnotou využitelnou i mimo zdrojový evidenční systém potenciálními uživateli dat včetně uživatelů z řad veřejnosti a to nezávisle na uživatelských funkcích evidenčního systému, ve kterém jsou spravována. Správa dat včetně zajišťování přístupu k datům se stane samostatnou manažerskou úlohou oddělenou od řízení samotného evidenčního systému.

Navrhujeme vytvoření nového právního předpisu. Přidání dalších ustanovení zákona č. 365/2000 Sb. není vhodné vzhledem k zachování systematické přehlednosti stávajícího předpisu a také proto, že navrhovaná úprava věcně přesahuje aplikaci tohoto zákona. Zaměřuje se na data a řízený přístup k nim, na rozdíl od existujícího předpisu, který reguluje informační systémy veřejné správy a povinnosti s nimi spojené.

3.2 Dotčené subjekty

Navrhovaná právní úprava se dotýká primárně správců evidenčních systémů, kteří budou mít nové povinnosti vyplývající z požadavků na efektivní a hospodárnou správu dat. Níže jsou uvedeny varianty zvažovaných povinných subjektů, které jsou podrobně popsány ve zprávě RIA.

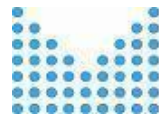
V rámci této části je nutné vzhledem k jednotnosti navrhovaného věcného záměru brát v potaz rovněž roli povinných subjektů v kontextu Části II, tedy zajištění řízeného přístupu k datům.

Dotčené subjekty: Varianta 1

Povinnými subjekty dle této varianty by byly ústřední orgány veřejné správy ve smyslu kompetenčního zákona (zákon č. 2/1969 Sb.).

Výhodou je, že jde o jasně a úzce definovanou množinu povinných subjektů, které navíc obecně disponují potenciálem pro snadné získání nezbytných znalostí a kompetencí pro efektivní výkon nových povinností.

Nevýhodou je, že její dopad je velice úzký a nevyhovuje záměru předkládaného materiálu.



Dotčené subjekty: Varianta 2

Výhodou široký rozsah působnosti, kdy mezi dotčené subjekty budou patřit všechny orgány veřejné správy, samosprávy a jejich podřízené organizace, případně další subjekty vykonávající veřejnou správu.

Nevýhodou je, že by navrhované řešení bylo ekonomicky velice nákladné pro subjekty, které nepodléhají zákonu č. 365/2000 Sb.

Dotčené subjekty: Varianta 3

Povinnými subjekty byly správci ISVS, tak jak jsou definovány v zákoně č. 365/2000 Sb. Odkaz na pojem správce ISVS automaticky neznámá, že budou z aplikace nového předpisu vyloučeni ti správci ISVS, kteří jsou vyloučeni z aplikace zákona č. 365/2000 Sb. (viz § 1 odst. 2 až 5 zákona č. 365/2000 Sb.).

Tato varianta ovšem zároveň předpokládá systém výjimek z působnosti navrhovaného předpisu. Je třeba zdůraznit, že tento zákon nebude automaticky přejímat výjimky z povinných subjektů ze zákona 365/2000 Sb., ale bude nezbytné nastavit je speciálně pro navrhovaný právní předpis. Při stanovení výjimek je třeba zohlednit povahu dané instituce (např. systémy pro potřeby nakládání s utajovanými informacemi, informace zpravodajských služeb a další uvedené v § 1 odst. 2 zákona č. 365/2000 Sb.), nebo praktické a ekonomické důvody (malé obce). Přesné stanovení výjimek musí být předmětem široké debaty a shody.

Výhodou je, že se jedná o poměrně širokou skupinu definovaných subjektů, které mají již zákonem č. 365/2000 Sb. definované povinnosti ve vztahu k ISVS. Vzhledem k úzké věcné vazbě mezi správou dat a ISVS tak nové povinnosti vyplývající z tohoto zákona nebudou představovat nezbytnost zabývat se zcela novými oblastmi. Výjimky pak zaručí, že nové povinnosti nedopadnou na případy, ve kterých by to nebylo z výše uvedených důvodů vhodné.

Tento rozsah povinných subjektů je vhodný i vzhledem k základnímu vymezení povinnosti zajištění řízeného přístupu k datům, a to i vzhledem k tomu, že chystaný návrh předpokládá vznik jednotného datového úřadu, který bude povinným subjektům v plnění jejich povinností při zajišťování řízeného přístupu pomáhat (viz kapitola 4 tohoto dokumentu).

Nevýhodou je užší rozsah aplikace oproti variantě 2.

Tato varianta je vhodná, protože představuje vhodný kompromis požadavku na širokou aplikaci nových povinností a zároveň eliminuje případné nežádoucí dopady příliš široké aplikace, ať už věcné nebo administrativní.

Varianty 1 a 2 nejsou vhodné. Smyslem navrhovaného zákona je zajistit efektivní správu dat v případě co možná největšího počtu povinných subjektů při zohlednění efektivnosti a účelu připravované právní úpravy. Varianta 1 se vztahuje na příliš malý počet subjektů. Naopak varianta 2 definuje počet povinných subjektů příliš široce a kladla by na některé z nich neúměrné ekonomické zatížení.

Navrhujeme variantu 3 při stanovení výjimek z působnosti zákona na dotčené subjekty, která bude nejlépe plnit cíl a účel navrhované právní úpravy, zajistí ochranu kolidujících zájmů a nebude příliš zatěžovat povinné subjekty, neboť část infrastruktury k tomu nezbytné musí mít již jako správci ISVS mít vybudovanou.

3.3 Zavedení nových pojmů

V současné době je z hlediska řízení e-governmentu na legislativní úrovni základním pojmem ISVS. Účelem navrhované úpravy je vedle regulace ISVS na stejnou úroveň postavit i **regulaci dat uchovávaných v ISVS**, resp. obecně v registru, evidenci, seznamu nebo rejstříku (dále jen evidenční systém), a **pojem datového rozhraní**, jako prostředek zpřístupnění těchto dat. Druhým cílem je zavést povinnost sdílet data prostřednictvím datových rozhraní co možná nejširšímu okruhu uživatelů dat v rámci čtyř druhů datových toků ve veřejné správě, kterými jsou otevřená data, veřejný datový fond, propojený datový fond a řízený přístup k datům.

Datové rozhraní orgánu veřejné správy (dále OVS) zpřístupňuje data nebo jejich část z jednoho nebo více evidenčních systémů OVS. Příkladem datového rozhraní OVS je datová sada obsahující kopii části dat z evidenčního systému nebo aplikační programovací rozhraní umožňující čtení části dat z evidenčního systému.

Prostřednictvím datových rozhraní OVS sdílí data ze svých evidenčních systémů s oprávněnými uživateli. Datové rozhraní má dvě úrovně přístupnosti (veřejné a neveřejné datové rozhraní). Veřejná datová rozhraní musí být bez omezení dostupná veřejnosti jako otevřená data. V případě datových rozhraní zpřístupňujících data agendových údajů evidovaných v registru práv a povinností také prostřednictvím veřejného datového fondu za účelem sdílení mezi orgány veřejné správy. Neveřejná datová rozhraní naopak musí být před neomezeným veřejným přístupem chráněna. To ale neznamená, že nejsou přístupné nikomu. Naopak, cílem je zavést povinnost zajistit jejich maximální možnou dostupnost v rámci řízeného přístupu a propojeného datového fondu oprávněným uživatelům. V případě neveřejných datových rozhraní zpřístupňujících data agendových údajů evidovaných v registru práv a povinností již existuje povinnost jejich sdílení mezi OVS prostřednictvím propojeného datového fondu. Sdílení neveřejných datových zdrojů s veřejností pak spadá do řízeného přístupu.

Následující tabulka shrnuje, jaká data jsou s kým sdílěna:

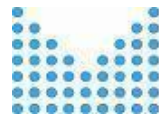
	Sdílení dat s veřejností	Sdílení dat agendových údajů mezi OVS
Veřejná data	Otevřená data (106/1999 Sb.)	Veřejný datový fond (111/2009 Sb.)
Neveřejná data	Řízený přístup	Propojený datový fond (111/2009 Sb.)

Tabulka 1: 4 druhy datových toků ve veřejné správě

Právní úprava řízeného přístupu v Českém právním řádu chybí.

Datové rozhraní může zpřístupňovat **primární data** nebo **odvozená data**. Zpřístupnění primárních dat z datové rozhraní znamená, že data z evidenčního systému jsou zpřístupněna způsobem nesnižujícím jejich informační hodnotu. Zpřístupnění odvozených dat z datového rozhraní znamená, že data z evidenčního systému jsou poskytnuta v upravené podobě, která jejich informační hodnotu nutně snižuje výměnou za zajištění ochrany kolidujících zájmů. Může se jednat např. o agregaci dat, náhodný výběr z dat, nahrazení hodnot v datech, vytvoření mapové vrstvy.

Správce datových rozhraní orgánu veřejné správy je útvar OVS nebo externí dodavatel zodpovědný za datová rozhraní zpřístupňující data z evidenčních systémů OVS. Odpovědnost za datové rozhraní zahrnuje odpovědnost za přesnost zpřístupnění obsahu datovým



rozhraním. Dále zahrnuje odpovědnost za popis datového rozhraní a odpovědnost za sdílení datového rozhraní s oprávněnými uživateli. Sdílení datového rozhraní zahrnuje nejen sdílení obsahu ale i jeho popisu.

Správce datových rozhraní provádí **datový přezkum**. Výsledkem provedení datového přezkumu je popis

1. informací reprezentovaných daty v evidenčních systémech OVS, které jsou pro OVS důležité, v podobě informačního modelu OVS, a jejich popis;
2. datových rozhraní jako způsobů sdílení dat z bodu 1. v podobě katalogu datových rozhraní OVS.

Informační model OVS je popisem struktury a významu (sémantiky) informací reprezentovaných daty v evidenčních systémech OVS. Informace je vždy údajem o nějakém subjektu nebo objektu práva nebo je údajem odvozeným z jiných údajů. Informační model OVS popisuje relevantní typy subjektů a objektů práva, relevantní typy údajů a relevantní souvislosti mezi nimi. Informační model OVS je celistvým popisem informací důležitých pro OVS.

Katalog datových rozhraní OVS popisuje datová rozhraní OVS jako způsoby zpřístupnění dat z evidenčních systémů OVS pro účely jejich sdílení s relevantními uživateli. Pro datové rozhraní je popsáno, z jakých evidenčních systémů jsou čerpána data a v jaké podobě jsou data datovým rozhraním poskytována. Popis podoby dat zahrnuje vymezení odpovídající části informačního modelu, popis transformací dat ze zdrojových evidenčních systémů provedených před zpřístupněním dat datovým rozhraním a také specifikace technické podoby poskytnutí dat (datové formáty, struktury, atd.). Důležitou složkou popisu datového rozhraní je také specifikace úrovně jeho přístupnosti (veřejné a neveřejné datové rozhraní).

Správce datových rozhraní průběžně:

- upravuje vytvořený informační model OVS tak, aby reflektoval změny v legislativě, v agendách a jednotlivých evidenčních systémech;
- vyhodnocuje poptávku po datových rozhraních ze strany vlastních zaměstnanců, jiných OVS a veřejnosti, na základě kterých definuje a vytváří nová datová rozhraní OVS, příp. upravuje existující datová rozhraní OVS a změny reflektuje v katalogu datových rozhraní OVS.

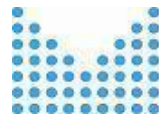
Katalogy datových rozhraní jsou veřejně dostupné s výjimkami, kdy by veřejnost katalogu způsobila konflikt s jiným chráněným veřejným zájmem nebo základním právem.

Národní katalog datových rozhraní OVS je jednotným místem, které zpřístupňuje popisy datových rozhraní v katalogů datových rozhraní OVS. Dále zprostředkovává zasílání žádostí o přístup k datovým rozhraním a žádostí o nová datová rozhraní relevantním OVS. Nově vznikne tzv. Národní katalog datových rozhraní OVS, který bude ISVS ve smyslu zákona č. 365/2000 Sb. Jeho správcem bude Ministerstvo vnitra.

3.4 Přehled nových povinností

Navrhovaná úprava zavede následující povinnosti jednotlivých povinných subjektů:

- vytvoření informačního modelu OVS na základě pravidel tvorby informačních modelů OVS vydaných Ministerstvem vnitra a jeho průběžná aktualizace,
- určování, vytváření a popisování datových rozhraní na základě stanovených povinností (viz dále), na základě vlastních potřeb a na základě poptávky oprávněných uživatelů



dat (jiné OVS, subjekty z řad veřejnosti), zajišťování jejich kvality a jejich sdílení oprávněným uživatelům,

- stanovení pravidel správy dat a datových rozhraní OVS v souladu s pravidly správy dat vydanými Ministerstvem vnitra a jejich dodržování,
- vedení katalogu datových rozhraní OVS

Dále navrhovaná úprava zavede následující povinnosti Ministerstva vnitra:

- vydání prováděcího předpisu, který stanoví pravidla tvorby informačních modelů OVS,
- vydání prováděcího předpisu, který stanoví pravidla správy dat a datových rozhraní pro OVS,
- správa ISVS Národní katalog datových rozhraní, který
 - zpřístupňuje záznamy v katalozích datových rozhraní jednotlivých OVS
 - umožňuje prohlédávání těchto záznamů
 - zprostředkovává zasílání žádostí o přístup k datovým rozhraním a žádostí o nová datová rozhraní relevantním OVS

3.5 Možné varianty

3.5.1 Evidenční systémy

Výše popsané povinnosti se týkají dat v evidenčních systémech. Je nutno definovat, co vše pod pojem evidenční systém spadá.

Evidenční systémy: Varianta 1

Povinnosti jsou zakotveny v rámci zákona 365/2000 Sb. To znamená, že jako evidenční systém chápeme pouze ISVS. Povinnosti se tak týkají pouze dat uchovávaných v ISVS a datových rozhraní zpřístupňující tato data.

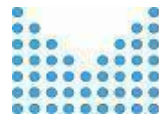
Evidenční systémy: Varianta 2

Povinnosti jsou zakotveny mimo kontext zákona č. 365/2000 Sb. Jedná se tedy o data spravovaná i v evidenčních systémech OVS, které nejsou ISVS, a také v ad hoc systémech pro sběr dat (např. tabulky vytvářené pracovníky OVS v tabulkových editorech pro různé ad hoc účely). Obecně řečeno se tedy povinnosti týkají všech registrů, evidencí, seznamů nebo rejstříků vytvářených a spravovaných OVS. Tato varianta je velice extenzivní a představovala by značné finanční i organizační náklady. Tato varianta se nejvíce jeví jako vhodná vzhledem k výrazné administrativní zátěži.

Vzhledem k očekávaným nákladům a přínosům byla vybrána varianta 1 u evidenčních systémů.

3.5.2 Podoba informačního modelu OVS

Informační model OVS, tedy popis datových struktur povinného subjektu, může mít různé úrovně detailu, které jsou různé nákladné a technicky náročné na provedení. Je nutno tuto úroveň detailu definovat tak, aby bylo dosaženo cíle navrhované právní úpravy a zároveň nebylo jeho provedení pro povinné subjekty nepřiměřeně náročné.



Informační model: Varianta 1

Informační model OVS není vůbec vytvářen. Neexistuje tak celistvý popis informací reprezentovaných daty uchovávaných v evidenčních systémech OVS. Existují pouze popisy datových rozhraní OVS, které poskytují pouze částečné popisy informací.

Informační model: Varianta 2

Informační model OVS je vytvářen v nestrukturované podobě textového popisného dokumentu doplněného o případné vizuální diagramy znázorňující důležité části modelu.

Informační model: Varianta 3

Informační model OVS je strukturovaným, ale primitivním popisem v podobě evidence typů subjektů a objektů práva a jejich údajů tak, jak je definováno v zákoně č. 111/2009 Sb. Tj. informační model OVS je vytvořen v podobě, která je již dnes evidována v registru práv a povinností jako základní informační model agend vykonávaných OVS.

Informační model: Varianta 4

Informační model OVS je vytvořen jako plnohodnotný konceptuální model v podobě [sémantického slovníku pojmů](#), tj. v podobě výčtu sémantických prvků odvozených ze sémantického slovníku veřejné správy doplněných o sémantické vazby mezi nimi. Je vyjádřen v otevřeném a strojově čitelném formátu, který umožňuje jeho libovolné následné zpracování, především jeho vizualizace, analýzy a propojování s informačními modely jiných OVS.

Varianty 1 a 2 nejsou vhodné, protože nikterak neřeší aktuální problémy, které má připravovaný právní předpis odstranit. Varianta 4 není vhodná vzhledem k relativně vysokým nárokům na know-how a schopnost provedení ze strany povinného subjektu.

Jako vhodná byla zvolena varianta 3 Informačního modelu, neboť protože dostatečně adresuje cíle navrhované právní úpravy a zároveň představuje vhodný kompromis mezi nákladností a přínosy.

3.5.3 Určování datových rozhraní

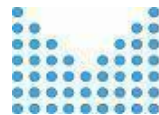
Správce datových rozhraní určuje a popisuje jednotlivá datová rozhraní OVS. Povinný subjekt je povinen udržovat seznam datových rozhraní OVS úplný a aktuální. Na základě poptávky určuje a popisuje nová datová rozhraní. Poptávka může vzniknout na základě vnitřních potřeb OVS, na základě potřeb jiných OVS i na základě potřeb veřejnosti. Jiné OVS a veřejnost poptávají nová datová rozhraní prostřednictvím národního katalogu datových rozhraní, případně prostřednictvím již existujících nástrojů datových toků, jako je propojený datový fond.

Datová rozhraní může u OVS poptat také ČSÚ na základě k němu podané poptávky týkající se zpřístupnění propojených dat od více OVS najednou. V tomto případě má navíc správce povinnost určit datová rozhraní v podobě požadované ČSÚ. Při definici poptávky ČSÚ specifikuje také požadovanou sémantickou a technickou podobu.

Pro každou množinu logicky souvisejících dat vedených v evidenčních systémech OVS může existovat i více datových rozhraní.

Při určování datových rozhraní je správce povinen nezávisle na poptávce pro každou sadu logicky souvisejících dat určit povinná datová rozhraní.

V základní podobě této povinnosti povinný subjekt určuje datová rozhraní a to: a) na základě zákonných povinností; b) na základě vlastní úvahy a c) na základě poptávky (formulované např. v předpisech 106/1999 Sb., 123/1998 Sb. nebo v chystaném návrhu zákona). Poptávka může přijít ze strany veřejnosti, nebo ze strany jiných OVS, případně ze strany plánovaného



jednotného datového úřadu (jakožto centrálního OVS propojujícího veřejnost a větší množství dalších OVS), který bude nadán oprávněním zajistit přístup k datovým rozhraním jiných povinných subjektů a zprostředkovat žadateli propojení většího množství dat různých původců.

Určování datových rozhraní je klíčovou součástí navrhované právní úpravy, která musí být v základní podobě přítomná. Nulová varianta je tak vyloučena.

3.5.4 Realizace a sdílení datových rozhraní

Pro datové rozhraní OVS zajišťuje soulad jeho skutečné technické podoby s popisem. Dále zajišťuje dostupnost datového rozhraní. Veřejné datové rozhraní musí být dostupné jako otevřená data, příp. prostřednictvím veřejného datového fondu. Neveřejné datové rozhraní je přístupné v rámci výkonu veřejné správy prostřednictvím propojeného datového fondu. Dále je neveřejné datové rozhraní přístupné veřejnosti řízeným přístupem za zákonem vymezenými účely, v určené technické podobě a za určených podmínek přístupnosti. Podmínky přístupnosti nesmí být diskriminační. Může se jednat o vzdálený přístup, ale je také možné, aby přístupnost byla podmíněna fyzickou návštěvou k tomu určeného pracoviště správce datového rozhraní.

Každý zájemce o zpřístupnění datového rozhraní má právo získat data prostřednictvím datového rozhraní za podmínek užití tohoto datového rozhraní, pokud splní určené podmínky přístupnosti. Nutnou podmínkou je naplnění zákonem vymezeného účelu. Zájemce musí splnit i další podmínky, pokud byly OVS určeny.

Detaily zajištění řízeného, tedy neveřejného, přístupu k datovému rozhraní jsou popsány v kapitole 4 tohoto materiálu.

3.5.5 Katalogizace datových rozhraní

Katalog datových rozhraní OVS je naplněn metadaty o datových rozhraních OVS ve strukturované podobě. Výsledný katalog je pak místem, kde jsou datová rozhraní OVS v jednotné strukturované podobě popsány, což umožňuje vyhledávání existujících datových rozhraní. Na druhou stranu s sebou vedení katalogu nese náklady. Je tak nutno určit, kterých datových rozhraní se katalogizace má týkat.

Povinnost katalogizovat veřejná datová rozhraní vyplývá již ze zákona č. 106/1999 Sb., kde je zavedena povinnost katalogizace v národním katalogu otevřených dat.

Katalogizace datových rozhraní: Varianta 1

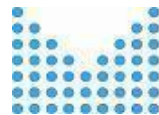
Povinnosti katalogizace datových rozhraní je dána pouze zákonem č. 106/1999 Sb. Neveřejná datová rozhraní sdílené prostřednictvím řízeného přístupu tak nejsou vůbec katalogizována. Jsou vytvářeny pouze ad hoc bez popisu a jednotné evidence. OVS tak nemá přehled o tom, jaké datové rozhraní OVS existují a jak jsou s kým sdíleny. V kontextu tohoto materiálu jde tak o nulovou a proto nedostatečnou variantu.

Katalogizace datových rozhraní: Varianta 2

Správce datových rozhraní popisuje a katalogizuje datová rozhraní aktivně zveřejňovaných dat v rozsahu, který vyplývá z povinností určení datových rozhraní (viz část 3.5.3 tohoto materiálu). Nově by tak byla popisována a katalogizována datová rozhraní využívaná v situacích, kdy dochází k předávání dat mezi OVS za účelem výkonu jejich agend prostřednictvím propojeného datového fondu a kdy dochází k povinnému poskytování informací veřejnosti podle zvláštních předpisů a zároveň nejde o otevřená.

Katalogizace datových rozhraní: Varianta 3

Nad rámec předchozích variant povinný subjekt popisuje a katalogizuje neveřejná datová rozhraní sdílená prostřednictvím řízeného přístupu, u kterých existuje širší poptávka než jen



jednorázová ad hoc poptávka od jednoho subjektu. Jedná se o taková datová rozhraní, která poptává více žadatelů nebo která jsou sice poptávána jenom jedním žadatelem, ale ten vyžaduje opakovaný přístup k aktualizovanému datovému rozhraní. Datová rozhraní poptávaná ad hoc (tj. jedním žadatelem pro jednorázový přístup) jsou popisovány a katalogizovány pouze z vlastní vůle správce datových rozhraní.

Katalogizace datových rozhraní: Varianta 4

Správce datových rozhraní popisuje a katalogizuje všechna neveřejná datová rozhraní, která musí určit povinně a všechna ta, která určil na základě poptávky.

Varianta 1 a 4 nejsou vzhledem ke svým nedostatkům vhodné. Varianta 1 nezahrnuje evidenci neveřejných datových rozhraní a varianta 4 by byla příliš nákladná. Varianta 3 by přinesla výrazné přínosy v podobě zajištění transparentnosti veřejné správy a snížení následných nákladů v případech opakovaných žádostí, nicméně představuje vyšší vstupní náklady na straně správce datového rozhraní. Je však třeba zvážit, zda by vstupní náklady nebyly příliš vysoké s ohledem na administrativní zátěž, kterou by katalogizace takových datových rozhraní představovala.

Doporučujeme zavedení varianty 2 pro katalogizace datových rozhraní, a to vzhledem k zajištění efektivního fungování navrhovaného předpisu. Tato varianta je vhodná, protože představuje velké přínosy za relativně nízkých nákladů.

3.5.6 Veřejnost katalogu datových rozhraní OVS

Katalog datových rozhraní OVS umožňuje získat přehled o tom, jaká datová rozhraní OVS nabízí potenciálním uživatelům k využití. V případě neveřejných datových rozhraní musí uživatelé splnit nediskriminační podmínky dané správcem datových rozhraní, aby mohli k datovému rozhraní přistoupit. Aby ale tuto funkci mohl katalog datových rozhraní plnit, musí být veřejně přístupný. Je však nutné rozhodnout, v jaké šíři mají být katalogizační záznamy veřejně dostupné, a to i v návaznosti na otázky zajištění ochrany osobních údajů a dalších právem chráněných zájmů.

Veřejnost katalogu datových rozhraní: Varianta 1

Katalog datových rozhraní je zcela veřejný s výhradou záznamů, jejichž zveřejnění by mohlo zasáhnout do kolidujících práv a právem chráněných zájmů, jako je např. ochrana osobních údajů, ochrana utajovaných informací atd.

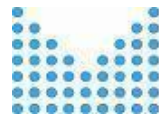
Veřejnost katalogu datových rozhraní: Varianta 2

Katalog datových rozhraní je zcela veřejný s výhradou záznamů, jejichž zveřejnění by mohlo zasáhnout do kolidujících práv a právem chráněných zájmů, jako je např. ochrana osobních údajů, ochrana utajovaných informací atd. a s výjimkou popisů datových rozhraní poptávaných ad hoc (tj. jedním subjektem pro jednorázový přístup). Popisy datových rozhraní poptávaných ad hoc je možné na základě diskrece povinného subjektu a případně po dohodě s poptávajícím subjektem zveřejnit s časovým odkladem od doby zpřístupnění datového rozhraní subjektu.

Veřejnost katalogu datových rozhraní: Varianta 3

Katalog datových rozhraní je zcela neveřejný.

Varianty 1 a 3 nejsou vhodné, protože u varianty 1 hrozí nepřiměřená byrokratická zátěž z jednorázových přístupů na základě žádosti a u varianty 3 nebude katalog splňovat požadavky na transparentnost a efektivitu fungování navrhovaného systému.



Doporučujeme proto variantu 2, která je dostatečně flexibilní na naplnění požadavku na transparentnost katalogu a zároveň nebude docházet k nepřiměřené byrokratické zátěži povinných subjektů. Možnost ad hoc datových rozhraní v katalogu bude zachována.

3.6 Úprava agend OVS

Vznikne nová agenda ohlášená Ministerstvem vnitra a vykonávaná všemi povinnými subjekty "tvorba, sdílení a evidence datových rozhraní". V rámci agendy má MV ČR koordinační a metodickou roli a spravuje ISVS národní katalog datových rozhraní. Povinné subjekty pak mají všechny výše uvedené povinnosti správců datových rozhraní.

Vznikne nová agenda ohlášená Ministerstvem vnitra a vykonávaná všemi povinnými subjekty "tvorba, sdílení a evidence informačních modelů". V rámci agendy má MV ČR koordinační a metodickou roli. Vykonávající OVS pak mají všechny výše uvedené povinnosti týkající se tvorby konceptuálních modelů OVS.

3.7 Úprava ISVS

3.7.1 Národní katalog datových rozhraní

Vznikne nový veřejný ISVS národní katalog datových rozhraní, jehož správcem bude Ministerstvo vnitra. Národní katalog datových rozhraní bude obsahovat katalogizační záznamy ze všech katalogů datových rozhraní OVS. Národní katalog datových rozhraní je AIS pro agendu "evidence datových rozhraní".

Národní katalog datových rozhraní bude možné vytvořit na bázi existujícího ISVS národní katalog otevřených dat. Vzhledem k tomu jsou očekávané náklady nízké.

3.7.2 Registr informačních modelů

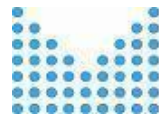
Vedle zajištění přístupu k popisu datových rozhraní je vhodné také zpřístupnit informační modely jednotlivých OVS. V současné době chybí registr informačních modelů a povinné subjekty nemají povinnost zveřejnit svůj informační model. To není žádoucí situace, protože by vedl ke stavu, kdy by každý povinný subjekt zveřejňoval svůj informační model OVS na svých webových stránkách. To by pak vedlo k roztržitésti a netransparentnosti v této oblasti.

Aby se uvedenému předešlo, je pro zajištění efektivní evidence nezbytné, aby vznikl "registr informačních modelů OVS". Půjde o ISVS zajišťující evidenci a správu informačních modelů jednotlivých OVS a jejich integraci do celistvého informačního modelu VS ČR. V tomto registru budou dále evidovány vazby prvků informačních modelů na datová rozhraní evidované v národním katalogu datových rozhraní. Dále tento registr umožní komukoliv informační modely prohledávat a získávat tak přehled o tom, jaké informace jsou ve veřejné správě uchovávány a jak spolu tyto informace souvisí a to i napříč jednotlivými OVS, agendami a věcnými doménami. Registr informačních modelů OVS bude poskytovat vazby na datová rozhraní evidované v národním registru datových rozhraní, prostřednictvím kterých jsou informace v podobě reprezentace daty dostupné.

3.8 Shrnutí variant

Pro přehlednost uvádíme na konci této části stručné přehledové shrnutí vybraných variant z předchozích podkapitol. Z variant upravujících různé aspekty správy dat, jak jsou navrženy v Části I věcného záměru zákona, byly vybrány následující:

- „Dotčené subjekty: Varianta 3 - Správci ISVS": Jako povinné subjekty budou stanoveni správci ISVS a zároveň z nich budou stanoveny patřičné výjimky



- „Evidenční systémy: Varianta 1“: Navrhovaná právní úprava dopadá pouze na data obsažená v ISVS.
- „Informační model: Varianta 3“: Informační model OVS je vytvořen v podobě, která je již dnes evidována v registru práv a povinností jako základní informační model agend vykonávaných OVS.
- Povinné subjekty budou určovat datová rozhraní pro sdílení jejich dat, a to: a) na základě zákonných povinností; b) na základě vlastní úvahy a c) na základě poptávky jiných OVS nebo veřejnosti.
- Povinné subjekty budou zajišťovat datové toky skrze určená datová rozhraní.
- „Katalogizace datových rozhraní: Varianta 2“: Povinný subjekt popisuje a katalogizuje datová rozhraní aktivně zveřejňovaných dat v rozsahu, který vyplývá z povinností určení datových rozhraní
- "Veřejnost katalogu datových rozhraní: Varianta 2": Katalog datových rozhraní je zcela veřejný s výhradou záznamů, jejichž zveřejnění by mohlo zasáhnout do kolidujících práv a právem chráněných zájmů
- V návaznosti na výše uvedené budou registru práv a povinností evidovány nově vniklé agendy "tvorba, sdílení a evidence datových rozhraní" a tvorba, sdílení a evidence informačních modelů"
- Budou zřízeny ISVS "Národní katalog datových rozhraní" a "Registr informačních modelů"

4 Návrh věcného řešení – Část II: Řízený přístup k datům

4.1 Cíl úpravy - obecné principy a myšlenky části

Cílem navrhované úpravy je zajistit bezpečné sdílení a opětovné využití informací (dat), které jsou vyloučeny z poskytování informací podle současné právní úpravy reprezentované zejména zákonem č. 106/1999 Sb. Sdílení má proběhnout tak, aby informační potenciál předmětných dat byl naplněn z co největší míry a zároveň byla maximálně šetřena kolidující práva a zájmy, které jsou chráněné specifickými ochrannými právními režimy. Efektivní umožnění řízeného přístupu je podmíněno existencí efektivní správy dat ze strany daného OVS, včetně provádění datových přezkumů a taktéž zavést možnost podávat žádosti o řízený přístup k datům skrze instituci, která bude fungovat jako centrální informační bod (jednotný datový úřad) a bude moci rozhodovat o zřízení přístupu k datům. Tento požadavek rovněž nepřímo vyplývá z návrhu nařízení o správě dat.

Právní úprava musí být nastavena tak, aby efektivně dopadala na co nejširší spektrum dat a informací, ale zároveň zajistila, že nedojde k jejímu zneužití, ať už proto, že by byl poskytnut přístup k datům, který by i v tomto kontextu byl nepřiměřený, nebo proto, že by nebyly přítomné dostatečně účinné záruky, které by zneužití získat dat zabránily. Z toho důvodu plánovaná právní úprava spočívá na následujících pilířích:

Právní úprava dopadá obecně na všechna data, k nimž je v současné době omezen přístup.

- o Jde tedy o data, která nemohou být poskytnuta v souladu se současnými právními zejména předpisy 106/1999 Sb. a 123/1998 Sb. nebo dalšími zvláštními předpisy.
- o Z dat, na které nová právní úprava dopadá i tak budou existovat výjimky v podobě dat, které se nemohou poskytovat ani prostřednictvím řízeného přístupu. Výjimka může být absolutní (např. data z databází zpravodajských služeb), nebo ad hoc posuzovaná vzhledem k dožadovanému řízenému přístupu (např. i přes zapojení všech technických, organizačních a právních opatření by poskytnutí řízeného přístupu v požadované podobě znamenalo nepřiměřený zásah do práva na ochranu osobních údajů).



Žadatel o řízený přístup k datům má povinnost prokázat právní důvod pro umožnění přístupu.

- Právním důvodem může být charakter účelu, za kterým je o informace žádáno (např. vědecký výzkum, statistika, management znalostí, výukové účely atd.) nebo charakter žadatele (např. vědecká instituce), případně kombinace obojího.

Pokud žadatel prokáže právní důvod pro řízený přístup, mají dožádané povinné subjekty obecně povinnost žádostem o řízený přístup vyhovět.

- Pokud i přes pokus o vzájemnou dohodu na tom, v jaké podobě a jakým způsobem řízený přístup umožnit dožádaný povinný subjekt trvá na tom, že řízený přístup není možný, musí prokázat možnost aplikace zákonné výjimky z řízeného přístupu. Výjimky je nezbytné interpretovat úzce.

Žadatel o řízený přístup a povinný subjekt spolu aktivně komunikují a hledají způsob, jak požadovaná data zpřístupnit tak, aby byla maximálně vytěžena jejich informační hodnota a zároveň byla zajištěna ochrana kolidujících práv a zájmů.

- Jde zejména o vhodné použití anonymizačních technik a další datové transformace, nastavení způsobu předání dat (online zabezpečenou VPN, fyzicky na místě atd.) a o vytvoření právních záruk prostřednictvím smlouvy o řízeném přístupu k datům.

Existuje jednotné informační místo, jednotný datový úřad, který má znalost a kompetence provádět:

- Podporu povinným subjektům, které data zpřístupňují v případech, že jsou data žádána od jednotlivých povinných subjektů
- Sdružování povinných subjektů v případě, že žádost směřuje k většímu množství z nich, případně uložení povinnosti data poskytnout a zajištění propojování jejich datových rozhraní
- V odůvodněných případech sám může rozhodnout o zpřístupnění dat řízeným přístupem a vytvoření nového datového rozhraní, kterým budou požadovaná data různých původců zpřístupněna

Rozhodnutí o nepovolení řízeného přístupu jsou přezkoumatelná.

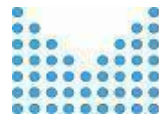
- Rozhodnutí by měla být přezkoumatelná nejprve v režimu správního řízení, případně soudně.

4.2 Vztah k dosavadním předpisům upravujícím přístup k informacím

Je zásadní jednoznačně vymezit vztah navrhované úpravy vůči existujícím právním režimům poskytování informací, zejména pak vůči obecnému předpisu v podobě zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Navrhujeme vytvoření nového předpisu s návazností na zákon č. 365/2000 Sb. a další aktuální legislativu. Vložení nových ustanovení do zákona 365/2000 Sb. není vhodné vzhledem k zásadnosti změny a zachování systematické přehlednosti předpisu.

Navrhovaný předpis je z hlediska zajišťování přístupu k vybraným informačním a datovým rozhraním chybějícím kouskem skládačky v roztříštěné právní úpravě dat veřejného sektoru. Není jeho cílem jakkoli změnit aplikaci stávajících právních předpisů v této oblasti.



Navrhovaný právní předpis bude obecným předpisem, podle kterého je možné žádat o řízený přístup k informacím, které jsou jinak podle jiných právních předpisů nedostupné (které jsou neveřejné/ není k nim možné udělit přístup) a podle kterého se bude postupovat v případě, že předmětem žádosti bude propojení dat různých původců.

Na základě žádosti o řízený přístup k datům bude možné získat přístup k existujícím informacím (datům), které jsou vyloučené z poskytování podle zákona č. 106/1999 Sb., podle zákona č. 123/1998 Sb. a dalších předpisů, které nějakým způsobem regulují a omezují přístup k určitým informacím. Mezi takové předpisy spadá v současné době rovněž zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování a zákon č. 256/2013 Sb., o katastru nemovitostí. Dále bude na základě žádosti o řízený přístup k datům možné získat společný přístup k datům různých původců.

Přednost před navrhovanou právní úpravou budou jako *lex specialis* mít takové předpisy, které komplexně upravují obecný řízený přístup k určitým specifickým informacím. To bude třeba posuzovat materiálně, tj. zda věcně je splněna podmínka možnosti žádosti o řízený přístup ze strany širší veřejnosti a zda jsou přítomné mechanismy pro určení konkrétních pravidel řízeného přístupu (např. podmínění poskytnutí dat uzavřením smlouvy, regulace způsobu předání dat atd.). Dá se očekávat, že mohou existovat zvláštní právní úpravy, které budou obsahovat specifická pravidla vytvořená vzhledem k podstatě a povaze konkrétních dat.

4.3 Dotčené subjekty – obecná povinnost umožnit řízený přístup k datům

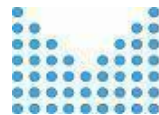
Z hlediska povinnosti poskytovat data řízeným přístupem je možné uvažovat o celé řadě subjektů veřejného sektoru, na které by mohla dopadnout. Tato část navrhovaného zákona ideově navazuje na část první v tom, že předpokládá, že pro zajištění řízeného přístupu k datům je prvně nezbytné provedené datových přezkumů, které povinným subjektům umožní znát, jaká data mají vlastně k dispozici. I vzhledem k tomu jsou následující varianty povinných subjektů formulovány ve vztahu k části 3.2 výše. Krom těch, které daty fakticky disponují, je třeba dále zahrnout podpůrné instituce, které zajistí, že bude aplikace nových právních norem účinná a efektivní.

Na základě analýzy dotčených subjektů provedených k navrhované části zákona se správě dat, se jeví jako ideální varianta povinných subjektů správci ISVS s výjimkami, takových, u kterých nebude poskytování řízeného přístupu vhodné nebo účelné ať už z důvodu toho, že disponují primárně informacemi, které je třeba zachovat neveřejné i v kontextu řízeného přístupu (např. zpravodajské služby), nebo proto, že by pro ně tato nová povinnost byla nepřiměřeně zatěžující (malé obce). Je třeba dodat, že výjimky z povinnosti zajistit řízený přístup k datům se mohou lišit (typicky být početnější a širší), než výjimky z povinností souvisejících se správou dat, jak byla pojednána v kapitole 3 tohoto dokumentu.

Kapitola 3.2 tohoto návrhu věcného záměru identifikovala jako vhodný základní rozsah povinných subjektů pro návrh „Dotčené subjekty: Varianta 3 - Správci ISVS“. To platí i v kontextu Části II.

Pro úplnost je nezbytné uvést, že variantně byla zvažována analogická úprava k zákonu č. 106/1999 Sb., protože se regulace týká poskytování informací veřejného sektoru. Podle této odmítnuté varianty by povinnými subjekty nových povinností byly povinné subjekty dle zákona č. 106/1999 Sb. Kladem této varianty je, že by nedocházelo k vytváření nového informačního režimu. Jako hlavními nevýhody byly identifikovány:

- Přílišná šíře aplikace. Není záměrem, aby povinnost dopadala na všechny veřejné instituce a malé obce a to z důvodů ekonomických i funkčních.



- Předpokladem efektivního naplnění nové povinnosti jsou existující datové přezkumy vytvářené podle první části navrhovaného předpisu. Uložit povinnost vytvářet datové přezkumy všem povinným subjektům dle zákona č. 106/1999 Sb. by byla ekonomicky a funkčně nepřiměřená (viz shrnutí v k variantě „Dotčené subjekty: Varianta 2 - Všechny orgány veřejné správy, samosprávy a instituce vykonávající veřejnou správu“).

4.4 Dotčené subjekty, kterým ze zákona vzniknou další povinnosti

Krom základních povinností vyplývajících pro povinné subjekty je pro zajištění efektivního fungování navrhované právní úpravy nezbytné založit specifické pravomoci vybraným orgánům veřejné správy. V následujícím úseku jsou již zahrnuty požadavky obecně vyplývající z nařízení o správě dat.

Správci existujících informačních infrastruktur

Ti plní roli informačního místa v určité věcné oblasti. Jde například o ČÚZK jako správce Geoportálu, nebo ŘSD jako správce NDIC. Tyto subjekty jsou v souladu s čl. 7 DGA očekávány jako věcně příslušné subjekty, které mohou plnit nápomocnou a poradní roli pro další povinné subjekty z jejich oblasti.

Český statistický úřad.

Rolí ČSÚ by mělo být jednotné informační místo ve smyslu čl. 8 DGA. Jako takové bude přijímat žádosti o zajištění řízeného přístupu k informacím, které pak bude dál předávat věcně příslušným správcům ISVS. Rolí ČSÚ bude rovněž zajištění propojování dat. V případě, že se bude žádost týkat většího množství správců ISVS najednou, může ČSÚ žádost po domluvě s nimi vyřídit sám a poskytnutí řízeného přístupu nařídit. Aby toto mohlo fungovat, bude nezbytné zajistit ČSÚ adekvátní pravomoci a technické zabezpečení.

Úřad pro ochranu osobních údajů

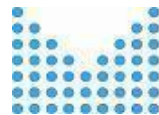
Vzhledem k tomu, že se ÚOOÚ postupně profiluje jako komplexní nezávislý informační úřad, je vhodné, aby plnil roli odvolacího místa při rozhodování o umožnění nebo neumožnění řízeného přístupu k datům. Určení ÚOOÚ jako obecného odvolacího místa v rámci tohoto řízení je účelné zejména z toho důvodu, že se dá očekávat, že na rozdíl od žádostí podle zákona č. 106/1999 Sb. bude většina relevantních žádostí o řízený přístup odborně složitější a je proto třeba specializované instituce, která dokáže tuto složitost posoudit. Zároveň je možné předpokládat, že žádostí o řízený přístup bude vzhledem k nezbytnosti prokázat právní zájem na získání řízeného přístupu řádově méně, než žádostí podle zákona č. 106/1999 Sb.

Další zákonem dané povinné subjekty

Ti, kteří disponují potenciálně zajímavými daty, ale leží mimo vymezení správců ISVS. V takovém případě by bylo vhodné řešení zahrnout jejich povinnost umožnit řízený přístup do zvláštních předpisů, které regulují jejich činnost. Zde se nabízí rovněž eventualita zajistit ve výjimečných odůvodněných případech možnost předávání dat B2G. Jako příklad se nabízí nemocnice pro zajištění přístupu k medicínským datům.

Odborná komise

Návrh předpokládá možnost vytvoření odborné komise tvořené autoritami z oblasti vědy a výzkumu (např. jako součást RVVI), která bude sloužit jako poradní orgán při umožňování řízeného přístupu a bude tak působit jako odborný garant, který dokáže posoudit oprávněnost požadavku. Cílem této úpravy je zajistit odborný dohled, který přispěje k zamezení zneužití dat.



4.5 Podmínky pro řízený přístup a další užití dat

Podmínkami pro řízený přístup a další užití dat jsou myšleny podmínky, které musí být splněny na straně žadatele, aby byl vůbec oprávněn data prostřednictvím řízeného přístupu obdržet a aby je mohl dále užívat. Jde o prokázání právního zájmu na obdržení dat řízeným přístupem, který je první úroveň ochrany, aby nedocházelo ke zneužití získaných dat. V tom se liší řízený přístup k datům od obecného práva na informace dle zákona č. 106/1999 Sb. Při určování oprávnění obdržet řízený přístup k datům je možné uvažovat o dvou variantách vymezení oprávnění a případně jejich kombinacích. První variantou je taxativní vymezení právního zájmu prostřednictvím předvídaných účelů, za kterými je možné o získání dat řízeným přístupem žádat. Druhou variantou je taxativní vymezení subjektů, které o řízený přístup žádat mohou.

Z první varianty je zřejmé, že úplné uvolnění účelů dalšího užití těchto dat je nežádoucí z hlediska ochrany osobních údajů, soukromí a dalších chráněných zájmů. Nabízí se nechat se inspirovat zahraniční právní úpravou, která již řízený přístup úspěšně obsahuje. Inspiraci je možné najít ve Finku, kde zákon o opakovaném užití zdravotnických a sociálních dat¹⁶ vymezuje následující účely, za kterými je možné data z uvedených databází dále zpracovávat:

- *scientific research*
- *statistics*
- *development and innovation activities*
- *steering and supervision of authorities*
- *planning and reporting duties by authorities*
- *teaching*
- *knowledge management*

V kontextu české právní úpravy se pak adekvátní nabízí následující účely dalšího užití:

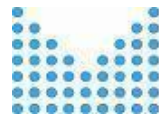
Efektivní výkon veřejné správy

- Přístup ke statistikám a možnost vytvářet detailní analýzy za využití dat jiných orgánů veřejné správy může vést k významnému zefektivnění výkonu veřejné správy.
- Žadatelem bude instituce vykonávající veřejnou správu, případně externí subjekt, který provádí smluvní výzkum nebo evaluaci pro orgány veřejné správy.
- Zavedení této možnosti přístupu k datům jiných institucí je účelné z toho důvodu, že prostřednictvím propojeného datového fondu má daný orgán veřejné správy přístup jen k údajům, které nezbytně potřebuje pro výkon svých agend. Tímto způsobem však může získat přístup k širšímu kontextu na základě, kterého se může efektivněji rozhodovat, nastavovat politiky nebo na základě kterého je možné lépe provádět nezávislou kontrolu a dozor nad činnostmi OVS.
- Žadatel každopádně bude muset být vždy schopen vysvětlit, proč řízený přístup potřebuje, popsat a odůvodnit rozsah, v jakém ho potřebuje a popsat účely, za kterými bude další zpracování probíhat. V kontextu ochrany osobních údajů musí zpracování být v souladu s GDPR (podrobněji bude popsáno dále).

Výzkum, vývoj a inovace

- Tento účel dalšího užití dat získaných řízeným přístupem zahrnuje široce užití pro vědecké účely. Terminologie bude přebrána ze zákona č. 130/2002 Sb.
- Žadatel se bude při podání žádosti prokazovat záznamy o plánovaném nebo probíhajícím výzkumu, včetně popisu způsobu správy výzkumných dat (data management plan). Povinný subjekt nebude mít za úkol hodnotit kvalitu plánovaného nebo probíhajícího

¹⁶ Viz <https://stm.fi/en/secondary-use-of-health-and-social-data>.



výzkumu, ale pouze jeho důvěryhodnost např. na základě toho s jakou institucí je žadatel afiliováný, zda byl výzkum schválen etickou komisí instituce atd.

Získání statistických dat a jejich další užití

- Statistickými daty se rozumí agregované nebo jinak transformované údaje tak, aby šlo údaje anonymizované, nebo takřka anonymizované, že riziko jejich zneužití bude zcela zanedbatelné.
- Právním zájmem na přístupu a opětovném použití těchto dat je pak výkon práva na svobodu projevu v širokém slova smyslu. Typicky tak oprávněnými žadateli budou krom vědců novináři, datoví analytici a další zástupci široké odborné veřejnosti.
- Součástí žádosti by měla být jasně specifikovaná představa toho, jak by data měla být transformována (anonymizována), nebo spíše, jaké informace mají být s pomocí těch dat získány. Není možné očekávat, že žadatel bude mít přesnou znalost o tom, jak data dožádaného subjektu vypadají a jak je efektivně upravit tak, aby šlo o prostá statistická data. Tato neznalost tak nemůže jít žadateli k tíži.
- V kontextu tohoto účelu hrozí možný překryv s právní úpravou zákona č. 89/1995 Sb., o státní statistické službě a zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
 - V případě prvně jmenovaného rozdíl spočívá v tom, že se řízený přístup věcně týká i oblastí, které leží mimo aplikace zákona č. 89/1995 Sb.
 - V případě druhého jmenovaného je situace složitější. Pokud budou údaje zcela anonymizované, dopadají rovněž zpět do působnosti zákona č. 106/1999 Sb. Zároveň je teoreticky *de iure* možné žádat o anonymizované údaje prostřednictvím zákona č. 106/1999 Sb. Na druhou stranu praxe ukazuje, že tento proces reálně příliš nefunguje. Vzhledem k tomu je vhodné zahrnout efektivní přístup ke statistickým datům do navrhované právní úpravy.

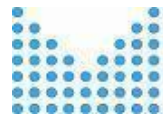
Výukové účely

- Využití dat ve výuce, typicky na středoškolské nebo vysokoškolské úrovni.
- Součástí žádosti bude popis kurikula plánované výuky včetně detailního popisu, jak bude s daty v rámci výuky nakládáno.

Druhá varianta vymezení rámce pro právní nárok by předpokládala vytvoření taxativního výčtu subjektů, které mohou o řízený přístup žádat. Tento přístup je však nevhodný, protože by již nepřiměřeně omezoval rozsah aplikace navrhované úpravy. Podstata žadatele však bude jistě následně hrát roli v samotném rozhodování povinného subjektu, zda řízený přístup umožní a jakým způsobem nastaví korektně záruky řízeného přístupu tak, aby kolidující práva a zájmy byly dostatečně ochráněny (viz dále).

4.6 Záruky zákonnosti a zajištění ochrany kolidujících zájmů

Navrhovaná právní úprava musí obsahovat takové záruky, že bude minimalizováno riziko zneužití dat jejich příjemci. Zneužitím se v tomto kontextu myslí v širokém slova smyslu jakékoli zpřístupnění a opětovné užití předmětných dat, které by bylo v rozporu s právem chráněnými zájmy (např. ochrana osobních údajů, obchodního tajemství, duševního vlastnictví atd.). První úroveň ochrany je nezbytnost prokázání právního zájmu, jak je uvedeno v bodě 4.4 výše. Avšak ani v těchto privilegovaných případech není možné jednoznačně stanovit, že žadatel má vždy oprávnění přistupovat ke všem neveřejným datům. Vzhledem k tomu je nezbytné zavést další úroveň jejich ochrany, které zajistí možnost řízeného přístupu k datům a zároveň budou chránit kolidující práva a zájmy. První z těchto úrovní představují výjimky, na které právní úprava řízeného přístupu nebude vůbec dopadat. Druhá pak upravuje způsob, jakým se řízený přístup zajišťuje a další technické a právní záruky, které jsou na příjemce dat kladeny.



4.6.1 Výjimky z poskytování

Je vhodné, aby z povinnosti umožnit řízený přístup existovaly výjimky pro případy, kdy by i řízeným přístupem došlo k nepřiměřenému zásahu nebo ohrožení kolidujících práv a zájmů. Tyto výjimky je možné identifikovat obecně buď jako absolutní (výjimky z aplikace předpisu), nebo relativní (neposkytnutí informace v kontextu konkrétního případu po vykonání testu proporcionality a zvážení možností limitujících možná rizika). V obou případech však musí důkazní břemeno prokázání existence a aplikovatelnosti výjimky na případ dané žádosti spočívat na dožadáném subjektu. To je nezbytné pro zajištění efektivního fungování právní úpravy žádostí o řízený přístup k datům.

A) Absolutní výjimky z povinnosti umožnit řízený přístup

Jde o takové případy, kdy je umožnění řízeného přístupu vzhledem k charakteru dat zcela vyloučeno pro od začátku nepřekonatelný zásah do kolidujících práv a zájmů. Jde například o vybrané oblasti dle ustanovení § 11 zákona č. 106/1999 Sb., tedy o data vztahující se:

- k bezpečnosti státu,
- k ochraně, bezpečnosti osob, majetku a veřejného pořádku,
- k ochraně zájmů České republiky a jejích občanů v zahraničí,
- k trestnímu řízení,
- k rozhodovací činnosti soudů s výjimkou rozsudků,
- k plnění úkolů zpravodajských služeb a poskytnutí této informace by ohrozilo plnění jejich úkolů či ochranu utajovaných informací
- k situaci, kdy povinný subjekt neposkytne informaci o činnosti orgánů činných v trestním řízení nebo bezpečnostních sborů, která se týká předcházení, vyhledávání, odhalování nebo stíhání trestné činnosti nebo ochrany bezpečnosti osob, majetku a veřejného pořádku, pokud by její poskytnutí ohrozilo práva třetích osob anebo schopnost orgánů veřejné moci předcházet trestné činnosti, vyhledávat nebo odhalovat trestnou činnost, stíhat trestné činy nebo zajišťovat veřejný pořádek a bezpečnost České republiky.

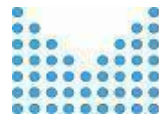
B) Relativní výjimky z povinnosti umožnit řízený přístup

V tomto případě jde potenciálně o všechna ostatní data, na které bude nový předpis dopadat. Základní zásadou je, že i data poskytovaná prostřednictvím řízeného přístupu musí být poskytována v souladu s právní úpravou, která je chrání. Rozdíl oproti zákonu o svobodném přístupu k informacím spočívá v tom, že poskytování dat prostřednictvím řízeného přístupu umožňuje vytvoření dostatečných přídatných záruk, že je taková zákonnost umožněna.

Povinný subjekt při umožňování řízeného přístupu bude zvažovat míru zásahu do chráněných kolidujících práv a zájmů, který může být řízeným přístupem způsoben. Základní metodologickým prostředkem pro vyhodnocení tohoto střetu nutně bude tradičně test proporcionality. Součástí tohoto testu bude muset povinný subjekt zároveň zvažovat způsob poskytnutí, který může riziko zneužití výrazně snížit (viz dále), stejně tak jako další možné technické a právní záruky, kterými se žadatel prokáže. Podobně jako v případě systému ochrany osobních údajů je vhodné, aby byla otázka řízeného přístupu upravena jako regulace postavená na hodnocení rizika. Čím nižší riziko, tím spíše je možné řízený přístup umožnit.

Dalšími zárukami, které při vyhodnocení možnosti poskytnutí bude muset povinný subjekt brát do úvahy, mohou být například:

- Smluvní ujednání s poskytovatelem dat zaručující povinnost mlčenlivosti, právní omezení dalšího užití dat, zakazující provádění zpětného ztotožnění atd.
 - Variantně mohou být ve formě prováděcího předpisu nabídnuty standardní smluvní doložky, které budou moci poskytovatelé dat využívat.



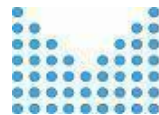
- V případě, že se bude jednat o osobní údaje nástroje předvídané GDPR jako je certifikace případně přihlášení se ke schválenému kodexu zpracování osobních údajů.
- I mimo rámec GDPR je možné uvažovat o systému certifikací / kodexů, které mohou fungovat jako prostředek zajištění souladu.
- Technické záruky mohou spočívat například ve způsobu zajištění ukládání dat, existence data management plánu a jeho realizace, nástroje zajištění kybernetické bezpečnosti atd.
- Roli při vyhodnocení bude hrát rovněž charakter žádajícího subjektu - např. pokud jde o výzkumnou instituci, data jsou žádána za účelem výzkumu a výzkumný plán byl schválen etickou komisí instituce, poskytovatel k tomu přihlédně.
- Existující sankční mechanismy, ať už v podobě smluvních sankcí, které budou součástí dohody o umožnění řízeného přístupu, anebo zákonných sankcí v podobě přestupků zakotvených v navrhovaném zákoně (případně obecné úpravě např. GDPR).

4.6.2 Způsoby řízeného přístupu

Konkrétní provedení toho, jak bude řízený přístup proveden, rovněž hraje zásadní roli v zajištění zabezpečení dat. I s odkazem na DGA je možné předvídat několik způsobů, jak data řízeným přístupem získat. Poskytovatel by pak měl na základě domluvy se žadatelem zvolit takový přístup, který zároveň naplňuje požadavky žadatele a zároveň odpovídá míře rizika, kterou data v kontextu dané konkrétní žádosti o řízený přístup představují, a tedy odpovídá požadavkům na zajištění zabezpečení. V základu je možné předvídat tři základní způsoby zajištění řízeného přístupu. Ty rovněž vycházejí z předpokladů stanovených v DGA. Všechny tři jsou pak aplikovatelné i v případě, kdy řízeným přístupem bude docházet k propojování dat různých původců.

- 1) Přístup ke statistickým a/nebo anonymizovaným (transformovaným) datům, které vznikly na základě požadavku žadatele. Vzhledem k tomu, že se jedná o anonymizovaná data, je jejich další užití regulováno primárně jen zásadou legální licence. Na druhou stranu, poskytovatel může jejich poskytnutí podmínit požadavkem na uzavření smlouvy, která například znemožní příjemci deanonimizaci dat. Předpokladem pro efektivní aplikaci tohoto způsobu je účelná komunikace mezi poskytovatelem a žadatelem. Přístup ke statistickým a/nebo anonymizovaným (transformovaným) údajům může být proveden např. online prostřednictvím elektronické pošty, nebo prostřednictvím speciálního aplikačního rozhraní.
- 2) Online přístup k neanonymizovaným datům. Zde je možné uvažovat o několika technických variantách, mezi kterými poskytovatel bude volit podle potřeby a povahy poskytovaných dat. Může jít například o zabezpečené připojení API, využití zabezpečené VPN nebo speciálního software v podobě klienta, kterým se žadatel připojí k databázi a získá k datům přístup. I způsob získání přístupu se může lišit podle potřeby. Žadatel může např. obdržet kopii databáze, ale v odůvodněných případech mu mohou být rovněž zobrazeny konkrétní údaje bez možnosti jejich snadného zkopírování.
- 3) Fyzický přístup v prostorách poskytovatele. Tato varianta počítá s přístupem, který bude k nejvíce citlivým datům, a riziko jejich zneužití nebo úniku je takové, že z bezpečnostního hlediska není možné jejich šíření online. Může jít například o přístup přes zabezpečenou konzoli v budově poskytovatele dat, kam žadatel může přijít a vytvořit si kopie dat, která potřebuje.

Až v případě, že žádný z předpokládaných způsobů přístupu není vzhledem k povaze požadovaných dat využitelný, protože nedokáže ani ve spojení s právními zárukami dostatečně odstranit riziko zneužití požadovaných dat, může povinný subjekt odmítnout umožnění řízeného přístupu.



4.7 Procesní otázky

Pro efektivní aplikaci řízeného přístupu bude nezbytné zvolit a zajistit efektivní proces, kterým se žádosti o řízený přístup budou vyřizovat. Je vhodné a žádoucí, aby byla rozhodnutí o umožnění nebo neumožnění řízeného přístupu přezkoumatelná a to jak v rámci vyšší instance samotného rozhodování, tak v rámci následného soudního přezkumu. Zároveň se jeví být nadbytečným vytváření samostatného procesního režimu, který by byl v pozici zvláštního předpisu. Obecně se tedy bude postupovat podle zákona č. 500/2004 Sb., správní řád, několika možnými odchylkami, jejichž účelem bude zajištění efektivnějšího výkonu nově upravených práv a povinností. Konečná rozhodnutí druhé instance pak budou standardně přezkoumatelná ve správním soudnictví. Jak bylo uvedeno výše, pokud povinný subjekt rozhodne, že není možné umožnit řízený přístup, musí ve svém odůvodnění jasně argumentovat, buď proč žadatel nedokázal prokázat, že hodlá údaje dále užívat za jedním ze zákonem předvídaných účelů, nebo musí povinný subjekt být schopný prokázat, že se na daný případ aplikuje jedna z výjimek nebo by bylo neproporcionální. Důkazní břemeno leží na povinném subjektu.

4.7.1 Proces řízeného přístupu včetně propojování dat

Proces řízeného přístupu: Varianta 1

Varianta 1 spočívá v tom, že subjekty povinné umožňovat řízený přístup jsou přímo správci konkrétních datových rozhraní (počítejme vzhledem k preferovaným variantám dotčených subjektů, že půjde o správce ISVS). Odvolacími orgány jsou pak orgány definované ve správním řádu, včetně rozkladů.

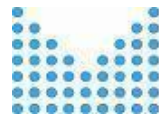
Proces řízeného přístupu: Varianta 2

Varianta 2 spočívá v tom, že subjekty povinné umožňovat řízený přístup jsou přímo správci konkrétních datových rozhraní (počítejme vzhledem k preferovaným variantám dotčených subjektů, že půjde o správce ISVS). Zároveň existuje jednotné místo, kde může žadatel o zajištění řízeného přístupu požádat (přičemž tento požadavek přímo vyplývá z DGA). V případě, že požadavek bude směřovat na větší množství datových rozhraní, bude mít jednotné místo pravomoc vydat rozhodnutí o umožnění řízeného přístupu k datům a poskytnutí dat od různých původců rovnou samo zajistí. Vhodným kandidátem na takové jednotné místo je ČSÚ. Nezbytnou podmínkou pro úspěšné nasazení jednotného datového úřadu s rozhodovací pravomocí je dostatečné udělení nových kompetencí ČSÚ, například v oblasti datové standardizace. Podvariantou by mohlo být rozložení nových pravomocí mezi ČSÚ a Ministerstvo vnitra.

Odvolacím orgánem by měl být pro oba zmíněné povinné subjekty (jak pro správce ISVS, tak pro jednotné místo) specializovaný datový úřad, a to z toho důvodu, že bude mít kapacitu, kompetence a znalost odvolání korektně posoudit. Jako zřejmá varianta se nabízí ÚOOÚ a to i vzhledem k tomu, že se v posledních letech vlivem pravomocí udělených zákonem č. 106/1999 Sb. profiluje jako jednotící informační úřad.

Proces řízeného přístupu: Varianta 3

Varianta 3 předpokládá vytvoření samostatného jednotného datového úřadu, nebo udělení nových pravomocí vybrané existující instituci, výhradně, prostřednictvím které se budou podávat žádosti o řízený přístup a tato instituce pak bude oprávněná uložit povinnost poskytnout řízený přístup koncovým věcným správcům ISVS, případně poskytnutí dat rovnou sama zajistí. Odvolacím orgánem by byl podobně jako ve variantě 2 odborný úřad, ideálně zřejmě ÚOOÚ. Výhody této varianty spočívají v centralizaci a usnadnění činnosti žadatelům. Hlavní výhodou této varianty je pak zajištění efektivního propojování různých datových rozhraní, což usnadní jejich následnou využitelnost zejména pro vědecké využití takových dat. Na druhou stranu určitou nevýhodou je logistická náročnost, protože jednotný úřad nebude



znát detaily databází a jejich obsahu, které jsou ve správě konkrétních správců ISVS. Tento problém je ale překonatelný dobrou správou datových rozhraní konkrétních správců ISVS, k čemuž směřuje první část tohoto návrhu. Druhým problémem pak je, že by takovému úřadu musely být svěřeny kompetence, které by mu umožnily přístup prakticky ke všem neveřejným datovým rozhraním, což může být v rozporu s principem minimalizace zásahu. Konkrétní nastavení pravomocí takového úřadu je tak nezbytně pečlivě vyvážit.

Proces řízeného přístupu: Varianta 4

Tato varianta je doplňkovou variantou, která je aplikovatelná současně s variantami 1-3. Spočívá ve vytvoření nezávislého poradního orgánu (např. pod RVVI), který bude pomáhat z odborného hlediska posuzovat žádosti o řízený přístup za vědeckými účely a sejme tak z povinných subjektů alespoň část tíhy spočívající v nezbytnosti mít dostatečné znalosti a kompetence, což v případě vysoce odborných žádostí může být problém. Přesné ukotvení takového poradního orgánu a míru jeho vlivu na proces o umožnění řízeného přístupu je nutné dále diskutovat.

Proces řízeného přístupu: Varianty 1 a 2 nejsou vhodné, protože Proces řízeného přístupu: Varianta 1 nezaručuje efektivní výkon při umožňování řízeného přístupu a jen obtížně by umožnila propojování dat. Proces řízeného přístupu: Varianta 2 vyžaduje, aby byly uvedené instituce dostatečně personálně a finančně zajištěny tak, aby svoji novou působnost dokázaly naplňovat, a to včetně korektního provádění anonymizačního procesu.

Vzhledem k ekonomickým a personálním požadavkům, včetně vysoké odbornosti a know-how zejména v procesech provádění anonymizace a zajištění zabezpečení předávání dat, je nejvhodnější Proces řízeného přístupu: varianta 3 ve spojení s doplňkovou Proces řízeného přístupu: Variantou 4. Plnění všech požadavků vyplývajících z funkčního a efektivního zajištění řízeného přístupu k datům není možné spravedlivě požadovat po všech správcích ISVS. Ostatně i DGA jednoznačně hovoří o vhodnosti jednotného informačního bodu, který bude s prováděním anonymizace pomáhat, případně ji bude sám vykonávat. Proces řízeného přístupu: Varianta 4 pomůže s efektivní aplikací navrhované právní úpravy.

4.7.2 Další procesní otázky

Lhůty

V souladu s DGA navrhujeme lhůtu pro umožnění řízeného přístupu 2 měsíce od podání žádosti, ve výjimečných případech prodloužitelná na 3 měsíce od podání žádosti. Je však třeba zdůraznit, že tato lhůta je určena k tomu, aby se povinný subjekt a žadatel aktivně domluvili na podobě, v jaké mají být data zpřístupněna, a na zárukách, které budou zavedeny, aby nedošlo ke zneužití zpřístupněných dat.

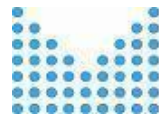
Poplatky

Povinný subjekt bude moci žádat o poplatek za umožnění řízeného přístupu ve výši, která odpovídá nákladům vynaloženým na umožnění řízeného přístupu.

Sankce

V případě, že bude aplikována jedna z variant, kde bude hrát zásadnější roli jednotný datový úřad, který bude moci nařídít umožnění řízeného přístupu, navrhujeme, aby připravovaná právní úprava obsahovala možnost uložit sankci za nesplnění této povinnosti.

Navrhovaný právní předpis bude rovněž obsahovat sankce v podobě přestupků, které by byly vymahatelné v případě, že žadatel použije data, k nimž dostal přístup v rozporu s pravidly řízeného přístupu. Doporučujeme zvážit rovněž o úpravu trestně právní roviny, ať už v podobě



nového trestného činu, nebo ideálně novely § 180 TZ (Neoprávněné nakládání s osobními údaji).

5 Návrh věcného záměru zákona

5.1 Účel a předmět zákonné úpravy

Cílem tohoto zákona je zajistit efektivní správu dat veřejného sektoru a umožnit řízený přístup k datům ze strany veřejnosti. Tyto základní cíle jsou obsaženy ve dvou základních částech navrhovaného zákona. První část se věnuje správě dat, druhá část se věnuje řízenému přístupu k datům.

Účelem první části je:

- zajistit, že data v ISVS dotčených povinných subjektů budou řádně popsána a dohledatelná
- zajistit, že budou řádně identifikována, popsána a katalogizována datová rozhraní, přes která probíhá předávání dat a že tato datová rozhraní budou dohledatelná

Účelem druhé části je:

- zajistit možnost řízeného přístupu k doposud neveřejným datům
- zajistit možnost propojení dat od většího množství jejich původců
- zajistit dostatečné zabezpečení řízeného přístupu, aby se limitovalo riziko zásahu do chráněných práv a zájmů

5.2 Vymezení pojmů

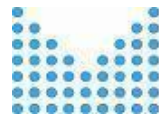
Pro účely tohoto zákona se rozumí:

- povinným subjektem správce informačního systému veřejné správy podle zvláštního zákona s odůvodněnými výjimkami;
- evidenčním systémem registr, evidence, seznam nebo rejstřík;
 - Pzn.: Evidenční systém bude obsahově odpovídat pojmu informační systém veřejné správy dle zvláštního zákona (č. 365/2000 Sb.). Pokud tento rozsah bude zachován i v rámci samotného návrhu zákona, ve finálním textu definice evidenčního systému nebude přítomná a bude využit přímo pojem informační systém veřejné správy.
- datovým rozhraním technické zajištění sdílení dat povinného subjektu jiným povinným subjektům nebo veřejnosti;
- informačním modelem popis struktury významu informací reprezentovaných daty v evidenčních systémech;
- datovým přezkumem analýza a evidence činností, které povinný subjekt s daty ve své správě provádí nebo má povinnost provádět

5.3 Správa dat

V odůvodněných případech budou zavedené výjimky z konkrétních povinností vyplývajících z této části zákona. Rozsah těchto výjimek je předmětem připomínkového řízení s tím, že nové povinnosti by primárně měly dopadat na maximálně velkou množinu povinných subjektů.

Povinný subjekt má z hlediska správy dat za povinnost:



- provádět datový přezkum
- vytvořit a udržovat aktuální informační model v souladu s pravidly tvorby informačních modelů vydanými Ministerstvem vnitra
- evidovat informační model v registru informačních modelů
- stanovit správce datových rozhraní, který bude zodpovědný za datová rozhraní zpřístupňující data z evidenčních systémů
- vytvořit a určit datová rozhraní a to jak na základě zákonných povinností, tak na základě poptávky uživatelů dat
- popsat a katalogizovat datová rozhraní
- stanovit pravidla správy dat a datových rozhraní v souladu s obecnými pravidly správy dat vydanými Ministerstvem vnitra
- garantovat přesnost zpřístupnění dat datovým rozhraním
- spravovat veřejný katalog datových rozhraní povinného subjektu

Ministerstvo vnitra má z hlediska správy dat za povinnost:

- spravovat Národní katalog datových rozhraní
- spravovat Registr informačních modelů
- kontroluje plnění povinností povinných subjektů a uděluje sankce
- prováděcím předpisem stanovit obecná pravidla správy dat
- prováděcím předpisem stanovit pravidla tvorby informačních modelů

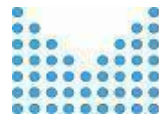
5.4 Řízený přístup k datům

Jednotný datový úřad má za povinnost:

- vyřizovat žádosti o řízený přístup k datům
- kooperovat s povinnými subjekty za účelem zajištění věcné relevance poskytovaných dat
- v případě žádosti o řízený přístup k datům, které jsou v gesci většího množství povinných subjektů, propojovat jejich datová rozhraní a případně vytvořit nové ad hoc datové rozhraní pro poskytnutí žádaných dat
- kooperovat s žadatelem o řízený přístup k datům, aby došlo k věcně maximálnímu možnému naplnění daného požadavku
- ve vhodných případech konzultovat žádosti o řízený přístup k datům s odborným poradním sborem zřízeným za tímto účelem
- ve vhodných případech provádět anonymizaci a pseudonymizaci poskytovaných dat
- ve vhodných případech umožnit přístup k datům prostřednictvím zabezpečeného vzdáleného přístupu
- ve vhodných případech umožnit přístup k datům v chráněném prostředí ve fyzických prostorách jednotného datového úřadu
- umožnit řízený přístup k datům na základě jednoznačných právně vymahatelných a nediskriminačních podmínek užití, které budou právně garantovat vysokou úroveň zabezpečení poskytnutých dat a budou tak předcházet riziku jejich zneužití
- udělovat sankce povinným subjektům v případě neuposlechnutí příkazu poskytnout požadovaná data

Povinné subjekty pro poskytování řízeného přístupu mají povinnost:

- spolupracovat s jednotným datovým úřadem při vyřizování žádostí o umožnění řízeného přístupu k datům
- poskytnout jednotnému datovému úřadu doménovou expertizu týkající se požadovaných dat



- ve spolupráci s jednotným datovým úřadem zajistit dostatečné zabezpečení řízeného přístupu k datům
- splnit příkaz poskytnout požadovaná data vydaný jednotným datovým úřadem

Vznikne odborný poradní sbor jako konzultační instituce při rozhodování o umožnění řízeného přístupu. Ideálně jako součást RVVI.

Povinnosti Úřadu pro ochranu osobních údajů:

- udělovat sankce za porušení podmínek užití dat poskytnutých řízeným přístupem
- působit jako odvolací instance pro přezkum rozhodnutí o neumožnění řízeného přístupu vydaných jednotným datovým úřadem

5.5 Přestupky

Za protiprávní jednání ve smyslu zákona by byla primárně považováno nesplnění povinností vyplývajících z požadavků na zajištění správy dat. Za protiprávní jednání bude rovněž považována nespolečenská OVS s jednotným datovým úřadem pro zajištění řízeného přístupu a neumožnění přístupu k datovému rozhraní a datům i přes pokyn jednotného datového úřadu, protože bez vymezení tohoto přestupku hrozí, že nebude možné zajistit efektivní výkon řízeného přístupu (tj. např. příliš dlouhé čekání na vyžádané informace a další praktická neužitečnost pro žadatele). Dále bude za protiprávní považováno takové jednání příjemce dat prostřednictvím řízeného přístupu, kterým by efektivně docházelo k narušení zabezpečení řízeného přístupu. Jde tak zejména o porušení povinnosti mlčenlivosti, porušení povinnosti neprovádět zpětné ztotožnění v případě anonymizovaných nebo pseudonymizovaných dat nebo jiné porušení dohody o řízeném přístupu uzavřené mezi poskytovatelem a příjemcem. Detailněji budou přestupky řešeny v následující fázi přípravy předpisu.

5.6 Změny souvisejících předpisů

Otázka nezbytných změn souvisejících předpisů bude detailně vyřešena v následující fázi přípravy předpisu. Předběžně je možné předpokládat, že může dojít k nezbytné novele zákona 365/2000 Sb., uvažovat je možné i o aktualizaci § 180 zákona č. 40/2009 Sb., trestní zákoník.

6 Promítnutí navrhovaného věcného záměru do právního řádu České republiky

Výsledkem věcného záměru je tvorba zákona vycházející z tezí věcného záměru, který bude mít dva cíle. Při dosažení prvního cíle by nový zákon měl zvýšit přehled orgánů veřejné správy o datech, která spravují a která využívají pro výkon svých agend. Data orgánů veřejné správy by měla přestat být pouze součástí spravovaných informačních systémů, ale měla by se stát sama předmětem zájmu jejich správců. Data by měla být cíleně spravována. Tím bude umožněna vyšší efektivita a ekonomičnost výkonu veřejné správy. Dále efektivní správa dat a vypracování datových přezkumů umožní lepší informovanost široké laické i odborné veřejnosti, která tak bude moci dále efektivněji vykonávat svá informační práva, ať již prostřednictvím existujících právních režimů, nebo prostřednictvím řízeného přístupu k datům, který přinese navrhovaný zákon.

Při dosažení druhého cíle by měl nový zákon umožnit efektivní přístup k datům a informacím veřejného sektoru, který doposud není možný ať už z důvodu jejich vyloučení z aplikace dosavadních právních úprav, nebo z důvodu nízké efektivity jejich aplikace. Řízený přístup k datům veřejného sektoru se bude týkat přístupu k datům, která jsou předmětem nějaké zákonné ochrany (např. proto že jde o osobní údaje, obchodní tajemství nebo práva duševního vlastnictví třetích osob), a to zejména pro účely vědeckého výzkumu, žurnalistiky a výkonu



práva na svobodu projevu v širším slova smyslu. Řízený přístup zároveň prostřednictvím technických a právních opatření zajistí, že riziko zneužití těchto dat bude minimální.

7 Soulad s ústavním pořádkem, s mezinárodními smlouvami, jimiž je Česká republika vázána, a se závazky vyplývajících pro Českou republiku z členství v Evropské unii

Navrhovaný zákon je v souladu s ústavním pořádkem, s mezinárodními smlouvami, jimiž je Česká republika vázána, a se závazky vyplývajících pro Českou republiku z členství v Evropské unii.

Navrhovaný zákon nikterak nezasahuje do oblastí, které jsou upraveny mezinárodními smlouvami, jimiž je Česká republika vázána. Možné režimy vyplývající z mezinárodních smluv, které omezují zveřejňování informací, budou v kontextu druhé části navrhovaného zákona respektovány. První část navrhovaného zákona pak cílí na ryze vnitrostátní veřejnoprávní úpravu principů řízení dat v informačních systémech. Stejný závěr pak platí pro hodnocení slučitelnosti navrhovaného zákona s Evropskou Úmluvou o ochraně lidských práv a základních svobody.

V kontextu práva EU je navrhovaný zákon komplementární k existující a rozvíjející se evropské datové legislativě tvořené zejména GDPR, a do budoucna nařízením o správě dat a případně dalšími. Navrhovaný zákon je s těmito předpisy v souladu a případně je věcně doplňuje, jako je tomu v kontextu chystaného nařízení o správě dat, k jehož harmonizaci může chystaný zákon sloužit.

Navrhovaný zákon je rovněž v souladu s ústavním pořádkem a požadavky, které z něj vyplývají.

8 Předpokládaný hospodářský a finanční dosah navrhované právní úpravy a další její dopady

Předpokládané hospodářské dopady budou spočívat zejména v nutných nákladech na:

- na provádění datových přezkumů. Půjde zejména o náklady vynaložené na přijetí nových, případně vyškolení stávajících pracovníků orgánů veřejné správy tak, aby odborně tuto činnost mohli zastat, případně náklady na zaplacení služeb externího dodavatele, který přezkumy provede,
- na určení, popis a katalogizaci datových rozhraní,
- na zajištění věcných personálních kapacit na vznik a správu národního katalogu datových rozhraní a registru informačních modelů, metodickou podporu a tvorbu pravidel pro správu dat,
- na zřízení infrastruktury, která umožní řízený přístup k datům a
- na vytvoření jednotného datového úřadu, ať už v podobě zřízení nové instituce (nedoporučováno), nebo rozšíření kompetencí některé ze stávajících institucí (např. ČSÚ nebo ÚOOÚ)

Z dlouhodobého náhledu je možné očekávat celkovou úsporu na provozu ISVS a dalších registrů provozovaných při výkonu veřejné správy, protože systematický přístup k datům a jejich uspořádání umožní efektivnější výkon veřejné správy.

Předpokládáme, že existence efektivního řízeného přístupu k datům přinese výhody spočívající v rozšiřování znalostí a aplikací v nových technologiích a postupech a umožní rozvoj vědeckého bádání.



9 Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Návrh nebude obsahovat úpravu, která by se mohla projevit v otázkách diskriminace a vztahu k rovnosti mužů a žen.

10 Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

První část návrhu, tedy právní úprava správy dat, nepřináší z hlediska ochrany soukromí a osobních údajů žádné negativní dopady. Návrh se zaměřuje na oblasti, které by povinné subjekty v pozici správců údajů už beztak měli naplňovat na základě povinností vyplývajících z GDPR a zákona č. 110/2019 Sb. Efektivní správa dat pak může jediné pomoci naplnit požadavky předpisů ochrany osobních údajů, ať už je to efektivnější zavedení zásad standardní a záměrně ochrany osobních údajů, povinnosti vést záznamy o zpracování a schopnosti naplňovat povinnosti vyplývající z práv subjektů údajů. V tomto směru může efektivní správa dat velice pomoci zejména naplnění práva na přístup. Určité riziko by teoreticky mohlo představovat katalogizování datových rozhraní (zejména v případě ad hoc datových rozhraní vzniklých na základě poptávky žadatele), nicméně i v tomto případě je dané riziko pro práva a zájmy subjektů údajů pouze na teoretické úrovni, protože katalogizační záznam bude obsahovat pouze metadata o datové sadě a nikoli zákonem chráněné údaje jako takové.

Druhá část návrhu regulace řízeného přístupu dopady na ochranu soukromí a osobních údajů mít bude, resp. může je mít, pokud bude provedena nevhodným způsobem. V současné době jsou osobní údaje z poskytování vyloučeny, pokud by takovým poskytnutím došlo k zásahu do práv a chráněných zájmů subjektů údajů. Navrhovaná úprava má zajistit možnost přístupu i k těmto datům, avšak pouze za předpokladu, že v každém konkrétním případě budou existovat dostatečné záruky proto, aby nedošlo k zásahu do práv a chráněných zájmů subjektů údajů. Zajištění vysoké úrovně ochrany osobních údajů je jedním ze základních pilířů navrhované právní úpravy. Dostatečné zabezpečení řízeného přístupu pak zajistí následující kombinace požadavků:

- nezbytnost prokázání právního zájmu na poskytnutí žádaných osobních údajů;
- technické a organizační prostředky ochrany;
 - o technická a organizační opatření aplikovaná u povinného subjektu;
 - o anonymizace a pseudonymizace poskytovaných údajů;
 - o přístup k datovému rozhraní přes zabezpečené online prostředí;
 - o přístup k datovému rozhraní v bezpečném fyzickém prostředí u poskytovatele dat;
- právní záruky v podobě jasné smluvní úpravy následného užití dat a jak smluvních, tak veřejnoprávních sankcí za jejich porušení;
- dohled ze strany ÚOOÚ.

Při vhodné aplikaci těchto záruk je možné dosáhnout rovnováhy, kdy zároveň bude možné za předvídanými účely poskytovat osobní údaje, jejichž poskytování je v současné době vyloučeno ustanovení § 8a zákona č. 106/1999 Sb., čímž dojde k možnosti jejich dalšího užití zejména za účely vědeckého výzkumu, a zároveň bude zachována vysoká úroveň jejich ochrany.



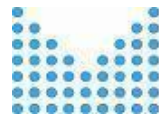
Plné legislativní zhodnocení dopadů regulace na ochranu soukromí a osobních údajů bude provedeno až v rámci přípravy textu zákona v návaznosti na konkrétní textaci.

11 Zhodnocení korupčních rizik

Návrh nevytváří korupční rizika. Návrh bude mít pozitivní vliv na antikorupční působení v ČR, protože akcentuje transparentnost v široké oblasti fungování veřejné správy.

12 Zhodnocení dopadů na bezpečnost nebo obranu státu

Při správném nastavení právního režimu regulované problematiky nemá návrh negativní vliv na bezpečnosti nebo obranu státu.



II. Odpovědi na dotazy povinných subjektů

1. Odpověď pro Národní knihovnu: Vyjádření k možnosti publikovat databáze Národní knihovny jako otevřená data (2019)

Národní knihovna České republiky (NKČR) spravuje databáze vzniklé z kooperativního projektu Národní autority České republiky. Tyto databáze obsahují jmenné (personální a korporativní) a věcné (tematické, geografické a formální) autority. Databáze vznikají kooperativně ve spolupráci s řadou dalších knihoven, které doplňují záznamy získané při provádění katalogizace a zároveň zpětně přebírají záznamy z Národních autorit do svých lokálních databází. Existuje zájem na tom, aby NKČR, aby plně zpřístupnila údaje z Národních autorit. V zápise ze setkání supervizorů projektu „Kooperativní tvorba a využívání souborů národních autorit“ v Národní technické knihovně ČR 28. 6. 2016 se uvádí, *“že báze autorit nebude považována za autorské dílo a nepodléhá tak Autorskému zákonu. Podléhá Zákonu na ochranu osobních údajů a také Zákonu o svobodném přístupu k informacím, protože databáze vzniká z veřejných finančních prostředků”*.

NKČR tvrdí, že není možné data poskytovat pod licencí CC0, protože dle jejího názoru představují hodnotu, se kterou je třeba zacházet s péčí řádného hospodáře. Kvůli tomu se dle názoru NKČR není možné práv k datům vzdát. Národní autority jsou důležitou součástí knihovních záznamů a logicky i zdrojem pro tvorbu entit v propojených knihovních záznamech. Nejasné právní postavení zmíněných dat prozatím blokuje možnost jejich zveřejnění v podobě (propojených) otevřených dat.

Druhým projektem, který je třeba posoudit, je projekt Souborného katalogu, který rovněž provozuje NKČR. Podobně jako v případě Národních autorit je databáze tvořena kooperativně ve spolupráci NKČR a dalších zapojených knihoven. Předávání dat je na rozdíl od Národních autorit však zasmluvněno tak, že zapojené knihovny mohou záznamy používat jen pro vlastní účely a právo na užívání záznamu je podmíněno trváním smlouvy uzavřené s NKČR.

Položené otázky je možné přeformulovat následovně:

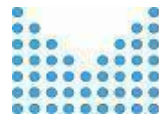
1. Jsou data přítomná v databázích Národních autorit chráněna nějakým absolutním majetkovým právem? Pokud ano, jakým? Jaký vztah jednotlivých přispěvatelů, kteří se na vzniku databáze podílejí?
2. Jakým způsobem je upraveno poskytování těchto dat v kontextu zákona č. 106/1999 Sb., o svobodném přístupu k informacím? Je zde možnost (ať už na straně NKČR, nebo na straně jednotlivých knihoven zapojených do projektu) poskytovat tato data? Je zde již existující povinnost tato data poskytovat?
3. Liší se nějak situace Souborného katalogu oproti Národním autoritám?

K první otázce

Předně je třeba konstatovat, že data samotná (samotné údaje) nejsou nijak autorskoprávně chráněná, ani se k nim neváže žádné jiné absolutní majetkové právo (např. věcné).¹⁷ Stejně tak je zřejmé, že součástí databáze není dílo, které by naplňovali definici autorského díla ve smyslu § 2 zákona č. 121/2000 Sb. (dále AutZ).¹⁸ Další z možných způsobů ochrany se nabízí ochrana struktury databáze a výběru jejích prvků jako samostatného autorského díla (jako

¹⁷ Viz též např. KOŠČÍK, Michal. Výzkumná data ve světle absolutních majetkových práv. In: KOŠČÍK, Michal et al. *Výzkumná data a výzkumné databáze. Právní rámec zpracování a sdílení vědeckých poznatků*. Praha: Wolters Kluwer ČR, 2018, s. 25–31.

¹⁸ Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.



autorskoprávně chráněná originální databáze) ve smyslu § 2 odst. 2 AutZ. I tento způsob ochrany se však v daném případě nebude aplikovat. Krom toho že, jak vyplývá ze zápisu ze setkání supervizorů projektu „Kooperativní tvorba a využívání souborů národních autorit“ v Národní technické knihovně ČR 28. 6. 2016, ani samotní tvůrci databáze za autorské dílo nepovažuje, nevykazují databáze Národních autorit ve způsobu výběru nebo uspořádání dat takovou míru originality, aby je bylo možné za dílo považovat. Podmínkami pro přiznání autorskoprávní ochrany databáze totiž je, že jde o autorův duševní výtvar a zároveň výběr prvků a jejich uspořádání musí být výsledkem tvůrčí činnosti. Dle rozhodovací praxe Soudního dvora EU pak není podmínka duševního výtvaru splněna tehdy, kdy „*vytvoření databáze je dáno technickými úvahami, pravidly nebo omezeními, která neponechávají žádný prostor pro tvůrčí svobodu*“.¹⁹ Vzhledem k tomu, že záznamy v databázích Národních autorit jsou plně podřízené účelu daného záznamu, kterým je jednoznačná identifikace daného pojmu, není možné hovořit o přítomnosti prostoru pro tvůrčí svobodu. Krom toho i pokud by byla databáze vyhodnocena jako že splňuje nezbytné požadavky na přiznání autorskoprávní ochrany jako originální databáze, byla by vzhledem k veřejnému charakteru databáze a jejímu veřejnému účelu velmi pravděpodobně, vyhodnocena jako úřední dílo ve smyslu § 3 písm. a) AutZ.

Z možných ochranných režimů tak zbývá jediné ochrana zvláštními právy pořizovatele databáze, která jsou upravena v § 88 a následujících AutZ. Zvláštní práva pořizovatele databáze (právo na vytěžování nebo na zužitkování celého obsahu databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva²⁰) náleží takovému subjektu (pořizovateli databáze), který na svou odpovědnost pořídí databázi, nebo pro kterou tak z jejího podnětu učiní jiná osoba.²¹ Nezbytnou podmínkou pro vznik těchto práv je pak přítomnost podstatného vkladu do pořízení, ověření nebo předvedení obsahu databáze, přičemž platí, že investice vynaložená na vytvoření prvků databáze se do vkladu na pořízení nepočítá.²² To znamená, že se započítává pouze vklad (finanční, časový, znalostní) vynaložený na zařazení již existujících prvků do databáze. Ku příkladu, v případě jmenných autorit tedy vytvoření katalogizačního záznamu (zařazení již existujících prvků jméno autora, a dalších informací o něm) je způsobilé být podkladem pro podstatný vklad. Pro následující úvahy předpokládejme, že Databáze národních autorit jsou chráněny zvláštním právem pořizovatele databáze, protože jsou této ochrany způsobilé vzhledem k značnému finančnímu a časovému vkladu, který je vynakládán pro pořízení, ověření nebo předvedení obsahu databáze.

Aby byla osoba oprávněná jako pořizovatel databáze je nezbytné, aby do vzniku databáze investovala (učinila podstatný vklad do pořízení, ověření nebo předvedení obsahu databáze) a zároveň, aby vznik databáze podnítila.²³ Z uvedeného vyplývá, že byť databáze Národních autorit vzniká v zásadě kooperačním způsobem NKČR a spolupracujících knihoven, je

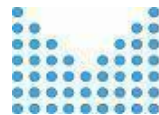
¹⁹ Bod 39 rozsudku Soudního dvora Evropské unie ze dne 1. 3. 2012, ve věci C-604/10 - Football Dataco a další, [dostupné z curia.europa.eu]. Viz též HUGENHOLTZ, P. Bernt. Directive 96/9/EC. In: DREIER, Thomas; HUGENHOLTZ, P. Bernt (eds.). *Concise European copyright law*. Second edition. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2016, s. 392.

²⁰ Viz § 90 odst. 1 AutZ.

²¹ Viz § 89 AutZ.

²² Srovnej HUGENHOLTZ, P. Bernt. Directive 96/9/EC. In: DREIER, Thomas; HUGENHOLTZ, P. Bernt (eds.). *Concise European copyright law*. Second edition. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2016, s. 405. Dále viz bod 42 rozsudku Evropského soudního dvora ze dne 9. 11. 2004, ve věci C-203/02 - The British Horseracing Board a další, [dostupné z curia.europa.eu] a bod 53 rozsudku Evropského soudního dvora ze dne 9. 11. 2004, ve věci C-444/02 – Fixtures Marketing, [dostupné z curia.europa.eu].

²³ Srovnej HUGENHOLTZ, P. Bernt. Directive 96/9/EC. In: DREIER, Thomas; HUGENHOLTZ, P. Bernt (eds.). *Concise European copyright law*. Second edition. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2016, s. 403.



pořizovatelem databáze NKČR, protože je to právě ona, kdo databázi spravuje a její vznik podnítl. Krom toho, záznamy dodané od spolupracujících institucí jsou ještě přímo zaměstnanci NKČR kontrolovány z hlediska správnosti a až následně zařazovány do báze Národních autorit.

Vedle právě uvedeného je však nezbytné uvést, že v souladu s § 94 AutZ se na zvláštní právo pořizovatele databáze přiměřeně použije ustanovení § 3 písm. a) AutZ, které zakládá výjimku úředního díla. Vzhledem k tomu, že databáze slouží veřejnému účelu (jak bylo přesvědčivě popsáno je důležitost databáze pro fungování knihovnických systémů, a tedy její veřejný charakter nezpochybnitelný) a byla vytvořena z veřejných prostředků, měla by se na tuto databázi výjimka úředního díla vztahovat a databáze by tak neměla být chráněna zvláštním právem pořizovatele databáze i přes to, že naplňuje znaky podstatného vkladu.

K druhé otázce

Poskytování informací veřejného sektoru je obecně upraveno v zákoně 106/1999 Sb., o svobodném přístupu k informacím (dále InfoZ),²⁴ který je hlavním nositelem aplikace aktivní složky práva na informační sebeurčení – práva na informace. Zákon ve svém § 4 odst. 1 rozlišuje dva způsoby poskytování informací, kterými jsou poskytování informací na žádost a zveřejněním. Položený dotaz se týká poskytování informací zveřejněním. Tento způsob se dále dělí na povinné poskytování informací zveřejněním, které povinné subjekty provádějí přímo na základě uložené zákonné povinnosti (např. informace uvedené v § 5 odst. 1 InfoZ) a na dobrovolné poskytování informací zveřejněním. Dobrovolné poskytování informací je takové, které povinný subjekt činí ve své diskreci na základě obecného zmocnění uvedeného v § 5 odst. 7 InfoZ. Ten zní: „*Povinný subjekt může informace podle odstavce 1 zveřejnit i dalšími způsoby a s výjimkami uvedenými v tomto zákoně může zveřejnit i další informace.*“ Obsah zveřejněných informací si povinný subjekt může určit s výhradou informací, o kterých zákon stanoví, že je není možné poskytovat.²⁵ Zákaz poskytnout nějaké konkrétní informace pak může vyplývat jak z ustanovení InfoZ, tak ze zvláštních předpisů upravujících konkrétní zmocnění a povinnosti daných subjektů, protože ty pak působí jako *lex specialis* vůči InfoZ.

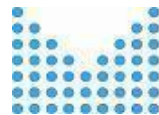
NKČR je zcela bez pochyby povinným subjektem dle zákona č. 106/1999 Sb.²⁶ Z toho důvodu je NKČR ustanovením § 5 odst. 7 InfoZ obecně zmocněna poskytovat i takové informace, které není jinak ze zákona povinná zveřejňovat. Co se týče kvality poskytovaných dat, každý povinný subjekt musí splnit podmínky stanovené v § 4b odst. 1 InfoZ, které je možné obecně shrnout tak, že poskytované informace mají být co nejotevřenější.

Ohledně argumentu, že data není možné poskytovat, protože by to představovalo nehospodárné nakládání s majetkem státu je možné uvést následující (pro potřeby následujících úvah předpokládejme s opatrnějším postojem, že je databáze Národních autorit chráněná zvláštními právy pořizovatele databáze, protože pokud by nebyla, tak by data samotná žádnou majetkovou hodnotu nepředstavovala, vzhledem k tomu, že se k nim nevazí žádná absolutní věcná práva). Právní úprava nakládání s majetkem státu (zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích) jako jeden ze základních důvodů pro využití majetku státu jeho organizačními složkami uvádí „plnění funkcí státu“ (§ 8 odst. 1, § 14) s přidanou povinností, že majetek musí být využíván účelně a hospodárně (§ 14 odst. 1). Poskytování informací veřejného sektoru způsobem umožňujícím následné využití je „plněním funkcí státu“. To je možné dovodit z řady relevantních právních dokumentů, včetně těch právně nejsilnějších. Tato činnost je způsobem, kterým stát pomáhat zajišťovat ústavně garantované právo na informace (čl. 17 Listiny základních práv a svobod).

²⁴ Zákon č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů.

²⁵ Srovnej např. § 7, 8a, a 9 až 11 InfoZ.

²⁶ NKČR je veřejnou institucí ve smyslu §2 odst. 1 InfoZ.



Požadavek na poskytování dat veřejného sektoru s možností následného využití pak přímo vyplývá z evropského práva, konkrétně ze směrnice 2003/98/ES, o opakovaném použití informací veřejného sektoru ve znění směrnice 2013/37/EU, která ještě požadavek na znovu využitelnost poskytovaných informací posílila. Právě z této směrnice vyplývá aktuální znění InfoZ. Výše zmiňovaný § 4b odst. 1 InfoZ například požaduje, aby formát i metadata poskytovaných informací co nejvíce splňovaly otevřené formální normy. Těmi jsou právě například technické a právní požadavky, které směřují k zajištění poskytování informací ve formátu otevřených dat. Poskytování informací jako otevřených dat v maximálně otevřené podobě (tzv. 5 hvězdiček, tedy propojená otevřená data), je tedy maximálním naplněním požadavku uvedeného v § 4b odst. 1.

Jako již čistě ekonomický argument podporující úspornost, a tedy oprávněnost, poskytování předmětných dat v podobě otevřených dat je fakt, že tento způsob (tedy publikace výstupů a umožnění přístupu k nim bez nutnosti zasílání jednotlivých dotazů do databáze) představuje pro daný informační systém výrazně menší zatížení jeho výpočetní kapacity, než kdyby tomu bylo naopak. Zároveň, vzhledem ke zjevným tendencím mířícím ke komplexnímu systému otevřených dat, pozorovatelným z výše uvedené evropské legislativy a mezinárodních závazků ČR, je pragmatické a ekonomicky výhodné publikovat informace standardizovaně jako otevřená data.

K závěru, že poskytování dat z databází Národních autorit nepředstavuje neekonomický zásah, který by mohl být hodnocen jako porušení povinností řádného hospodáře NKČR, je třeba uvést, že tento závěr je v souladu s východisky relevantních právních ustanovení práva EU. Čl. 1 odst. 6 směrnice č. 2019/1024,²⁷ která nahradí v současné době stále ještě účinnou směrnicí 2003/98/ES ve znění směrnice 2013/37/EU, uvádí, že povinné subjekty nesmí vykonávat zvláštní práva pořizovatele databáze s cílem bránit opakovanému použití dokumentů nebo je omezit nad rámec stanovený touto směrnicí. I pokud by tedy NKČR zvláštní právo pořizovatele databáze k databázím Národních autorit svědčilo, v souladu s budoucí právní úpravou jej nebude mít možnost vykonávat. Vzhledem k tomu je třeba konstatovat, že případné udělené licence CC BY, případně vzdání se práv prostřednictvím prohlášení CC0 nic nebrání.

K třetí otázce

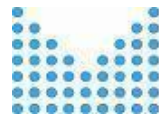
K posouzení právního režimu Souborného katalogu bohužel nemáme k dispozici dostatečné množství informací. Pokud o toto posouzení budete mít v budoucnu zájem, bylo by myslím vhodné domluvit se na osobním setkání, na kterém danou otázku probereme.

Závěrem

Výše uvedenou argumentaci je možné shrnout následovně:

- Data přítomná v databázích Národních autorit mohou být chráněna toliko zvláštními právy pořizovatele databáze ve smyslu § 88 a následujících AutZ. V takovém případě by byla pořizovatelem databáze, a tedy oprávněným vykonavatelem těchto práv NKČR. Je však možné, že se na danou databázi aplikuje výjimka úředního díla dle § 3 písm. a) AutZ a v takovém případě by předmětná data nebyla nijak majetkově chráněna.
- I v případě, že jsou databáze Národních autorit chráněné zvláštním právem pořizovatele databáze, žádné zákonné ustanovení NKČR nebrání v tom, aby je uvolnila jako otevřená (propojená) data. Nová evropská úprava v podobě směrnice 2019/1024 pak dokonce zapovídá vykonávání těchto práv povinnými subjekty.

²⁷ Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.



Zveřejnění daných dat pod licencí CC BY nebo CC0 tedy nepředstavuje protiprávní zásah do povinností vyplývajících z povinností nakládání s veřejným majetkem s péčí řádného hospodáře.

2. Komunikace s Parlamentním institutem – K povinností vyplývajícím z § 4b odst. 2 (2019)

Zaslaný dotaz:

Vážený pane/paní,

obracím se na Vás jménem Parlamentního institutu, což je vědecké, vzdělávací a informační středisko Poslanecké sněmovny Parlamentu České republiky. V současnosti vypracovávám materiál týkající se politiky otevřených dat. Ráda bych si skrze tento dotaz ověřila základní informace týkající se povinnosti obcí zveřejňovat informace v otevřeném formátu, respektive povinnosti zveřejňovat otevřená data.

Předpokládám, že z formálního hlediska obce jsou povinnými subjekty k poskytování otevřených dat s ohledem na znění § 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „InfZ“). Dle § 4b odst. 2 „povinné subjekty zveřejňují informace obsažené v jimi vedených nebo spravovaných registrech, evidencích, seznamech nebo rejstřících“, nicméně seznam informací zveřejňovaných jako otevřená data, který byl stanoven nařízením vlády č. 425/2016 Sb. de facto na obce nedopadá, neboť tyto vyjmenované registry, evidence, seznamy a rejstříky jsou vedeny převážně (možná dokonce i zcela) jinými subjekty než obcemi. Na obce tudíž povinnost dle § 4b odst. 2 InfZ de facto nedopadá. Méně jasný mi je výklad § 4b odst. 1 InfZ. Předpokládám, že existuje návaznost mezi ustanovením § 4b odst. 1 a § 5, tj. informace poskytnuté zveřejněním v elektronické podobě musí být zveřejněny i v otevřeném formátu. Je-li to možné, měly by být i strojově čitelné a je-li to zároveň i vhodné, měly by být doprovázeny metadaty. Poskytnuté informace tudíž nemusí být otevřenými daty ve smyslu § 3 odst. 11) InfZ, neboť způsob ani účel následného využití nemusí být neomezený a obce nemusí informace evidovat v národním katalogu otevřených dat, nicméně stále zákon požaduje alespoň zveřejnění v otevřeném formátu.

Skrze tento email bych Vás požádala o upřesnění, doplnění případně i o opravu mého výkladu ohledně povinnosti obcí zveřejňovat otevřená data. Nerada bych poskytla dále, neúplné nebo dokonce mylné informace. Bude-li to pro Vás pohodlnější, můžete mi informace poskytnout telefonicky na číslo 257 172 239. Zároveň bych Vás požádala o odpověď co nejdříve, ideálně dnes nebo zítra, neboť práce kterou zpracovávám, by měla být odevzdána v těchto dnech. Předpokládám, že informace, které mi poskytnete, budu moci následně promítnout do obsahu práce a zároveň Vás citovat jako zdroj informací.

Předem Vám děkuji za odpověď.

S pozdravem a přáním hezkého dne

Odpověď:

Vážená paní magistro,

předně, omlouvám se za pozdní odpověď, doufám, že Vám to takto bude stačit.

Ohledně Vašeho dotazu uvádím, že Vaše interpretace je obecně správná. Ustanovení § 4b odst. 2 zákona č. 106/1999 Sb. opravdu slouží toliko jako prostředek pro zmocnění vlády k vydání nařízení, ve kterém je přítomný seznam informací, které jsou jako otevřená data



publikována povinně. V současné době v nařízení vlády č. 425/2016 Sb. není žádná položka, která by se týkala obcí.

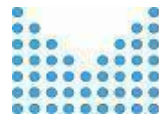
Na všechny povinné subjekty spadající pod zákon č. 106/1999 Sb. (včetně obcí), které poskytují informace zveřejněním však (jak správně uvádíte) dopadá povinnost uvedená v ustanovení § 4b odst. 1 tohoto zákona. Toto ustanovení se obecně vztahuje na všechny informace, které povinné subjekty poskytují zveřejněním ať už dobrovolně (na základě zmocnění přítomném v § 5 odst. 7 zákona č. 106/1999 Sb.) nebo povinně (na základě povinnosti založené zákonem č. 106/1999 Sb., nebo jakýmkoli jiným). Pokud jiný právní předpis upravuje detailní způsob poskytování specifických informací zveřejněním, tak má tento předpis samozřejmě dle zásady *lex specialis* přesnost.

Obce by tedy měly v případech, kdy poskytují informace zveřejněním, dodržet podmínky uvedené v citovaném ustanovení. To znamená, že informace mají být publikovány v otevřeném formátu a pokud je to vhodné tak rovněž ve strojově čitelném formátu. Vhodnost je pak třeba posuzovat dle faktické technické povahy informace - např. pokud jde o tabulku nebo prostý text, strojová čitelnost by měla být zachována (cílem je zabránit publikacím textových nebo tabulkových dokumentů, které jsou nejprve vytištěné a pak zpět nascanované jako obrázky, což efektivně zamezí jakémukoli strojovému zpracování). Stejně je pak třeba interpretovat i požadavek možnosti a vhodnosti na publikaci metadat s informací souvisejících (typicky se bude jednat například o datum vydání informace, identifikace jejího původce, případně klíčová slova, která se k informaci váží).

Poslední požadavek, který je v citovaném ustanovení přítomný je, že "formát (informace) i metadata by měly co nejvíce splňovat otevřené formální normy". Otevřená formální norma je dle § 3 odst. 9 "pravidlo, které bylo vydáno písemně a obsahuje specifikace požadavků na zajištění schopnosti různých programových vybavení vzájemně si poskytovat služby a efektivně spolupracovat". Kupříkladu, Odbor hlavního architekta eGovernmentu postupně vytváří a aktualizuje otevřené formální normy pro klíčové informace, které jsou často předmětem poskytování velkým množstvím povinných subjektů. Seznam těchto otevřených formálních norem je možné nalézt online zde: <https://opendata.gov.cz/otevřené-formální-normy:start>. V případě, že poskytovaná informace je nějakou otevřenou formální normou upravena, měla by ji "co nejvíce" splňovat. Tato součást povinností se rovněž týká všech povinných subjektů dle zákona č. 106/1999 Sb.

Je tedy pravdou, že obce nemají povinnost poskytovat informace v kvalitě otevřených dat, nemusí provádět registraci v národním katalogu OD a teoreticky mohou omezit způsob a účel následného užití informace, byť z právní vymahatelnosti je takové omezení je poměrně nejisté (k možnosti právní vymahatelnosti takového omezení vizte blíže argumentaci obsaženou např. na s. 142 a následujících - MÍŠEK, Jakub. Právní aspekty otevřených dat [online]. Brno, 2019, 172 s. Rigorózní práce, Masarykova univerzita, Právnická fakulta. Dostupné z: https://is.muni.cz/th/sqe7a/rigo_opendata_final.pdf). Na druhou stranu, pokud by si obec přála některé informace poskytovat jako otevřená data, obecně jí v cestě neleží žádná zákonná překážka (s výjimkou omezení daných ochranou práv duševního vlastnictví třetích osob, osobních údajů a podobně).

Závěrem bych Vás rád požádal, zda byste do zpracovávaného materiálu mohla uvést, že Odbor hlavního architekta eGovernmentu působí jako místo podpory, na které je možné se obracet v případech dotazů (ať už právních, nebo technických) týkajících se poskytování otevřených dat. Rovněž bych Vás rád požádal, zda byste nám následně mohla vypracovaný materiál poskytnout. Moc Vám děkuji.



Pokud budete mít k oblasti právní úpravy otevřených dat ještě jakékoli další dotazy, neváhejte se prosím na mě nebo na mé kolegy obrátit.

S pozdravem,

Jakub Míšek

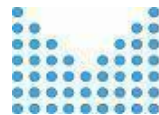
3. Vysvětlení pro OLEG: Otevřené formální normy na obsahy úředních desek (2020)

Koncept otevřených formálních norem (dále OFN) zavedla směrnice č. 2013/37/EU, která novelizovala směrnici 2003/98/ES a do českého právního řádu byla provedena v zákoně č. 106/1999 Sb. Jedná se o měkký nástroj technického sjednocování poskytování typizovaných informací veřejného sektoru. Těmi jsou informace, kterými disponuje (a zveřejňuje je) velké množství různých subjektů, a u kterých je zájem na jejich vzájemné kompatibilitě a snadné strojové zpracovatelnosti. Dobrým příkladem jsou právě informace na úředních deskách.

Otevřenou formální normou se myslí legislativně neupravený technický normativní dokument, který velice detailně popisuje, jakým způsobem (v jakých formátech a strukturách) mají být dané informace poskytovány. Směrnice ani zákon nepředvídají žádnou oficiální autoritu, která je oprávněna OFN vydávat. V současné době nicméně probíhá tvorba několika klíčových OFN na půdě OHA, mezi nimi rovněž OFN upravující úřední desky. Pro představu, zde jsou příklady současných pracovních verzí OFN. Výhodou OFN je její flexibilita. Vzhledem k tomu, že se v průběhu používání a životnosti OFN může ukázat jako nezbytné ji specifikovat detailněji, nebo aktualizovat vzhledem k technickému vývoji, je neformální způsob jejich vydávání vhodnou vlastností. OFN je zároveň veskrze technický dokument, jehož adresátem jsou primárně lidé, kteří přímo připravují data k publikaci (zpravidla IT oddělení). Do budoucna je však možné uvažovat o vytvoření podpory pro malé obce, například v podobě formulářových řešení, které umožní vytváření exportů v souladu s danou OFN i pro subjekty, které nemají dostatečnou interní technickou kapacitu.

V současné době zákon č. 106/1999 Sb. uvádí, že povinné subjekty by při poskytování informací zveřejněním by povinné subjekty měly dbát na to, že formát i metadata poskytovaných informací by měly co nejvíce splňovat otevřené formální normy. Chystaná novela, která právě prochází mezirezortním připomínkovým řízením, roli OFN posiluje, nicméně stále se jedná o relativně „měkkou“ povinnost.

Z hlediska právě posuzovaného návrhu, tedy že by se obsah úředních desek měl poskytovat jako otevřená data, s tímto úmyslem rozhodně souhlasíme. Zároveň se domníváme, že by detailní technický popis datových formátů a struktury měl být regulován měkce prostřednictvím OFN. Výhoda flexibility, kterou toto řešení přináší, je významná a máme za to, že tak detailní popis, jaký by byl pro efektivní sjednocení praxe poskytování informací z úředních desek za potřebí, není vhodné nastavovat prostřednictvím podzákonného prováděcího předpisu. Méně formální flexibilní nástroj se jeví jako vhodnější i z toho důvodu, že již v současné době zkušenost ukazuje, že řada povinných subjektů neplní ani ty povinnosti, které vyplývají již ze současného znění zákona č. 106/1999 Sb. Zároveň vzhledem k absenci sankcí v tomto zákoně není příliš pravděpodobné, že by se situace zlepšila prostřednictvím „tvrdé“ regulace. Vzhledem k tomu je možné předpokládat, že cesta „měkkou“ regulace nepřinese žádné faktické nevýhody z hlediska dodržování předepsaných norem, a naopak výhoda v podobě flexibilního technického řešení převažuje.



4. Reakce na Estonský *white paper* k možnosti publikovat jako otevřená data osobní údaje na základě jejich zařazení od HVDs (2020)

Reaction to Estonia's concerns regarding the publication of HVDs with personal data

Careless publication of public registers can lead to severe risk for data subjects. Furthermore, the balance between rights and interests of data subjects and interests of third parties on data processing must be maintained and at the same time, we must ensure that the legal framework maintains the high level of personal data protection. Generally, on the ground level, we agree with the message conveyed by the Estonian position paper. However, at the same time, we think that we should stress out, that publication of selected personal data in the open data quality is not infringing any GDPR rules per se. It is for the following reasons:

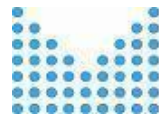
1) It is necessary to differentiate between the data processing on the side of public sector body (that is the publication of the data) and the data processing conducted by the third party, which reuses the data. These two processing activities have different originators and, more important, different purposes. Whereas the purpose of data processing on the side of the public sector body is to make the data public and to allow their secondary use, the purpose on the side of the third party is whatever legal processing they choose. The purpose limitation principle generally applies when there might be a new processing done by the same data controller. However, that is not the case with reuse of open data containing personal data.

2) When the third party (the re-user) starts with the data processing, it becomes data controller with all the duties, which arise from GDPR. More specifically, in accordance with the accountability principle the data controller must make sure, that the processing follows all other basic principles. E.g. he must process actual up-to-date data (accuracy), only such data that are necessary for the purpose he set (data minimisation), and he has to have a legal ground for data processing (legality), the processing must not exceed rights and interests of data subjects (fairness) and data subjects must be informed about the processing (transparency).

3) It is tough to meet the conditions presented in the second paragraph adequately. E.g. probably the only applicable legal ground for data processing when reusing public data is the legitimate interest. Thus, in a lot of the cases the secondary use would not be possible, because the data controller will not meet the requirements of the balancing test present in art. 6 para. 1 letter f) of GDPR. In our opinion the debate should focus on the secondary use and its legality, applicability, and possibility in general, and not so much on the act of publication, because that per se is not problematic.

4) Another example might be the question of transparency, that is how data controllers should effectively inform about their processing. For instance, in the Czech Republic, we expect creation of a new part of open data catalogue, which (by law) will be used for catalogisation of services and products that use personal data. This register can server as a right place which can effectively help both data controllers to fulfil their duties and data subject to perform their rights.

5) It is essential that data protection authorities effectively perform their tasks and impose sanctions on data controllers who process the data illegally, because they do not fulfil duties arising from GDPR. However, in our opinion, the complexity and compicacy of this task should not serve as a ground for banning publication of open data with personal data altogether.



We welcome the general request for conducting a proper DPIA during the legislation process. At the same time, we would very much welcome to shift the debate concerning personal data and open data from "let's question, whether it is possible" to "let's try to make it possible and safe for the data subjects". The problem is not creation of implementing act, or publication of the data. The complications might arise when such data is reused in a wrong (illegal) way. The Czech experience shows that high quality open data from business registers are essential for effective transparency. In our opinion it should be available for legitimate uses. The question, which must be adequately answered, is how to make sure that it is not used inadequately.

5. Vyjádření OHA MVČR k otázce poskytnutí dat z webové stránky www.kudyznudy.cz společnosti SmartGuide s.r.o. (IČ: 07254890) (2020)

Toto vyjádření se týká otázky, zda a za jakých podmínek je možné (nebo zda existuje povinnost) poskytovat informace zveřejněné na stránce kudyznudy.cz společnosti SmartGuide. Ta má zájem tyto informace přebírat v aktuální podobě prostřednictvím API a následně opětovně využívat ve svých komerčních službách.

Webová stránka kudyznudy.cz je tvořena převážně autorskoprávně chráněným obsahem (články a další texty, fotografie, videomateriál atd.), případně obsahuje rovněž osobní údaje registrovaných uživatelů (otázce osobních údajů se však tento dokument blíže nevěnuje). Z autorskoprávního hlediska je nutné rozdělit obsah stránky na ten, který je tvořen zaměstnanci a externími pracovníky agentury CzechTourism (a agentura je proto v pozici vykonavatele práv k těmto dílům, která vznikla jako díla zaměstnanecká) a ten, který vytvořen a vkládán registrovanými uživateli portálu. Vztah mezi uživateli a provozovatelem portálu je popsán v dokumentu „Pravidla provozování Portálu“ (<https://www.kudyznudy.cz/autorska-prava>), který je rovněž jediný dokument, zabývající se otázkou autorských práv k obsahu. K tomu je nezbytné poznamenat, že jím bohužel nejsou upraveny licenční vztahy mezi uživateli portálu a agenturou. Tento fakt představuje poměrně zásadní problém, který by do budoucna měl být řešen, protože vnáší do vztahu uživatelů a agentury velkou míru právní nejistoty. Pravidla dále uvádí, že obsah stránky je reprodukovatelný jen s předchozím písemným souhlasem agentury, s výhradou výslovně uvedených výjimek.

V současné době agentura poskytuje (po uzavření smlouvy o spolupráci: <https://www.kudyznudy.cz/podminky-poskytovani-pristupu-k-api>) obsah portálu prostřednictvím API „Kudy z nudy Public content API“ v rozsahu následujících dat:

- a. interní ID (guid) akce na portálu Kudy z nudy;
- b. název akce;
- c. datum poslední aktualizace akce na Portálu;
- d. datum prvního vytvoření akce;
- e. anotace akce, excerpt (perex);
- f. adresa stránky na portálu KZN;
- g. adresa teaser obrázku;
- h. datum konání akce „od“; a
- i. datum konání akce „do“.

Analýza současné situace

Poskytování a opětovné užití informací veřejného sektoru je právně upraveno na evropské úrovni směrnicí 2003/98/ES (ve znění směrnice 2013/37/EU), která bude od 17. července 2021 nahrazena směrnicí EU č. 2019/1024 o otevřených datech a opakovaném použití



informací veřejného sektoru. Základním principem stávající i nadcházející právní úpravy je zajištění, aby informace veřejného sektoru byly poskytovány takovým způsobem, který co nejvíce usnadní a umožní jejich následné užití. To platí jak z hlediska technického (proto právní úprava upřednostňuje otevřené a strojově čitelné formáty), tak z hlediska právního (následné užití zveřejněných informací by nemělo být jakkoli omezeno nad rámec zákona). Tato evropská právní úprava je na české úrovni obsažena v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím.

Je třeba souhlasit se závěry, že v současné době neexistuje povinnost aktivně poskytovat (zveřejňovat) informace z portálu kudyznudy.cz (ani dalších webových stránek), a pokud tak agentura CzechTourism činí, jedná tak v rámci své diskrece, která vyplývá mimo jiné rovněž např. z § 5 odst. 6 zákona č. 106/1999 Sb. (ve znění k srpnu 2020). Je však nutné připomenout, že i v případě, kdy jsou informace poskytovány dobrovolně, musí poskytovatel naplnit standard kvality stanovený § 4b odst. 1 téhož zákona.

Dále je možné souhlasit s tím, že agentura CzechTourism nemůže pro další užití zveřejnit informace, které jsou chráněné autorským právem třetích osob, pokud k tomu není licenčně oprávněna. Takové oprávnění není možné interpretovat z *Pravidel provozování Portálu* a není tedy možné jednoznačně tvrdit, že nositelé práv k obsahu by s dalším nakládáním s jejich autorskoprávně chráněnými díly souhlasili. Vzhledem k charakteru Portálu je zřejmě možné dovodit, že externí přispěvatelé implicitně souhlasí s užitím jejich děl v kontextu provozu portálu, ale již není možné jednoznačně tvrdit, že by souhlasili rovněž s jejich dalším užitím jinými subjekty. V kontextu dalšího užití v současné době zveřejněných informací je možné maximálně poukázat na výjimky a omezení autorského práva, které jsou obsaženy v zákoně č. 121/2000 Sb. (§ 29 a následující), zejména pak citační výjimku, kterou je zřejmě možné aplikovat na zveřejněné perexy a anotace (pokud by vůbec tyto texty byly autorskoprávně chráněné).

Vedle toho je ale dále nezbytné zdůraznit, že agentura CzechTourism je jako státní příspěvková organizace povinným subjektem podle zákona č. 106/1999 Sb. Z toho vyplývá její **povinnost poskytovat informace na základě žádosti učiněné dle tohoto zákona**. Žadatel může specifikovat, jakým způsobem si přeje, aby mu informace byly poskytnuty a povinný subjekt obecně musí v tomto ohledu žadateli vyhovět, ledaže by takový způsob představoval nepřiměřenou zátěž (§ 4a odst. 3 zákona č. 106/1999 Sb.). Jedním ze zákonem předvídaných způsobů je rovněž poskytování informací prostřednictvím API (§ 4a odst. 2 písm. e)). Povinný subjekt může podmínit poskytnutí informace zaplacením nákladů nezbytných na umožnění takového poskytnutí. Vzhledem k zásadě publicity veřejné správy pak musí povinný subjekt poskytnout všechny vyžádané informace, které nejsou zákonem z poskytování vyloučeny. Jednou z takových zákonem předpokládaných výjimek je i situace, kdy by poskytnutím informace bylo zasaženo do práv duševního vlastnictví třetích osob.

Z výše uvedeného vyplývá, že pokud by agentura CzechTourism obdržela žádost o informace obsažené na Portálu ve smyslu zákona č. 106/1999 Sb., a žadatel si je přál získat prostřednictvím API, je obecně povinna tyto informace poskytnout. Pokud by poskytnutí informací tímto způsobem představovalo nepřiměřenou zátěž, tak (za předpokladu že jsou již online) postačí, když na požadované informace odkáže. V rozhodnutí o vyřízení žádosti je však nezbytné řádně odůvodnit, v čem nepřiměřenost zátěže spočívá. Pokud jde například jen o výši nákladů, které by stálo zpřístupnění informací tímto způsobem, měl by povinný subjekt dát žadateli možnost dané náklady uhradit a informaci poskytnout způsobem, jaký žadatel preferoval.

Z hlediska autorského práva výše uvedené beze zbytku platí pro obsah vytvořený zaměstnanci a externími pracovníky agentury. Ten musí CzechTourism poskytnout vždy. Máme za to, že



argument nemožnosti rozlišení, zda je o vlastní obsah, nebo obsah dodaný uživateli, není možné použít, protože „nepořádek“ v datech povinného subjektu nemůže jít k tíži žadatele.

V případě autorských děl, která agentura CzechTourism nemá dostatečně licenčně zajištěná (tedy obsah vkládaný uživateli Portálu) je situace odlišná. Samotné poskytnutí díla by spíše nepředstavovalo zásah do autorského práva, a to ze dvou důvodů. Za prvé ta díla jsou již veřejnosti sdělována prostřednictvím Portálu a za druhé, samotné poskytnutí informace (díla) je možné zahrnout pod aplikaci tzv. úřední licence ve smyslu § 34 autorského zákona. Na druhou stranu, takové poskytnutí by bylo pro žadatele značně matoucí, protože by díla vytvořená uživateli Portálu stejně nemohl dále opětovně užívat z důvodu nedostatečného licenčního oprávnění. Z toho důvodu je racionálně odůvodnitelné odmítnout poskytnutí těchto informací dožádaným způsobem, případně pouze odkázat na webové stránky.

Výše uvedené je možné shrnout následovně:

I) V případě aktivního poskytování informací zveřejněním je věcný rozsah zveřejněných informací na uvážení agentury CzechTourism, protože neexistuje zákonná povinnost tyto informace poskytovat. Způsob provedení jejich zveřejnění však musí být v souladu s § 4b odst. 1 zákona č. 106/1999 Sb.

II) V případě žádosti o poskytnutí obsahu Portálu prostřednictvím API na základě zákona č. 106/1999 Sb. je ideálním zákonným řešením poskytnout informace v rozsahu informací (dat), které nejsou chráněny zvláštním zákonným režimem (tj. prostá data), a dále v rozsahu autorskoprávně chráněných děl, ke kterým CzechTourism vykonává autorská práva. Ve zbylém rozsahu by bylo vhodné odkázat na existující aplikaci Portálu. CzechTourism může poskytnutí informace podmínit úhradou poplatku ve výši nezbytných nákladů na poskytnutí informace. CzechTourism dále může odmítnout poskytnout informace prostřednictvím API, pokud by byl tento způsob nepřiměřeně náročný, což je však třeba dostatečně odůvodnit.

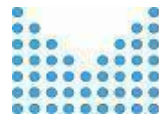
Doporučení do budoucna

Nad rámec výše uvedeného bychom Vám na základě provedené analýzy rádi navrhli ke zvážení následující doporučení:

1. Domníváme se, že omezení následného užití informací z Portálu pouze na nekomerční aplikace není vhodným řešením. Jakkoli v současné době nikterak neodporuje textu zákona č. 106/1999 Sb., je v rozporu s duchem celé právní úpravy představované směrnicemi 2003/98/ES a EU 2019/1024. Cílem právní úpravy informací veřejného sektoru je zajištění možnosti jejich opakovaného užití za jakýmkoli dalším zákonným účelem a způsobem, a to včetně využití komerčního. Směrnice EU 2019/1024 předvídá omezení tohoto principu jen v případě prokázaného závažného veřejného zájmu.

2. Vzhledem k tomu, že služby CzechTourism silně pracují s autorskoprávně chráněným obsahem třetích stran, je nezbytné precizně licenčně vyjasnit, za jakých podmínek je tento obsah vkládán a jak s ním může CzechTourism dále nakládat. Silně doporučujeme zvážení využití licencí Creative Commons, které jsou celosvětovým standardem pro licencování otevřeného obsahu online. Konkrétně bychom doporučili využití licence CC BY 4.0, která umožní další neomezené nakládání s licencovaným obsahem pod podmínkou uvedení autora a zdroje.

6. Doporučení k vyhodnocování povinnosti vyplývající z § 5a odst. 2 zákona č. 106/1999 Sb. (2021)



K § 5a odst. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Nový § 5a odstavec 2 zavedl za účelem následného efektivního využití zveřejněných informací povinnost poskytovat každému dostupné informace obsažené v registrech jako otevřená data. Pojem „registr“ je legislativní zkratkou založenou v § 5a odst. 1, která označuje registry, evidence, seznamy nebo rejstříky obsahující informace, které jsou na základě zákona každému přístupné, přičemž se jedná jen o takové registry, které jsou vedené nebo spravované na základě zákona, tedy nikoli dobrovolně vedené registry (které si povinné subjekty vedou samy o svém rozhodnutí). Jinými slovy, § 5a odst. zakládá povinnost poskytovat informace, které jsou na základě zákona veřejné, a které jsou vedené v zákonem založených nebo předvídaných registrech také jako otevřená data. Jedná se o projev zásady „standardního zpřístupnění dokumentů ve formě otevřených dat“ stanovené bodem 16 preambule a čl. 5 odst. 2 Směrnice 2019/1024 (tzv. „Open Data směrnice“).

Z důvodu ochrany osobních údajů se tato povinnost nevztahuje na údaje o jménu a příjmení, datum narození, rodné číslo a adresu trvalého pobytu nebo bydliště. Rok narození a název obce trvalého pobytu jsou zanechány jako údaje poskytované jako otevřená data z důvodu možnosti zkoumání statistik. Výjimka o vyloučení osobních údajů se nevztahuje na případy, kdy jsou poskytované údaje uvedeny v registrech v souvislosti s podnikáním nebo jinou obdobnou výdělečnou činností nebo v souvislosti s členstvím fyzické osoby ve statutárním nebo jiném orgánu právnické osoby nebo s výkonem funkce statutárního orgánu nebo v souvislosti s postavením skutečného majitele podle zákona upravujícího evidenci skutečných majitelů.

Je třeba připomenout, že příjemci takto zveřejněných informací, které obsahují osobní údaje, se dostávají do pozice správce údaje ve smyslu Obecného nařízení o ochraně osobních údajů (nařízení EU č. 2016/679) se všemi povinnostmi, které se k tomuto postavení váží.

Pokud existuje zvláštní právní úprava, která specificky vymezuje technický způsob poskytování informací zveřejněním, § 5a odst. 2 se vzhledem k aplikaci zásady *lex specialis* nepoužije.

Ustanovení obsahuje výjimku pro zveřejňování dokumentů ze sbírky listin. Jde například o listiny ze sbírky obchodního rejstříku a dalších rejstříků osob. Tato výjimka je zařazena proto, že princip zveřejňování informací ve formě otevřených dat (tedy v otevřeném a zejména strojově čitelném formátu) může představovat problém pro plnotextové dokumenty obsažené ve sbírce listin. Naopak technicky a realizačně poměrně jednoduché a stále informačně velmi hodnotné je zveřejňování metadat o těchto dokumentech. Pokud by výjimka nebyla zavedena, dopadla by povinnost na všechny sbírky listin všech povinných subjektů, což by u velké části z nich představovalo zcela zásadní problém z hlediska nákladů na splnění takové povinnosti. Zároveň by informační přidaná hodnota takto zveřejňovaných plnotextových dokumentů těmto nákladům neodpovídala. Je však třeba připomenout, že veřejné dokumenty ze sbírky listin je stále třeba zveřejňovat v souladu s obecnými požadavky na kvalitu poskytovaných informací, které jsou vyjádřeny v § 4b zákona č. 106/1999 Sb.

§ 5a odst. 2 nahradil předchozí právní úpravu povinných otevřených dat spočívající v nařízení vlády č. 425/2016 Sb., které provádělo § 4b odst. 2 zákona č. 106/1999 Sb. ve znění pozdějších předpisů v účinnosti do 24. 7. 2021. Nové ustanovení věcně nepředstavuje velký rozdíl, protože i do nařízení vlády č. 425/2016 Sb. mohly být vybírány pouze informace, které již byly na základě zákona veřejně dostupné a byly vedeny v zákonem založených předvídaných registrech. Z toho důvodu platí i nadále povinnost, která se vztahovala na informace uvedené nařízení vlády č. 425/2016 Sb. Povinné subjekty, které spravují informace, na které tato povinnost od července 2021 dopadla nově mají na jejich zveřejnění lhůtu do 31.



12. 2023 a to na základě Čl. LI zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

Při analýze, které informace je potřeba v souladu s § 5a odst. 2 poskytovat jako otevřená data je možné vyjít z jednoduchého schématu dělení informací, kde můžeme definovat následujících 5 kategorií:

Kategorie 1 – Informace, které již byly součástí nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, a existuje tedy povinnost jejich poskytování v podobě otevřených dat. Tato povinnost platí i nadále a okamžitě po nabytí účinnosti změnového zákona č. 261/2021 Sb. Přejícné ustanovení se totiž týká pouze odkladu zveřejnění, ale pokud již informace zveřejněná byla, tato povinnost je naplněna a bylo by proti smyslu zákona, kdyby se přejícné ustanovení vykládalo jako možnost odstranění těchto informací a pak jako následná povinnost jejich opětovného zveřejnění.

Kategorie 2 – Informace, které povinný subjekt musí poskytovat jako otevřená data podle § 5a odst. 2 (přejícné ustanovení zakládá lhůtu na splnění této povinnosti do 31. 12. 2023). Jedná se o takové informace, u nichž již existuje primární povinnost jejich poskytování povinnými subjekty a které jsou zároveň vedené v zákonem založených nebo předvídaných registrech. Jinými slovy, informace vedené v zákonem založených nebo předvídaných registrech, které má již povinný subjekt povinnost poskytovat, budou povinně poskytována rovněž jako otevřená data. Zároveň je třeba nezapomenout na nutné provedení pseudonymizace v souladu s výjimkou uvedenou v § 5a odst. 2.

Kategorie 3 – Informace, které je možné poskytovat jako otevřená data na základě diskrece povinného subjektu (v souladu s ustanovením § 5 odst. 5 zákona č. 106/1999 Sb., o svobodném přístupu k informacím). Jde tedy o informace, u kterých neexistuje právní povinnost jejich zveřejnění, nebo o informace, které jsou sice zveřejňovány na základě právní povinnosti, ale nejsou vedeny v zákonem založeném nebo předvídaném registru. Takové informace může povinný subjekt zveřejnit, pokud se tak na základě vlastní diskrece rozhodne. Tyto informace je však nezbytné poskytovat v kvalitě, kterou předepisuje § 4b, která se otevřeným datům přibližuje.

Kategorie 4 – Informace, které není možné poskytovat jako otevřená data proto, že je jejich poskytování vyloučenou výjimkou uvedenou v § 8a nebo v § 9-11 zákona č. 106/1999 Sb., případně jiným zvláštním zákonem.

Kategorie 5 – Informace, které jsou zcela vyňaty z působnosti zákona 106/1999 Sb., o svobodném přístupu k informacím. Právní úprava otevřených dat podle tohoto zákona se tak na ně přímo nevztahuje a pro jejich poskytování je třeba se řídit jejich zvláštními právními předpisy. Jde například o informace spadající pod působnost zákona č. 123/1998 Sb., nebo o informace katastru nemovitostí.

7. Dotazy zaslané od společnosti Databox po provedeném školení na téma právní úprava otevřených dat (2021)

Dotazy - otevřená data

Prosím Vás o objasnění následujícího:

- **Existují nějaké limity pro zpracování otevřených dat pro komerční účely?**

Na obecné úrovni nikoli. Tato problematika je upravena evropskou směrnicí č. 2019/1024 o otevřených datech, která navazuje na tzv. PSI směrnicí č. 2003/98/ES.

Cílem této právní úpravy je zajistit, aby informace veřejného sektoru, které jsou zveřejňované členskými státy byly v co nejširší míře opětovně použitelné za minima právních překážek a za co nejnižších nákladů. V českém právním prostředí je PSI směrnice implementována v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím. Na implementaci Open data směrnice stále čekáme.

Zákon o svobodném přístupu k informacím upravuje obecně otázku jaké informace je možné publikovat (obecně jakékoli u kterých to zákon nevylučuje) a způsob publikování informací (opět, tak aby bylo jejich další užití co nejsnadnější). Je třeba dodat, že pojem „otevřená data“ hovoří primárně o technické a právní kvalitě poskytovaných informací veřejného sektoru, nikoli o jejich obsahu.

Otázku dalšího užití zákon výslovně neřeší. Ta je tak řešena obecnou zásadou legální licence, tedy že každý může činit v rozsahu toho, co není zákonem vyloučeno. Z toho důvodu je omezené další užití informací veřejného sektoru v případech, že tyto informace jsou chráněny nějakými zvláštními ochrannými režimy (např. právo duševního vlastnictví, obchodní tajemství, nebo ochrana osobních údajů), a zároveň tyto zvláštní ochranné režimy dané specifické další užití vylučují (např. nemám k dispozici licenci, která by mi umožnila užití díla; zpracování osobních údajů by nebylo podloženo právním titulem podle čl. 6 odst. 1 GDPR atd.). V konkrétních případech tak limity pro další zpracování otevřených dat mohou spočívat ve zvláštních právních režimech, které regulují dané informace.

- **Jaké existují možnosti zpracování otevřených dat pro nekomerční účely?**

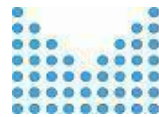
Zákon nerozlišuje mezi komerčními a nekomerčními účely. Evropské právo v podobě PSI i Open data směrnice vyžaduje opětovnou využitelnost za jakýmkoli účely.

Obecně tedy viz výše.

- **Bude na webu NKOD existovat nějaká část webu, kde bude možné plnit informační povinnost těch, kteří využívají a zpracovávají otevřená data, která obsahují osobní údaje? (Jiná forma plnění informační povinnosti podle nařízení GDPR, např. e-mailem - nemáme vždy, telefonicky - kapacitně nejsme schopni zajistit, nebo poštou - příliš finančně i časově nákladné, pro nás představuje nepřiměřené úsilí.) - zmiňoval jste to na konferenci, prosím Vás o detailnější informace.**

Výhledově (po přijetí implementační novely Open Data směrnice) se plánuje rozšíření funkcionality NKOD, aby zde bylo možné registrovat rovněž služby a produkty, které otevřená data využívají. Součástí této registrace pak bude rovněž indikace, zda jsou v nich využívány osobní údaje a pokud ano, tak o jaké osobní údaje se jedná. Doufáme, že tento krok umožní subjektům údajů efektivně vykonávat jejich práva a zároveň technicky umožní správcům údajů naplnit svoji informační povinnost. Jak se daná aplikace projeví v praxi zatím nedokážeme předvídat.

- **Jak vhodně používat cloud computing pro ukládání otevřených dat, především, pokud obsahují osobní údaje?**



Tato otázka se netýká přímo problematiky právní úpravy otevřených dat, ale plnění povinností správce osobních údajů obecně. Vzhledem k tomu na ni nemohu ze své pozice odpovědět. I proto, že vyžaduje širší analýzu a nutnost vyhodnocení konkrétní situace.

- **A když jsou data pouze uložena v zašifrované podobě, je nutná zpracovatelská smlouva podle nařízení GDPR s poskytovatelem cloudu?**

Viz výše.

Nicméně obecně – i zašifrovaná data jsou stále osobní údaje, pokud existuje možnost jejich rozšifrování. Pouze představují nižší riziko pro práva a zájmy subjektů údajů. Vzhledem k tomu, že jde stále o osobní údaje, je třeba se řídit povinnostmi vyplývajícími z GDPR, včetně uzavření zpracovatelské smlouvy.

- **Data, která jsou prezentována jako otevřená data na vlastním webu organizace, ale nejsou v NKOD - lze je považovat a zpracovávat jako otevřená data?**

Ano. Stále je o zveřejněné informace veřejného sektoru (mimořádně, to platí i pro takové informace, které nejsou označeny jako otevřená data), obecně tedy platí to, co jsem uvedl k první otázce. Registrace v NKODu není konstitutivní za jakéhokoli úhlu pohledu, má pouze přehledový efekt.

- **Když zpracujeme otevřená data z více zdrojů, musíme výsledky a výstupy poskytnout také v podobě otevřených dat? Musíme u dat uvádět nějakou licenci pro další zpracování? A jak je to s uvedením zdroje - stačí pouze obecný odkaz na web instituce nebo musí být uveden aktivní zdroj přímo místa, kde lze otevřená data získat?**

Případná otázka dalšího licencování není jakkoli podmíněna množstvím zdrojů, ze kterého při tvorbě služby nebo produktu opětovný uživatel čerpá. Jakákoli povinnost poskytnout dále obsah by byla založena maximálně v podobě licenční smlouvy s doložkou v principu share alike (například CC BY-SA). Předně je však třeba zdůraznit, že licencovat (a tedy i licenční smlouvou vymáhat jakékoli podmínky dalšího užití dat) je možné pouze obsah, který je chráněn právy duševního vlastnictví – tedy typicky autorským právem nebo zvláštními právy pořizovatele databáze. To však většinou nebude ten případ dat poskytovaných jako otevřená data. Prostá data nejsou jakkoli chráněná, nevztahuje se na ne ani vlastnické právo (prostá data není možné „vlastnit“ v právním slova smyslu).

Tedy přímá odpověď na Vaše dotazy – ze zpracování otevřených dat (získaných ať už z jednoho nebo více zdrojů) nevyplývá žádná povinnost tato data dále poskytovat.

Moc nerozumím dotazu, zda musíte uvádět nějakou licenci pro další zpracování – ze zákona obecně nevyplývá žádná povinnost pro Vás jako příjemce dat s daty jakkoli nakládat (mohou ale vyplývat dílčí povinnosti podle právní povahy dat a jejich specifické ochrany).

Ohledně uvedení zdroje obecně stačí uvést název publikující instituce. Vhodné je

například uvést rovněž kdy byla data sesbírána, případně jak často probíhá aktualizace dat v aplikaci.

- **V příloze posílám návrh naší informace na naše webové stránky, mohu poprosit o Vaše hodnocení, zda jsou informace vhodně podané, celistvé, případně co bychom měli doplnit nebo upravit apod.?**

Omlouvám se, komplexní vyhodnocení informačního dokumentu je rovněž mimo rozsah možných konzultací, které z pozice MV můžeme poskytovat.

Pár obecných poznámek:

- Nemyslím si, že je možné aplikovat právní titul plnění smlouvy podle čl. 6 odst. 1 písm. b). Tento právní titul je limitován opravdu jen na zpracování, které je zcela striktně nezbytné pro splnění smlouvy, jíž je subjekt údajů stranou. Z Vašeho dokumentu však taková informace nevyplývá.
- Balanční test by měl být přítomný a argumentovaný. Dá se očekávat, že pro ÚOOÚ nebude dostatečná informace, že byl proveden, ale bude chtít vidět i to konkrétní provedení.
- Pozor, stránky jednotlivých společností obecně nespádají pod právní úpravu otevřených dat (to že jsou data online neznamená, že jsou otevřená). To bude důležité při argumentaci oprávněného zájmu.
- Zkontrolujte si, že Vaše informační dokumenty v celku naplňují požadavky čl. 14 GDPR. Zatím ten pocit nemám.

8. Vyjádření pro Národní knihovnu ohledně možnosti publikace jejich databází jako otevřená data (2021)

K obavě vzdání se práv v rámci licencí CC k datům, za jejichž vznik a správu byly vynaloženy veřejné prostředky.

Veřejná licence CC BY 4.0 je licence nikoli obecné vzdání se práva. Je to licence bezúplatná a licencováním pod touto licencí se poskytovatel zavazuje, že nabízený obsah nebude poskytován za úplatu. Obecně je účelem této licence umožnit co nejširší možnost dalšího užití daného obsahu. Slovo „waive“ se v licenci opravdu vyskytuje, ale jen na několika místech, které z hlediska toho, že se jedná o licenci a nikoli absolutní vzdání se toho práva, nehrají příliš roli. Konkrétně jde o následující:

Článek 2, oddíl a) odst. 4.: „Poskytovatel Vás opravňuje vykonávat Licencovaná práva prostřednictvím všech médií a formátů známých v tuto chvíli i vzniklých v budoucnu a provádět technické úpravy k tomu potřebné. Poskytovatel se vzdává práva zakázat Vám technické úpravy potřebné k výkonu Licencovaných práv, a to včetně technických úprav potřebných k obcházení Účinných technických prostředků a/nebo souhlasí s tím, že toto právo nebude vykonávat. Pro účely této Veřejné licence platí, že samotné úpravy povolené v tomto článku 2(a)(4) nikdy nevedou k vytvoření Zpracovaného obsahu.“

Komentář: V tomto případě jde o závazek poskytovatele, že nebude omezovat technické úpravy obsahu, a konkrétně, že nebude vymáhat případné překonání DRM (tedy technických prostředků ochrany autorského práva). Vzhledem k tomu, že obsah poskytovaných databází není (předpokládám) chráněný DRM, není ustanovení relevantní.



Článek 2, oddíl b) odst. 1: „Na osobnostní práva, jako například právo na nedotknutelnost, se tato Veřejná licence nevztahuje, stejně jako na právo na podobu a soukromí a/nebo další obdobná osobnostní práva; nicméně, k tomu, aby Vám umožnil vykonávat Licencovaná práva se Poskytovatel v nejširším možném rozsahu vzdává a/nebo se zavazuje je nevykonávat.“

Komentář: Osobnostních práv se v českém právním řádu vzdát nedá. Toto ustanovení není v kontextu českého práva aplikovatelné, resp. je aplikovatelné v rozsahu, kdy se poskytovatel licence zavazuje práva nevykonávat. Krom toho, zvláštní právo pořizovatele databáze osobnostní stránku nemá, a toto ustanovení proto z hlediska tohoto práva není relevantní.

Článek 2, oddíl b) odst. 3: „Poskytovatel se v nejširším možném rozsahu vzdává veškerých práv, na jejichž základě od Vás může vybírat odměnu za vykonávání Licencovaných práv, ať už přímo či prostřednictvím kolektivního správce na základě jakéhokoli systému dobrovolné, rozšířené nebo povinné kolektivní správy. Ve všech ostatních případech si Poskytovatel výslovně vyhrazuje právo vybírat takovou odměnu.“

Komentář: Toto ustanovení souvisí s tím, že jde o bezúplatnou licenci. Majetkových práv autorských se opět v českém právním řádu vzdát nedá, dají se pouze licencovat. V tomto smyslu je také nezbytné číst dané ustanovení. Druhá část ustanovení se týká odměn od kolektivních správců – z hlediska knihovních dat pak kolektivní správa nehraje žádnou roli. V případě digitalizovaných děl to může být jinak, ale to je mimo rozsah tohoto vyjádření.

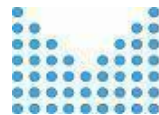
Uvedené je možné shrnout, že licence CC BY 4.0 je opravdu licence a nikoli vzdání se práv a to zejména proto, že jiného z hlediska open data relevantního práva, než zvláštního práva pořizovatele databáze se není možné v českém právu vzdát. Naprosté vzdání se práva pak představuje CC0 – tu ale není možné použít na autorské právo (potom se chová jako CC BY).

Opětovně musíme uvést, že i případné vzdání se zvláštního práva pořizovatele databáze není nijak zákonně vyloučeno – ostatně z již aplikovatelné OD směrnice (směrnice č. 2019/1024) jasně vyplývá závazek, že poskytovatelé dat nesmějí vykonávat zvláštní právo pořizovatele databáze tak, aby jakkoli omezilo další užití obsahu databáze. Jedinou možností, jak tento požadavek naplnit je buď licencovat obsah databáze pod veřejnou licenci CC BY 4.0, nebo se těchto práv vzdát, např. prostřednictvím prohlášení CC0.

Neporušuji zveřejněním pravidla pro správu majetku?

Ministerstvo vnitra nemá pravomoc autoritativně rozhodnout o otázkách spojených s nakládáním s majetkem státu, nicméně dle našeho odborného názoru, jakožto gestora problematiky otevřených dat a sdílení veřejných dat s veřejností obecně, a ostatně i z české a evropské legislativy vyplývá, že publikace dat zdarma je v pořádku a měla by být podporována. Nad rámec legislativy jsme také přesvědčeni, že zveřejňování informací NK v podobě otevřených dat naplňuje cíle, pro které byla jakožto instituce zřízena.

Předně je třeba říct, že je problematické klasifikovat prostá data (tedy data, která nepodléhají nějakému zvláštnímu režimu ochrany např. právy duševního vlastnictví) jako majetek státu. Určitě tam není problém ve chvíli, kdy jsou pevně navázána na fyzický nosič (např. data na CD, data na konkrétním disku atd.) – s tím si umíme poradit, protože ta data sdílí právní osud toho nosiče. Z hlediska prostých dat, která jsou jen uložena pouze ve virtualizované podobě v databázi je však jejich vyhodnocení jako „majetku“ nejasné. Zákon o nakládání s majetkem státu pak tuto otázku vůbec neřeší, je tedy nezbytné vyjít z obecného předpisu v podobě OZ, ze kterého ovšem opět dojdeme k doktrinárně přijímanému názoru, že k prostým datům se nevztahuje žádná absolutní majetková práva – data tedy není možné „vlastnit“ v právním slova smyslu. Je možné maximálně technicky omezovat přístup k nim, případně tento přístup



podmínit smluvními podmínkami, které je pak možné vymáhat. Ukládání těchto podmínek je však z principů evropského práva (OD směrnice č. 2019/1024 a ostatně i před ní PSI směrnice 2003/98/ES) vyloučeno.

Ohledně platné právní úpravy se není možné v tuto chvíli úplně odkázat na platné předpisy nad rámec uvedených pravidel zákona č. 106/1999 Sb. Z hlediska nezbytnosti umožnění dalšího užití dat, která se nachází v databázi chráněné sui generis právy je nezbytné odkázat na čl. 1 odst. 6 směrnice 2019/1024, který uvádí: „*Subjekty veřejného sektoru nevykonávají právo pořizovatele databáze podle čl. 7 odst. 1 směrnice 96/9/ES s cílem bránit opakovanému použití dokumentů nebo je omezit nad rámec stanovený touto směrnicí.*“ Toto ustanovení v zásadě říká, že databáze chráněné sui generis právy, které jsou poskytovány veřejnosti, je nezbytné co nejotevřeněji licencovat, nebo se daného práva vzdát. Jakkoli tato formulace ještě nebyla implementována do zákona 106 je nepochybné, že v nějaké formě implementována bude. Pokud platí takováto úprava pro obsah chráněný právem duševního vlastnictví, tím spíš bude platit pro prostá data.

Co se týče digitalizovaných děl, tak zákon o svobodném přístupu k informacím zveřejnění umožňuje a PSI/OD směrnice počítají s tím, že do jejich působnosti spadají digitalizovaná díla. Pokud jsou to autorskoprávně volná díla (70 let po smrti autora), tak jsme přesvědčeni, že ve zveřejnění nic nebrání, pokud jde o digitalizovaná díla, která jsou ještě autorskoprávně chráněná, tak bychom radili zdrženlivost zejména, protože předpokládáme, že NK k tomuto nemá licenci.

Mohu poskytovat otevřená data i bez zákonné povinnosti?

Ano. Dle § 5 odst. 5 zákona č. 106/1999 Sb., o svobodném přístupu k informacím mohou informačně povinné subjekty obecně zveřejňovat informace, ledaže by se v konkrétním případě jednalo o zákonem omezenou výjimku (například protože jde o osobní údaje nebo obchodní tajemství).

Informace poskytované zveřejněním, ať už povinně nebo na základě této dobrovolnosti, je třeba poskytovat v souladu s § 4b v otevřeném formátu (alespoň jednom), a pokud to umožňuje technická specifikace informace, tak musí být formát i strojově čitelný. Zákon zároveň stanoví, že formát i metadata by měly co nejvíce splňovat otevřené formální normy, což jsou podzákonná psaná pravidla, často technického charakteru, která mají zajistit standardizaci a interoperabilitu mezi různými poskytovateli informací, aby byla co nejvíce zajištěna možnost opětovného užití informací. Zákon tedy předpokládá co možná nejotevřenější způsob publikace informací. Na stránce <https://data.gov.cz/ofn/> naleznete otevřené formální normy, které směřují ke správné publikaci otevřených dat, a které mají být v souladu s § 4b co nejvíce dodržovány.

Otázka podoby implementace směrnice 1024/2019 – směrnice výslovně uvádí náhradu nákladů knihovnám a jiným paměťovým institucím, ale v české implementaci není...?

Tato ustanovení byla už součástí předchozí PSI směrnice a do českého práva implementována nebyla. Směrnice stanovuje jen minimální standard, který však zákonodárce členského státu může překonat. Pokud se tak rozhodne nevyužít výjimku, která je upravena v čl. 6 odst. 2 písm. b) OD Směrnice, nemusí.



Jaké náklady si NK může říct za poskytování dat?

Řídí se to zákonem č. 106/1999 Sb. – konkrétně § 17 odst. 1:

„Povinné subjekty jsou v souvislosti s poskytováním informací oprávněny žádat úhradu ve výši, která nesmí přesáhnout náklady spojené s pořízením kopií, opatřením technických nosičů dat a s odesláním informací žadateli. Povinný subjekt může vyžádat i úhradu za mimořádně rozsáhlé vyhledání informací.“

Ideálně tedy zdarma. Více viz výše – předchozí otázka.

Jak postupovat v situaci, kdy NK vymaže osobní údaje ze svých databází žádost, ale neví, kdo všechno si tato data převzal a měl by je tedy také vymazat? Toto není pro NK problém. Dá se očekávat, že bude data zveřejňovat jako dumpy – je pak na příjemcích, aby si udržovali databázi aktuální. V tomto směru je důležitý § 9 zákona č. 110/2019 Sb. o zpracování osobních údajů. Ten vytváří fikci, že v případě předávání údajů pomocí evidence (tj. i otevřená data) stačí změna v evidenci pro to, aby se považovalo za splněnou povinnost o informování příjemců údajů.