# **SBORNÍK** 27. ROČNÍKU KONFERENCE **ISSS**

**12.–13.5.**25
**Hradec**Králové


isss 2025

**generální** partner


**hlavní** partneři








**hlavní AI** partner


**partneři**






**odborní** partneři





partner **odborného bloku**

ATS TELCOM

spolupracují

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

MPSV

Královéhradecký kraj

ict unie

pořadatelé

TRIADA

Kraj Vysočina

ČESKÝ ZAVINÁČ

ponca

hlavní partner projektu

Hradec Králové už 800 let

REGINA

# **Záštitu** konferenci poskytli

**Petr Pavel**, prezident České republiky
**Miloš Vystrčil**, předseda Senátu Parlamentu České republiky
**Petr Fiala**, předseda vlády České republiky
**Martin Dvořák**, ministr pro evropské záležitosti
**Petr Kulhánek**, ministr pro místní rozvoj
**Martin Kupka**, ministr dopravy
**Petr Koleta**, hejtman Královéhradeckého kraje
**Asociace krajů** České republiky

# Obsah

# ORP a kybernetické hrozby: Analýza odborných zdrojů v kontextu připravované regulace

Ing. Lucie Burianová, Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra regionálních studií
Mgr. Petr Štěrba, Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra hospodářských dějin

## Úvod

Kybernetická bezpečnost se v kontextu moderní veřejné správy stává klíčovým předpokladem pro spolehlivé a důvěryhodné poskytování digitálních služeb. Zatímco centrální instituce a provozovatelé kritické infrastruktury jsou již několik let podrobeni regulaci prostřednictvím zákona č. 181/2014 Sb., o kybernetické bezpečnosti, obce dosud žádné právní povinnosti v této oblasti neměly. Odpovědnost za kybernetickou bezpečnost u obcí tak byla většinou nepřímo delegována na stát či dodavatele informačních systémů, což vedlo ke značné roztříštěnosti přístupů a nerovnoměrné úrovni ochrany.

V souvislosti s přijetím směrnice Evropského parlamentu a Rady (EU) 2022/2555, známé jako NIS2, dochází ke změně. Nová směrnice zásadně rozšiřuje okruh regulovaných subjektů a zahrnuje mezi ně i veřejnou správu, včetně obcí s rozšířenou působností. Transpozice těchto požadavků do české legislativy probíhá prostřednictvím návrhu nového zákona o kybernetické bezpečnosti, jehož cílem je stanovit povinnosti i pro tzv. subjekty v režimu nižších povinností. To vyvolává otázku, nakolik jsou v návrhu zákona a souvisejících dokumentech skutečně reflektována rizika, která odborná literatura považuje za klíčová v kontextu municipalit.

Cílem tohoto příspěvku je na základě analýzy vědeckých studií identifikovat hlavní rizika kybernetické bezpečnosti na úrovni obcí a následně posoudit, zda a jak jsou tato rizika systémově řešena v rámci českého právního, strategického a metodického rámce, zejména v souvislosti s implementací NIS2. Výzkum se opírá o syntézu poznatků publikovaných v odborné literatuře a jejich porovnání s aktuálním návrhem české legislativy a podpůrných dokumentů Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Pozornost je zaměřena především na oblasti, které jsou často považovány za problematické: personální kapacity, organizační odpovědnost, technologická zastaralost a meziodborová koordinace.

## Nový zákon o kybernetické bezpečnosti

I přes to, že obce představují klíčovou součást veřejné správy, tak do nedávné doby se na ně nevztahovala žádná plošná legislativní povinnost v oblasti kybernetické bezpečnosti. Zásadní obrat přináší evropská směrnice NIS2, která prostřednictvím návrhu nového zákona o kybernetické bezpečnosti (ZoKB) zavádí systémové požadavky pro obce s rozšířenou působností. Tím dochází k prvnímu institucionálnímu ukotvení kybernetické bezpečnosti na úrovni místní samosprávy.

Směrnice NIS2 byla navržena Evropskou komisí v prosinci 2020 jako reakce na rostoucí kybernetické hrozby a nedostatky předchozí právní úpravy. Po sérii vyjednávání byla přijata jako směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU. Schválena byla v listopadu 2022 a vstoupila v platnost 16. ledna 2023. Jejím cílem je posílit bezpečnost subjektů poskytujících klíčové a důležité služby prostřednictvím nových povinností v oblasti ochrany informačních systémů, řízení kybernetických rizik, hlášení incidentů a zajištění přeshraniční spolupráce.

Transpozice směrnice do právního řádu České republiky proběhne prostřednictvím nového zákona o kybernetické bezpečnosti, jehož přijetí se očekává v roce 2025. Členské státy EU měly povinnost začlenit ustanovení směrnice NIS2 do své národní

legislativy do 17. října 2024. Nový zákon o kybernetické bezpečnosti nebude ovšem obsahovat pouze NIS2, ale i další legislativní dokumenty jako například vyhlášky.

Oproti předchozí směrnici přináší NIS2 několik zásadních změn. Rozšiřuje okruh povinných subjektů, nově zahrnuje i organizace ve veřejné správě a dalších strategických odvětvích. Zpřesňuje požadavky na bezpečnostní opatření, zavádí přísnější dohled nad jejich dodržováním a nově umožňuje ukládání sankcí za jejich porušení. Dále posiluje evropskou koordinační kapacitu prostřednictvím sítě EU-CyCLONe (European Cyber Crises Liaison Organisation Network), která slouží ke koordinaci a reakci na přeshraniční kybernetické incidenty.

Samotné obce by měly zabezpečovat primárně ty informační systémy, které samy provozují, což znamená užší rozsah aktiv, na která budou zaváděna bezpečnostní opatření. Jedná se například o spisovnou službu, elektronickou poštu, úřední desku nebo ekonomický systém. Konkrétní bezpečnostní opatření budou vycházet z agend, které určitá obec vykonává. Podle poslední verze návrhu nového ZoKB by měly všechny ORP být zařazeny do tzv. režimu nižších povinností. Dále by ORP měly zavést tzv. neopominutelná opatření, a poté tzv. vyhodnotitelná opatření, která budou určena na základě konkrétních agend a činností, jež ORP vykonávají. Pro přehled je jejich detailní popis níže.[1]

**Neopominutelná opatření**

- Systém zajišťování minimální KB
- Požadavky na vrcholné vedení
- Bezpečnost lidských zdrojů
- Řízení kontinuity činností
- Řešení kybernetických bezpečnostních incidentů

**Vyhodnotitelná bezpečnostní opatření – každá obec si jejich dodržování musí vyhodnotit sama**

- Řízení přístupu
- Řízení identit a jejich oprávnění
- Detekce a zaznamenávání kybernetických bezpečnostních událostí
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

## Výzvy a rizika pro ORP

Rostoucí digitalizace veřejné správy a zvyšující se počet elektronických služeb pro občany je spojeno s vyšším rizikem kybernetických hrozeb. Analýza odborné literatury i dalších veřejně dostupných zdrojů potvrzuje existenci řady strukturálních, personálních a systémových zranitelností, které mohou ohrozit nejen stabilitu a funkčnost informačních systému, ale i samotnou ztrátu důvěry občanů ve využití digitálních technologií ze strany státu.

Vědecké studie zaměřené na kybernetickou bezpečnost municipalit [1, 4, 8] konzistentně poukazují na riziko v podobě nedostatečných investic do technického zabezpečení, chybějící personální kapacity a chybějící organizační odpovědnost. Například Caruson ve své studii uvádí, že z výzkumného vzorku méně, než polovina obcí disponuje základní bezpečnostní politikou a pouze 22 % má připravený plán reakce na incidenty [1]. Podobně i další studie zaměřená na podobnou problematiku upozorňuje na absenci srozumitelného rámce řízení rizik na lokální úrovni, a na skutečnost, že veřejné organizace nejsou schopné vyhodnotit účinnost přijatých opatření, a to z důvodu absence zpětné vazby z incidentů a odborná evaluace [8].

1 Další informace: https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67aca68381589befac075202#s2-rozsah-regulovane-sluzby-a-vykon

Někteří autoři upozorňují na to, že kybernetická bezpečnost v obcích je často brána jako výlučně technický problém svěřený IT oddělení bez strategického ukotvení v rámci řízení organizace. To vede k tomu, že kyberbezpečnost není začleněna do širšího rámce organizačního řízení rizik, což je v rozporu s moderním přístupem prosazovaným rámcem NIST Cybersecurity Framework či směrnicí NIS2 [5].

Zjištění navíc poukazují na rizika spojená s rychlou digitalizací bez odpovídající bezpečnostní architektury [7]. Přijetí nových informačních systémů často předbíhá budování jejich ochrany, a to jak na úrovni infrastruktury, tak organizační kultury. V mnoha případech chybí odpovědná osoba za kybernetickou bezpečnost, nejsou realizována školení zaměstnanců a chybí krizové scénáře nebo pravidelné testování odolnosti systémů vůči útokům.

Z výše uvedených poznatků je zřejmé, že rizika spojená s kybernetickou bezpečností obcí jsou komplexní a víceúrovňová – týkají se jak technických, tak organizačních, lidských i finančních aspektů. Jejich přehled shrnuje následující tabulka:

Tabulka č. 1: Rizika kybernetické bezpečnosti obcí, doporučená opatření a jejich řešení v ČR

| **Název rizika** | **Doporučená opatření** | **Řešení v ČR (pro všechny aktéry)** | **Řeší se v návrhu nového ZoKB?** |
|---|---|---|---|
| Neefektivní využití investic do bezpečnosti | Strategie řízení rizik<br>Prioritizace bezpečnostních opatření řešící konkrétní slabiny<br>Tvorba bezpečnostní strategie a plán rozvoje<br>Využití sdílených služeb a centrální podpory<br>Pravidelné hodnocení efektivity | Povinnost řízení rizik dle ZoKB a vyhlášky 82/2018 Sb.<br>Národní strategie KB ČR 2021–2025<br>Podpůrný materiál NÚKIB | Ano, zařazením do režimu nižších povinností, zavedením principu přiměřenosti –<br>Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu, nevyžaduje přijmout všechna bezpečnostní opatření |
| Nedostatek personálních kapacit | Outsourcing bezpečnostních služeb<br>Zřízení bezpečnostního manažera | x | Ano, ale pouze – osoba zodpovědná za KB nemusí být nový zaměstnanec, ZoKB explicitně neřeší nedostatek personálních kapacit (neposkytuje finanční zdroje, ani nepřiděluje kapacity) |
| Vysoké náklady na útoky a jejich dopady | Plán obnovy provozu<br>Zálohování a testování<br>Pojištění kybernetických rizik | Částečně řešeno ve vyhlášce | Ano řeší: svými bezpečnostními opatřeními snižuje náklady a jejich dopad (např. školení zaměstnanců, Stanovení pravidel ochrany aktiv a přípustné způsoby jejich používání, Pořízení a schválení bezpečnostní politiky) |
| Slabá organizační odpovědnost a přehled o datech | Odpovědná osoba za kybernetickou bezpečnost<br>Identifikovat technická a datová aktiva | ZoKB<br>Podpůrný materiál NÚKIB | Ano řeší:<br>Určení osoby zodpovědné za KB, pořízení a schválení bezpečnostní politiky, explicitní definování povinností vrcholného vedení,<br>Přehled o datech – zavedení bez. opatření – Stanovení pravidel ochrany aktiv a přípustné způsoby jejich používání |

| | | | |
|---|---|---|---|
| Nízká úroveň školení a povědomí zaměstnanců | Pravidelná školení a simulace (phishing)<br>Zařazení volených zástupců do programu vzdělávání | Podpůrný materiál NÚKIB<br>Programy NÚKIB pro školy, úřady i samosprávy | Ano řeší – explicitně požaduje školení zaměstnanců, a to především administrátorů a osoby zodpovědné za KB |
| Zastaralé technologie bez ochrany | Aktualizace systémů<br>Vícefaktorová autentizace<br>Bezpečnostní nástroje | Částečně řešeno ve vyhlášce | Ano, návrh nového ZoKB požaduje stanovení bezpečnostních požadavků v souvislosti s akvizicí, vývojem a údržbou, což mimo jiné znamená, že musí být systémy a jejich ochrana aktualizovány |
| Izolovaný přístup uvnitř organizace | Vytvoření koordinační skupiny<br>Zapojení IT oddělení obce do strategických rozhodnutí | x | Ano, vyžaduje školení zaměstnanců, vytvoření politik bezpečného chování uživatelů a zajištění kontroly dodržování bezpečnostní politik a pravidel a postupů pro řešení porušení |

*Zdroj: vlastní výzkum*

Na základě shrnutých poznatků v tabulce č. 1 lze analyzovat, jakým způsobem jsou klíčová rizika kybernetické bezpečnosti obcí reflektována v českém právním, metodickém a strategickém rámci. Z analýzy vyplývá, že některá opatření mají částečnou nebo úplnou oporu ve stávajících dokumentech – zejména v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB), prováděcí vyhlášce č. 82/2018 Sb. a v podpůrných dokumentech vydaných NÚKIB. Je však třeba zdůraznit, že tyto právní předpisy se dosud nevztahovaly na obce. Jejich aplikace v prostředí obcí tedy nebyla právně závazná, ale spíše dobrovolná.

S příchodem nové evropské směrnice NIS2 a její transpozicí do českého právního řádu formou nového zákona o kybernetické bezpečnosti se však situace mění. Obce s rozšířenou působností (ORP) budou nově zařazeny do tzv. režimu nižších povinností, což znamená, že pro ně vznikne řada nových závazků – např. v oblasti řízení rizik, stanovení odpovědné osoby, zavedení bezpečnostní politiky a hlášení incidentů. Přesto zůstává důležité rozlišovat, která opatření budou skutečně povinná, a která nadále zůstávají pouze doporučeními bez přímé vymahatelnosti.

## Neefektivní využití investic do bezpečnosti

Riziko neefektivního využití investic do kybernetické bezpečnosti je v českém prostředí podpořeno existujícími nástroji – zejména zmíněnou legislativou a metodikami jako Průvodce řízením aktiv a rizik (NÚKIB). Tyto nástroje poskytují základní rámec pro identifikaci aktiv, vyhodnocení zranitelností a prioritizaci opatření. Přesto je v praxi velmi obtížné určit, co je ve veřejné správě skutečně efektivní investicí. Neexistuje jednotná metodika pro vyjádření návratnosti bezpečnostních opatření, a jednotlivé obce často nemají kapacity pro ekonomické hodnocení těchto rozhodnutí.

Výše zmíněný průvodce řízením aktiv přináší princip přiměřenosti – tzn. že náklady na zaváděná opatření by neměly převyšovat pravděpodobné náklady spojené s potenciálním incidentem. Tento přístup může pomoci zejména menším obcím, které nemají kapacitu zavést všechna opatření v plném rozsahu. Pozitivním krokem zůstává podpora sdílených služeb, která je akcentována i v Národní strategii kybernetické bezpečnosti ČR 2021–2025.

## Nedostatek personálních kapacit

Oproti jiným oblastem představuje nedostatek personálních kapacit pro zajištění kybernetické bezpečnosti jednu z nejzásadnějších překážek v praxi. Mnoho obcí, zejména těch menších, není schopno dlouhodobě zajistit kvalifikovaný personál, přičemž trh práce nabízí jen velmi omezené možnosti. Chybí rovněž systémová podpora pro sdílení expertních kapacit nebo centrální

nabídku školených odborníků. Zavádění pozice odpovědné osoby za kybernetickou bezpečnost se tak v praxi často omezuje na formální přiřazení této agendy některému z existujících zaměstnanců – a to bez odpovídající odbornosti, času nebo podpory.

Návrh ZoKB sice vyžaduje určení osoby zodpovědné za kyberbezpečnost, nicméně neřeší způsob jejího financování ani dostupnost personálu na trhu. V principu se tedy nejedná o systémové řešení nedostatku lidských zdrojů, ale spíše o přenesení odpovědnosti na samotné obce.

### Vysoké náklady na útoky a jejich dopady

Riziko vysokých nákladů spojených s kybernetickými útoky je v metodických dokumentech částečně řešeno prostřednictvím požadavků na plán obnovy provozu, zálohování dat a jejich testování. Tato opatření mají pomoci minimalizovat dopady incidentu a zkrátit dobu výpadku. V praxi jsou však zaváděna nerovnoměrně a často chybí nejen plánování, ale i testování funkčnosti záloh. Přitom právě obnovitelnost dat bývá v praxi jedním z hlavních bodů selhání.

Navrhovaný ZoKB se tomuto tématu věnuje nepřímo – některá z bezpečnostních opatření (např. školení, bezpečnostní politika, řízení přístupů) přispívají ke snížení pravděpodobnosti incidentu a minimalizaci jeho dopadů. Samotné finanční nástroje, jako je kybernetické pojištění, zůstávají mimo rámec zákona a jejich využívání je zatím spíše výjimečné.

### Slabá organizační odpovědnost a přehled o datech

Analýza vědeckých studií zabývajících se kybernetickou bezpečností ve veřejné správě [5, 7, 8] ukazuje, že nedostatečně definovaná organizační odpovědnost patří mezi opakující se slabiny na úrovni místních samospráv. Z výzkumů vyplývá, že v mnoha organizacích není jednoznačně určeno, kdo nese odpovědnost za bezpečnost informačních systémů, a zároveň chybí přehled o datech, přístupech i zodpovědných osobách. Agenda kybernetické bezpečnosti bývá často rozptýlena mezi různé útvary a osoby, které postrádají potřebné kompetence nebo autoritu.

Návrh nového zákona v reakci na NIS2 již počítá s tím, že i obce v režimu nižších povinností budou muset určit odpovědnou osobu za kyberbezpečnost, přijmout bezpečnostní politiku a zavést základní opatření vedoucí k ochraně aktiv. Dále je požadováno výslovné vymezení rolí a povinností vrcholového vedení, čímž se kybernetická bezpečnost začleňuje do obecného řízení organizace.

Jako důležitý podpůrný nástroj lze uvést Průvodce řízením aktiv a rizik (NÚKIB), který poskytuje obcím návod, jak systematicky identifikovat svá technická a informační aktiva, přiřazovat jim odpovědnosti a definovat pravidla přístupů. Ačkoliv se jedná o dobrovolný materiál, jeho využití může významně přispět ke zvýšení přehledu o datové infrastruktuře a ke zlepšení řízení bezpečnostních opatření.

### Nízká úroveň školení a povědomí zaměstnanců

Lidský faktor je v oblasti kybernetické bezpečnosti opakovaně označován jako nejslabší článek celého systému. Vědecké studie [2, 4, 7] uvádějí, že právě nedostatečné školení a nízká úroveň bezpečnostního povědomí zaměstnanců často vedou k incidentům – typicky v důsledku kliknutí na škodlivé odkazy, špatné správy hesel či nezabezpečené práce na dálku.

V českém prostředí je vzdělávání zaměstnanců doporučováno prostřednictvím materiálů NÚKIB i v rámci Národní strategie kybernetické bezpečnosti, nicméně není systematicky kontrolováno ani metodicky jednotné. Tato situace se mění s návrhem nového ZoKB, který již explicitně požaduje školení zaměstnanců, zejména administrátorů a odpovědných osob, a zároveň klade důraz na školení formou simulací a praktických cvičení (např. phishingové testy).

### Zastaralé technologie bez ochrany

Mnoho obcí provozuje starší softwarové a hardwarové systémy, které jsou nekompatibilní s moderními bezpečnostními standardy. Tyto systémy bývají záplatovány nepravidelně, nepodporují klíčová opatření jako vícefaktorovou autentizaci, šifrování či

segmentaci sítě, a často neumožňují implementaci pokročilých nástrojů správy bezpečnostních událostí. V řadě případů se jedná o tzv. legacy systems, které i přes svou technologickou zastaralost plní klíčové funkce v chodu obce – např. správu obyvatel, účetnictví nebo provoz klientských portálů.

Tento stav je důsledkem především omezených finančních a investičních kapacit obcí, které často narážejí na nízké rozpočty, nemožnost čerpat účelové prostředky a neexistenci dlouhodobé strategie obnovy techniky. V praxi se obce často dostávají do cyklu, kdy obnova techniky trvá několik let, a ve chvíli, kdy je dokončena, jsou pořízené systémy již technologicky zastaralé. Tento fenomén představuje zásadní strukturální překážku, která brání dosažení minimální bezpečnostní úrovně, a přitom není překonatelná pouze organizačními opatřeními.

Na rizika spojená s technologickou zaostalostí opakovaně upozorňuje odborná literatura [2, 3], která zastaralé technologie označuje za tzv. „bezpečnostní dluhy" – tedy oblasti, kde organizace vědomě nebo z nutnosti rezignují na standardy z důvodu kapacitního vyčerpání nebo finanční nedostupnosti.

Český návrh zákona o kybernetické bezpečnosti sice zmiňuje požadavky na zajištění bezpečnosti v rámci akvizice, vývoje a údržby systémů, což znamená, že systémy mají být průběžně aktualizovány a chráněny. Návrh však neobsahuje žádný konkrétní nástroj nebo mechanismus, jak financovat modernizaci těchto systémů, ani podporu jejich obměny. Proto je nutné, aby stát či centrální autority zajišťovaly cílenou finanční podporu (např. prostřednictvím dotačních titulů), nabídku sdílených nástrojů nebo cloudových služeb, které umožní i menším obcím naplnit požadavky směrnice NIS2.

### Izolovaný přístup uvnitř organizace

Obce často čelí izolovanému přístupu, kdy jednotlivé odbory úřadu fungují odděleně, bez sdílení informací, koordinace a zapojení IT do strategického rozhodování. Tento roztříštěný přístup brání efektivnímu řízení kybernetické bezpečnosti a vytváří zranitelná místa napříč organizací. Obce by se měly zaměřit na meziodborové koordinace a systémového řízení [5, 8].

Návrh nového zákona o kybernetické bezpečnosti tuto oblast přímo neřeší, ale vyžaduje nastavení bezpečnostní politiky, školení a pravidel pro chování uživatelů, čímž vytváří předpoklad pro lepší spolupráci napříč úřadem. V praxi se doporučuje zřízení koordinační skupiny, která propojí IT, vedení a klíčové agendy, a zajistí jednotný přístup k bezpečnosti.

### Diskuze

Výše uvedená zjištění naznačují, že implementace požadavků směrnice NIS2 na úrovni obcí, zejména obcí s rozšířenou působností, může být ovlivněna řadou institucionálních a praktických bariér. Vysoký počet samosprávních jednotek a jejich značná variabilita z hlediska velikosti, organizační struktury a dostupných kapacit zásadně ztěžují zavádění jednotného systému opatření. Z rozdílné míry technického a personálního vybavení a odlišné úrovně zkušeností s řízením kybernetických rizik, vyplývá riziko nerovnoměrné implementace i naplňování zákonných povinností.

Jedním z významných omezujících faktorů je nedostatek kvalifikovaných odborníků na kybernetickou bezpečnost na trhu práce, přičemž státní správa včetně obcí má kvůli omezeným mzdovým možnostem ztíženou pozici při jejich náboru. Tento strukturální problém nelze řešit na úrovni jednotlivých obcí samostatně, a proto se jako jedno z možných řešení nabízí využití modelu sdílených odborných kapacit na regionální úrovni. Spolupráce v rámci místních akčních skupin, svazků obcí či jiných meziobecních struktur by mohla přispět ke snížení nákladů a efektivnějšímu využití dostupných lidských zdrojů.

Kromě otázky kapacit se v praxi objevují i pochybnosti ohledně přiměřenosti některých technických a organizačních opatření. Pokud budou implementována řešení, jejichž provozní nebo technologická náročnost výrazně převyšuje reálné potřeby daného subjektu, může to vést k neefektivnímu využívání prostředků. Zvýšené náklady mohou souviset nejen s pořízením technologií, ale také s následnými požadavky na školení zaměstnanců, správu dokumentace a průběžný provozní dohled. Za těchto podmínek je důležité důsledně uplatňovat princip přiměřenosti, který směrnice NIS2 předpokládá, a posuzovat udržitelnost jednotlivých opatření v provozním prostředí samospráv.

Pro zvýšení relevance a efektivity regulačních zásahů je nezbytné systematicky pracovat s potřebami a zkušenostmi samotných obcí jako koncových uživatelů bezpečnostních politik. Tyto subjekty disponují specifickými znalostmi svého provozního a personálního zázemí, které často nejsou v centrálních návrzích dostatečně reflektovány. V tomto kontextu se jako užitečné jeví vytvoření nástroje nebo platformy umožňující obcím sdílet své podněty, identifikovat problémové oblasti a poskytovat zpětnou vazbu. Výstupy z těchto mechanismů by mohly sloužit jak pro evaluaci implementace, tak pro cílené rozšíření podpůrných aktivit v oblastech, jako jsou školení, metodická podpora či systémová koordinace. Vhodnou formou mohou být tematická šetření, konzultace nebo online dotazníky.

Dalším aspektem, který se objevuje v odborné literatuře, je vztah mezi bezpečnostními incidenty a důvěrou veřejnosti v digitální služby veřejné správy. Opatření v oblasti kybernetické bezpečnosti by proto neměla být vnímána pouze jako nástroj pro technické zajištění provozu, ale i jako prostředek k udržení důvěry občanů. Incidenty, které vedou k úniku dat nebo dlouhodobému výpadku služeb, mohou negativně ovlivnit legitimitu digitální agendy a způsobit pokles její akceptace ze strany veřejnosti.

V neposlední řadě lze za důležitý předpoklad úspěšné implementace považovat rozvoj spolupráce s akademickými a výzkumnými institucemi. Ty mohou působit jako metodická a analytická opora při vyhodnocování rizik, nastavování politik i zajištění odborného vzdělávání. Propojení praxe samospráv s výzkumem může vést k formulaci lépe cílených a udržitelných opatření, která budou odpovídat specifickým podmínkám jednotlivých typů obcí.

## Shrnutí

Tento příspěvek se zaměřuje na analýzu hlavních rizik kybernetické bezpečnosti na úrovni obcí s rozšířenou působností (ORP) v souvislosti s implementací směrnice NIS2 a návrhem nového zákona o kybernetické bezpečnosti v České republice. Na základě tematické analýzy vědecké literatury a srovnání se současným legislativním a metodickým rámcem byla identifikována následující klíčová rizika v podobě: nedostatečné personální kapacity, neefektivní využívání investic do bezpečnostních opatření, technologická zastaralost informačních systémů, slabá organizační odpovědnost a přehled o datech, nízká úroveň bezpečnostního povědomí zaměstnanců a izolovaný přístup mezi odbory v rámci úřadů.

Zjištění ukazují, že navrhovaný zákon o kybernetické bezpečnosti se snaží některá rizika částečně zmírnit, zejména prostřednictvím principu přiměřenosti, povinnosti řízení rizik, určení odpovědné osoby a požadavků na školení. Nicméně klíčové překážky, jako je nedostatek kvalifikovaného personálu a neexistence mechanismů pro financování technologické modernizace, zůstávají systémově neřešeny. Vzhledem k dosavadní absenci jednotného mechanismu pro sběr zpětné vazby od obcí by mohlo být přínosné zvážit vytvoření platformy, která by umožnila širší zapojení koncových uživatelů do nastavování a ladění bezpečnostních politik.

Příspěvek dále doporučuje posílení regionální spolupráce (nebo skrz MAS), zavedení participativních konzultačních mechanismů, větší propojení s akademickým sektorem a důsledné vyhodnocování přiměřenosti opatření s ohledem na místní podmínky. Kybernetická bezpečnost obcí by tak měla být chápána nejen jako legislativní povinnost, ale jako klíčová součást důvěryhodného a funkčního výkonu veřejné správy.

Literatura

[1] CARUSON, K., MACMANUS, S., A., MCPHEE, B., D. (2012). "Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success." Journal of Homeland Security and Emergency Management 9 (2): 1–22.

[2] CHOODAKOWSKA, A., KAŃDUŁA, S., PRZYBYLSKA, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. Lex Localis [online]. vol. 20, no. 1, s. 161-192. ISSN 1581-5374.

[3] FUNK, K., COOPER, M., DUPUIS, N., SHARK, A., BOWEN, D. (2019). "Protecting Our Data: What Cities Should Know About Cybersecurity." National League of Cities. https://www.nlc.org/sites/default/files/2019-10/CS%20Cybersecurity%20Report%20Final_0.pdf.

[4] HOSSAIN, S. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences [online]. vol. 14, no. 13, s. 5501.

[5] MASOMBUKA, M., GROBLER, M., DUVENAGE, P. (2021). Cybersecurity and local government: Imperative, challenges and priorities [online]. Reading: Academic Conferences International Limited. 285-293,XIII s. Copyright - Copyright Academic Conferences International Limited Jun 2021; Poslední aktualizace - 2024-06-26.

[6] NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost. (2024, 6. prosince). Kybernetická bezpečnost obcí (verze 1.0). https://portal.nukib.gov.cz/storage/uploads/2025/02/14/podpurny-material_kyberneticka-bezpecnost-obci_uid_6753022f5e89b_uid_67af075214cc3.pdf

[7] NORRIS, D., F., MATECZUN, L., K., FORNO R. (2022). Cybersecurity and local government. Hoboken: Wiley, 2022. ISBN 978-1-119-79806-9.

[8] PREIS, B., SUSSKIND, L. (2020). Municipal Cybersecurity: More Work Needs to be Done. Urban Affairs Review, 58(2), 614–629. https://doi.org/10.1177/1078087420973760

[9] PURSE, R., MATHIESON, D. (2024). Cyber risk: A crucial business issue for municipalities. Municipal World [online]. vol. 134, no. 6, s. 13–14. ISSN 00273589.

# Digitalizace a automatizace ve státní správě a samosprávě: Klíč k efektivitě, transparentnosti a bezpečnosti

Ing. Petr Hamák, senior konzultant, ALVAO

Modernizace a digitalizace jsou nezbytnou součástí rozvoje státní správy, samosprávy a jimi zřizovaných organizací, včetně nemocnic. Automatizace procesů, efektivní řízení workflow, transparentnost a bezpečnost dat jsou klíčové prvky pro zkvalitnění služeb veřejnosti a vnitřní fungování institucí. Bezproblémová správa IT aktiv, efektivní reporting a jasná odpovědnost v rámci jednotlivých organizačních celků jsou dnes nutností.

Právě v těchto procesech hraje důležitou roli česká společnost ALVAO, která nabízí řešení zaměřené na efektivní správu IT a digitálních procesů. Její nástroje ALVAO Service Desk a ALVAO Asset Management pomáhají řídit procesy, propojit data mezi institucemi a poskytovat přehled o správě majetku a odpovědnostech jednotlivých pracovníků. ALVAO je dnes zastoupeno v téměř všech krajích, na krajských a městských úřadech i v rámci ministerstev a jejich organizací.


## Bezpečnost, majetek a NIS2

Kromě efektivity je klíčovou oblastí i bezpečnost a kybernetická ochrana. S příchodem směrnice NIS2 se veškeré veřejné instituce musí přizpůsobit přísnějším bezpečnostním požadavkům, což zahrnuje i řádnou evidenci a správu IT majetku. Právě v tomto směru ALVAO usnadňuje organizacím splnění nových legislativních požadavků díky sofistikovanému řešení správy majetku a jeho ochrany.

ALVAO Asset Management umožňuje jasné evidování hardware i software, sledování licencí a průběžné kontroly souladu s bezpečnostními standardy. Veškeré procesy jsou zdokumentované, což usnadňuje audit a splnění regulatorních požadavků.

## ALVAO v nemocnicích: Klíč k efektivitě a bezpečnosti

Specifickou oblastí, kde ALVAO nachází široké uplatnění, jsou nemocnice. Fakultní nemocnice Brno-Bohunice a Nemocnice Jihlava patří mezi přední uživatele, kteří ocenili přizpůsobení ALVAO požadavkům zdravotnických zařízení. Nemocnice potřebují nejen efektivní řízení IT aktiv, ale také podporu pro servisní požadavky a bezchybný provoz kritických informačních technologií. ALVAO Service Desk pomáhá rychle reagovat na uživatelské požadavky a řídit servisní procesy.


## Microsoft, cloud a nové možnosti

ALVAO je plně integrováno s ekosystémem Microsoftu a funguje jak v on-premise, tak v režimu SaaS (v obou variantách je k dispozici integrace na Copilot). To poskytuje institucím flexibilitu a možnost volby podle jejich potřeb.

Nově byla společnost ALVAO schválena jako oficiální dodavatel v rámci Dynamického nákupního systému č. 3 (DNS 3) spravovaného Digitální a informační agenturou (DIA). To znamená, že veškeré orgány státní správy a samosprávy mohou ALVAO snadno a transparentně pořizovat v rámci tohoto mechanismu.

## AI jako motor efektivní digitalizace

Nedílnou součástí modernizace je využití umělé inteligence (AI), která usnadňuje adopci digitalizačních procesů. ALVAO implementuje AI prvky, které napomáhají automatizaci rutinních úkonů a zrychlují řešení servisních požadavků. Například AI-driven kategorizace ticketů a predikce častých požadavků pomáhají snížit zátěž pro IT oddělení a zkracují čas nutný pro vyřízení požadavků.

## Závěr

ALVAO je české řešení s dlouholetou praxí ve státní správě a samosprávě. Poskytuje nejen efektivní nástroje pro řízení procesů, ale také klíčovou podporu pro kybernetickou bezpečnost a transparentní správu majetku. Vzhledem k neustále se vyvíjejícím legislativním požadavkům a rostoucím nárokům na digitalizaci se ALVAO stává nepostradatelným partnerem pro veškeré organizace ve veřejném sektoru.

www.alvao.cz

# Od eDokladů k EUDIW pro města a obce

Bc. Jiří Hubálek, Město Litoměřice
Mgr. Tomáš Lechner, Ph.D., TRIADA, spol. s r. o

## Úvod

V roce 2021 byl Komisí EU proveden přezkum uplatňování nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, které je označované jako nařízení eIDAS. Jedním ze závěrů bylo, že nařízení nedosáhlo svého potenciálu, pokud jde o účelnost, neboť bylo oznámeno jen omezené množství režimů elektronické identifikace, což omezuje pokrytí občanů EU oznámeným režimem elektronické identifikace. Podle Zprávy Komise Evropskému parlamentu a Radě o hodnocení nařízení eIDAS to bylo v předmětném roce 59 % obyvatelstva EU. V reakci na tento přezkum byla v dubnu loňského roku přijata novelizace nařízení, která zavádí s výhledem do konce roku 2026 evropskou peněženku digitální identity.

Česká republika byla nejen jedna z těch členských států, které v době přezkumu měla svou elektronickou identitu realizovanou, ale navíc se rozhodla ještě v „předvečer" schválení finální podoby novelizace nařízení, tedy v době, kdy se o něm několik let diskutovalo, vytvořit vlastní řešení, které má některé rysy společné s plánovanou evropskou peněženku digitální identity a může by tak být chápáno jako jistá „rozcvička" pro aplikaci tohoto evropského nástroje. Digitální a informační agentura, která tento projekt zastřešuje, eDoklady i tímto způsobem také představila v rámci předchozího ročníku konference ISSS (viz [1]).

V tomto příspěvku si ukážeme praktický příklad realizace eDokladů a jejich užití na městském úřadě právě s výhledem na budoucí evropskou peněženku digitální identity.

## Možnosti použití eDokladů

Povinné uznávání digitálního stejnopisu občanského průkazu uloženého v aplikaci eDoklady platí pro všechny městské a obecní úřady od 1. ledna letošního roku. Obce s rozšířenou působností měly tuto povinnost již o 6 měsíců dříve. Nutno poznamenat, že obecně v praxi procesů, které jsou vykonávány městskými a obecními úřady, není zase tolik případů, kdy je vyžadována identifikace jednající osoby prostřednictvím občanského průkazu. A pokud ano, pak se většinou jedná o výkon přenesené působnosti státní správy. Z toho pohledu byl také vybrán pro tuto studii případ obce s rozšířenou působností, která vykonává nejširší rozsah přenesené působnosti.

Použití prokazování digitálním stejnopisem občanského průkazu je striktně vymezeno na fyzické ověřování, tedy na případy, kdy lze také použít klasickou plastovou kartičku občanského průkazu. Nové přístupy tedy nerozšiřují možnosti do online prostoru a využití digitálních služeb, kde je k prokázání totožnosti třeba využití elektronické identifikace zavedené zákonem č. 250/2017 Sb., o elektronické identifikaci, tedy prostřednictvím kvalifikovaného systému elektronické identifikace, ale přidávají alternativní postupy do klasického fyzického ověřování.

Ověřovaná osoba má tedy na výběr, buď použít svůj klasických občanský průkaz v podobě plastové kartičky, nebo použít k prokázání digitální stejnopis občanského průkazu uložený v aplikaci eDoklady na svém mobilním telefonu. Oba postupy prokázání totožnosti jsou z legislativního hlediska stejné, i když po procesní stránce je vhodné zmínit dva významné rozdíly. Tím nejdůležitějším je lepší aplikování principu minimalizace dat z pohledu ochrany osobních údajů. V rámci prokázání totožnosti pomocí digitálního stejnopisu občanského průkazu uloženého v aplikaci eDoklady jsou ověřující straně poskytovány pouze ty údaje, které jsou pro daný typ a proces nezbytné.

Druhým procesním rozdílem pro uživatele aplikace eDoklady je kromě novodobého zvyku nosit s sebou všude mobilní telefon, a tím si zajistit, že automaticky mám takto vždy s sebou dostupný i občanský průkaz, to, že v aplikaci vzniká každým ověřením

historie těchto aktů, čím je možné s určitou mírou důkazní spolehlivosti zpětně prokázat, že k poskytnutí potřebných informací ze strany ověřované osoby skutečně došlo.

Pro ověřující osobu je procesních změn více, neboť kontrola digitálního stejnopisu občanského průkazu neprobíhá pouze vizuálně, jako u plastové kartičky, ale je podložena přenosem dat. Znamená to jednak přípravu technického zajištění tohoto přenosu a jednak zaškolení uživatelů, jak tento přenos realizovat. Digitální a informační agentura připravila dvě možnosti vlastní technické realizace [2]:

- Komunikace dvou mobilních telefonů s přenosem pomocí Bluetooth komunikace, což je vhodné zejména pro použití v terénu, např. při místních šetřeních.
- Komunikace mobilního telefonu ověřované osoby s webovou aplikací ověřovatele, což je vhodné zejména při ověřování na přepážkách, protože webová aplikace dává možnost dalšího zpracování dat.

## Evropská peněženka digitální identity

Evropskou peněženkou digitální identity se podle čl. 3 odst. 42 nařízení eIDAS rozumí prostředek pro elektronickou identifikaci, který uživateli umožňuje bezpečně ukládat, spravovat a ověřovat osobní identifikační údaje a elektronická potvrzení atributů za účelem jejich poskytnutí spoléhajícím se stranám a dalším uživatelům evropských peněženek digitální identity a podepisovat prostřednictvím kvalifikovaných elektronických podpisů nebo pečetit prostřednictvím kvalifikovaných elektronických pečetí. Z pohledu elektronické identifikace půjde o prostředek na vysoké úrovni záruky, což znamená nejširší možnosti použití.

Primárně je tedy tento prostředek směrován do online prostoru, nicméně jeho využití má být dle čl. 5a odst. 4 písm. a) použitelná i v off-line režimu s cílem přistupovat k veřejným a soukromým službám, přičemž má být zajištěna možnost výběrového zpřístupňování údajů. Právě v tomto off-line použití se potkává procesní podobnost eDokladů s budoucí evropskou peněženkou. Avšak celkově budou možnosti použití evropské peněženky pro uživatele mnohem širší a bohatší, a to zejména o možnost elektronického potvrzování atributů. Nepůjde tak jen o pouhé prokázání totožnosti, ale též o prokázání dalších právních skutečností, např. dosaženého vzdělání nebo získaného osvědčení.

Evropská komise k tomu přijala 28. listopadu 2025 pět prováděcích aktů:

- Prováděcí nařízení Komise (EU) 2024/2979 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce evropských peněženek digitální identity
- Prováděcí nařízení Komise (EU) 2024/2982 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhra-ní, které mají být podporovány evropským rámcem pro digitální identitu
- Prováděcí nařízení Komise (EU) 2024/2977 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o osobní identifikač-ní údaje a elektronická potvrzení atributů vydávané k evropským peněženkám digitální identity
- Prováděcí nařízení Komise (EU) 2024/2981 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o certifikaci evrop-ských peněženek digitální identity
- Prováděcí nařízení Komise (EU) 2024/2980 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o oznámení Komisi týkající se evropských peněženek digitální identity

Platí, že do 24 měsíců ode dne vstupu uvedených prováděcích aktů v platnost (dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie, které je datované k 4. prosinci 2024) poskytne každý členský stát svým občanům alespoň jednu evropskou peněženku digitální identity. Výsledným milníkem je tedy 24. prosinec 2026, což rozhodně není termín nikterak vzdálený. A proto je velmi dobře, pokud jsou přípravné kroky realizovány včas s dostatečným předstihem.

## eDoklady v Litoměřicích

Město Litoměřice patři mezi obce s rozšířenou působností. Městský úřad se skládá z 13 odborů a 5 útvarů, na kterých pracuje celkem 204 úředníků. Před zavedením ověřování pomocí eDokladů jsme provedli analýzu potřeb, z níž jsme primárně vyloučili volební agendu, kterou jsme řešili až následně samostatně, protože pro volební komise byla povinnost přijímat eDoklady nastavena až od 1. ledna 2025.

Projekt zavedení eDokladů jsme si rozdělili do čtyř částí:

- Analýza požadavků odborů na ověřování občanského průkazu
- Technické řešení zahrnující instalaci a nastavení
- Zaškolení uživatelů
- Ověření provozu

V první fázi jsme oslovili všechny odbory z hlediska jejich potřeb pro ověřování. Šlo jednak o konkrétní procesy, v nichž je třeba ověření totožnosti občana, a jednak o počty uživatelů. U procesů bylo důležité rozhodnout, který z technických způsobů řešení bude vyžadovat. Zda ověření pomocí mobilní aplikace eDoklady, nebo před webovou čtečku. Z analýzy vyplynulo, že téměř na všech odborech jsou kombinovány obě možnosti. Detailní výsledky jsou shrnuty v Tab. 1.

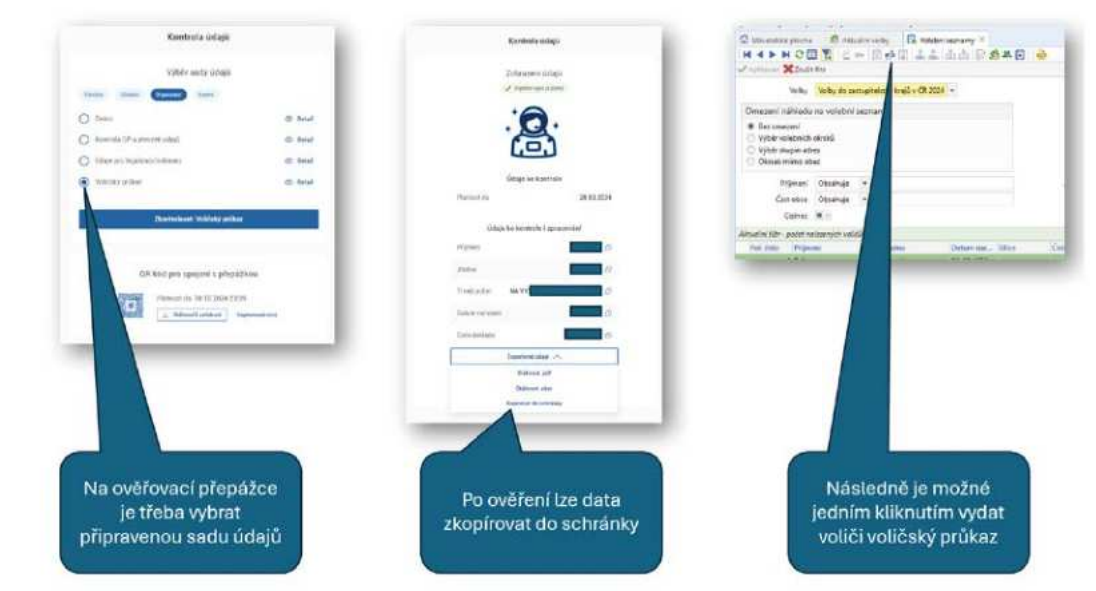
| Způsob ověřování | Počet zařízení/přístupů | Konkrétní odbory, kde je využito |
|---|---|---|
| Mobilní zařízení | 44 | SÚ; OŽÚ; OŽP; OSVaZ; OS; ODaSH; MP |
| Webová aplikace | 83 | SÚ; OŽÚ; OŽP; OŠKSaPP; OS; OE; OSaSH; KSaT; MP |

*Tab. 1. Výsledky analýzy potřeb ověřování eDokladů*

Poté jsme se přihlásili do ověřování a nastavili přístupové role pro jednotlivé uživatele v prostředí JIP/KAAS. Následovala instalace aplikací na služební mobilní telefony a jejich nastavení. Dále byly připraveny virtuální přepážky pro ověřování přes webovou aplikaci. Každý postup jsme primárně odzkoušeli. Na lokálních stanicích jsme rovněž ověřili přihlášení uživatelů a generování QR kódů pro přepážky.

Důležitou a podstatnou součástí projektu zavedení eDokladů na městském úřadě bylo zaškolení všech uživatelů, po kterém následovalo ověření provozu tak, abychom k 1. červenci 2024 byli plně připraveni, až k nám přijde první občan, který se bude chtít prokázat eDokladem.

Jak došlo následně k rozšíření možností přenosu údajů z webové aplikace, vytipovali jsme ve spolupráci s dodavatelem informačního systému procesy, kde by bylo výhodné využití tohoto přenosu údajů z webové aplikace do informačního systému. Nejčastějším případem se ukázalo ověřování, tedy legalizace podpisu a vidimace listin. Mezi další případy patří vydávání voličských průkazů, které je ilustrováno na Obr. 1.




*Obr. 1. Ukázka procesu vydání voličského průkazu s podporou eDokladů.*

Po devíti měsících máme zkušenosti, že použití eDokladů ze strany občanů je zatím v menšině. Celkový počet ověření za tuto dobu jsou nižší desítky. Nejčastěji jsou využity na odboru dopravy na úseku řidičských průkazů a vozidel. Očekáváme však, že situace se výrazně změní v rámci podzimních voleb do Poslanecké sněmovny Parlamentu ČR.

## Shrnutí

Pro ověřování eDokladů využíváme na našem úřadu oba přístupy, tedy jak mobilní aplikaci, tak webovou čtečku. Pro úředníky, kteří se pohybují v terénu při kontrolních dnech jsou využívány služební mobilní telefony s mobilní aplikací eDoklady. U tohoto způsobu ověření dokladu oceňujeme zejména možnost pohodlného a rychlého použití, ověření v offline režimu a sdílení údajů přes QR kód. Pro úředníky, kteří využívají na úřadě webovou verzi eDokladů, velmi oceňujeme jednoduchý přístup bez instalace aplikace a pro celkovou efektivitu pak následnou možnost přenosu údajů do IS Munis. Jak už bylo řečeno, tak počítáme s tím, že podzimní volby do Poslanecké sněmovny Parlamentu ČR budou dalším impulzem pro občany, aby této možnosti prokázání totožnosti využili.

Z pohledu přípravy na budoucí evropskou peněženku digitální identity jsme si odzkoušeli realizaci projektu, který má z uživatelského pohledu obdobné parametry. Byť u nás nakonec převažuje řešení přes webovou aplikaci, jejíž důležitou předností je variantní možnost následného použití dat, které snižuje chybovost a zvyšuje efektivitu procesů, ale které zřejmě není tím způsobem, jakým bude možné pracovat s evropskou peněženku digitální identity. Nicméně máme nemálo instalací mobilní aplikace, kde lze očekávat, že po uživatelské stránce bude budoucí evropský nástroj podobný. Znamená to, že až tento nástroj přijde, nebudou z jeho použití mít naši úředníci obavy a jeho zavedení tak bude z tohoto úhlu pohledu určitě jednodušší. Z technického úhlu pohledu nelze zatím nic konkrétního předjímat.

Literatura

[1] Blok Digitální a informační agentury na konferenci ISSS 2024. Dostupné na <https://2024.isss.cz/program/?den=2024-05-14#kalendar>.

[2] HRACH, Z. EDoklady a ověřovatelé. Dostupné na <https://archiv.isss.cz/archiv/2024/download/prezentace/dia_hrach.pdf>.

# Elektronická spisová služba má smysl

Bc. Kateřina Hůlková, Petr Laštovička, Městský úřad Červený Kostelec
Mgr. Tomáš Lechner, Ph.D., TRIADA, spol. s r. o

## Od listinné k elektronické spisové službě

Spisová služba je definována zákonem č. 499/2004 Sb., o archivnictví a spisové službě, jako odborná správa dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností. V roce 2009, když byly zavedeny datové schránky, které významným způsobem akcelerovaly užívání elektronických dokumentů ve veřejné správě, byl ruku v ruce s tím zaveden výkon spisové služby v elektronické podobě v elektronickém systému spisové služby. Pravidla po fungování tohoto nástroje jsou definována primárně citovaným zákonem, dále prováděcí vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby, a v neposlední řadě Národním standardem pro elektronické systémy spisové služby.

Posun od listinné k elektronické spisové službě nelze spatřovat jen ve změně formy, ale zároveň ve významné úpravě procesního základu. Znamená to, že elektronický systém spisové služby se netýká jen finálního produktu procesů v podobě dokumentů, ale též samotných procesů tvorby těchto dokumentů. To, že jde z pohledu spisové služby o nově integrovanou oblast, lze doložit i na poměrně překotném vývoji názvosloví. Entitě, která ještě není dokumentem, se v roce 2009 podle první verze národního standardu říkalo záznam, následně v roce 2017 byla přejmenována na koncept. V této souvislosti lze přímo citovat z národního standardu zveřejněném ve věstníku Ministerstva vnitra čá. 57/2017:

„Mezi další významné změny patří odstranění pojmu záznam a zavedení pojmu koncept (rozpracovaný dokument), který je spravován v elektronickém systému spisové služby shodně jako dokument, avšak může existovat ve více verzích a nemusí být evidován v evidenci dokumentů."

Pod tlakem definice elektronického dokumentu v nařízení eIDAS byl nakonec v roce 2023 opuštěn i pojem koncept. Opět doložíme citací z národního standardu zveřejněném ve věstníku Ministerstva vnitra čá. 42/2023:

„Další koncepční změnou s dopadem na požadavky národního standardu je opuštění pojmu rozpracovaného dokumentu (konceptu) a jeho nahrazení povinnou tvorbou a ukládáním verzí všech komponent dokumentu po celou dobu jeho životního cyklu v rámci elektronického systému spisové služby."

Původní přístup ke spisové službě jen jako evidenci závěrečných výsledků procesů lze stále ještě najít například ve správním řádu, který v § 17 odst. 4, jenž se týká spisu, stanoví, že nevykonává-li příslušný správní orgán spisovou službu, předá spis po právní moci rozhodnutí správnímu orgánu, který pro něj spisovou službu vykonává. To by se dalo zjednodušeně chápat tak, že z pohledu správního řádu, je spisová služba důležitá, až když spis nabyde právní moci. Opak je však v současné době pravdou. Elektronická spisová služba se proplétá všemi činnostmi, které orgány veřejné moci vykonávají. A s tím se dostává do konfliktu snaha o unifikaci procesů napříč všemi organizacemi veřejné správy, kterou představuje zejména národní standard, a různorodost procesních předpisů v podobě správního řádu, daňového řádu, soudního řádu správního atd.

Bohužel jsme, možná i kvůli tomu, v poslední době svědky různých výjimek z povinností spisové služby, jako např. ve školském zákoně (§ 62 odst. 5 školského zákona stanoví, že národní standard pro elektronické systémy spisové služby se na informační systém o přijímacím řízení, kromě transakčního protokolu, nepoužije) nebo v zákoně č. 326/2021 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronizaci zdravotnictví, a který vyjmul ze spisové služby vedení zdravotnické dokumentace.

Otázkou je, proč se tak děje a proč si spisová služba drží určitý punc strašáku, kterému se všichni snaží spíše vyhnout, místo toho, aby využili její služby a výhody pro správu elektronických dokumentů, pro které dokáže zajistit věrohodnost původu dokumentů, neporušitelnost jejich obsahu a čitelnost, tvorbu a správu metadat náležejících k těmto dokumentům a připojení údajů prokazujících existenci dokumentu v čase.

## Elektronická spisová služba Munis ERMS jako součást informačního systému Munis

Abychom mohli odpovědět položenou otázku, můžeme se podívat na příklad uceleného informačního systému, jehož součástí je také modul spisové služby. Jde o informační systém Munis, jehož tvůrcem i dodavatelem je společnost Triada. Elektronický systém spisové služby Munis ERMS zajišťuje veškeré etapy výkonu spisové služby od příjmu, přes evidenci, rozdělování, oběh a vyřizování s vytvářením spisů, vyhotovování vlastních dokumentů, jejich podepisování a ztvárnění ve výstupním datovém formátu, odesílání, ukládání ve spisovně a vyřazování ve skartačním řízení, tedy vše co vyžaduje zákon č. 499/2004 Sb., o archivnictví a spisové službě, dále upřesněný prováděcí vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

Pro uživatelskou přehlednost a komfort je modul rozdělen do několika funkčních aplikačních částí, jejichž přehled je na Obr. 1. Po licenční stránce se ale jedná o jednotný celek, který nabízí všechny potřebné funkcionality pro celý životní cyklus dokumentu i pro procesní záležitosti tvorby spisů.


*Obr. 1: Aplikace, které dohromady tvoří elektronický systém spisové služby Munis ERMS.*

Elektronická spisová služba se stala vhodným a výhodným místem pro uložení elektronických dokumentů vznikajících v organizacích veřejné správy a zároveň užitečným konektorem, který organizace spojuje s centrálními nástroji e-Governmentu, jako jsou například datové schránky. Kromě toho efektivně pomáhá s vlastní tvorbou dokumentů, byť v těchto případech může být schována na pozadí. Národní standard pro elektronické systémy spisové služby definuje v kapitole 8.1 Vazby mezi informačními systémy spravujícími dokumenty rozhraní, které umožňuje pomocí synchronní i asynchronní komunikace, přenos metadat entit i obsahu elektronických dokumentů mezi informačními systémy spravujícími dokumenty původce. Toto rozhraní je realizováno prostřednictvím webových služeb a schémat XSD uvedených v příloze č. 1 k tomuto standardu. Standardizace tohoto rozhraní významně přispěla k posílení role spisové služby jako páteřní agendy.

Nad rámec tohoto standardu lze využívat v souladu s požadavkem 8.1.32 ještě další doplňující informace, jejichž výčet a rozsah následného užití závisí na implementaci rozhraní mezi elektronickým systémem spisové služby a informačním systémem spravujícím dokumenty. Kromě toho mají ucelené informační systémy další možnost využití pevnějších vazeb na základě požadavku č. 2.9.1 národního standardu pro elektronické systémy spisové služby, který zní [3]: „Je-li samostatná evidence dokumentů napojena na eSSL, musí tak být realizováno rozhraním podle kapitoly 8.1, jehož prostřednictvím samostatná evidence dokumentů zajišťuje správu entit v eSSL, není-li jiný způsob napojení efektivnější." V rámci uceleného informačního systému lze tedy využít i další efektivnější vazby, které podporují uživatelský komfort a sdílení informací.

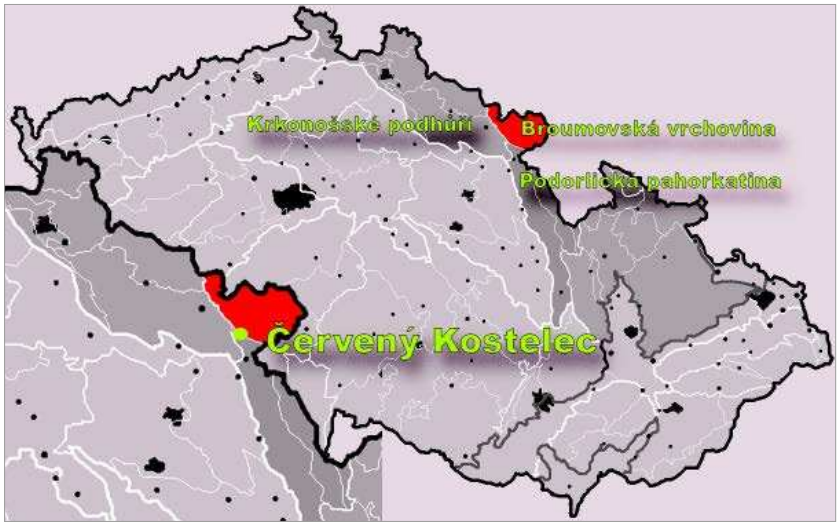
Z uvedeného jasně plyne, že využití elektronické spisové služby v rámci uceleného informačního systému je výhodné. Proč je tedy často přístup uživatelů odmítavý a proč se objevují výše zmíněné výjimky v předpisech? Dle zkušeností z různých organizací lze důvody zřejmě shrnout do následujících bodů:

1. Přetrvávající pocit, že spisová služba je stále jen místo pro evidenci výstupů z procesů, ruku v ruce s podceňováním důležitosti role archivnictví v uchovávání informací. Jedinou cestou pro překonání tohoto omezeného pohledu je osvěta a školení.
2. Vyhýbání se elektronizaci procesů ve smyslu toho, že stejně se nakonec všechno vytiskne, takže vlastně není třeba implementovat nástroje pro zajištění správy elektronických dokumentů. Tlak na změnu tohoto přístupu je nedílnou součástí celého rozvoje e-Governmentu a významným způsobem jej lze najít v mnoha předpisech, včetně nařízení eIDAS, nebo zákonu č. 12/2020 Sb., o právu na digitální služby.
3. Celková složitost legislativního popisu spisové služby, kterou lze doložit i tím, jak dlouho se diskutuje nad rozborem pravidel pro atestaci elektronických systémů spisové služby a kolik vysvětlujících stanovisek již bylo k tomuto tématu vydáno Ministerstvem vnitra [4].
4. Absence podpory vedení organizací, které mají ve zvyku výkon spisové služby stejně jako důležitost kvalitní elektronizace procesů podceňovat. Jinými slovy, je třeba si uvědomit, že elektronizace a digitalizace není jen záležitost IT odborů, ale otázkou celkového fungování organizace. Obdobný posun ve vnímání problematiky elektronizace lze spatřovat při implementaci směrnice NIS2 pro oblast kybernetické bezpečnosti, kde je stanovena odpovědnost řídících orgánů a výkonných ředitelů [viz např. čl. 20 a čl. 32 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)].

## Využití elektronické spisové služby městským úřadem Červený Kostelec

Když jsme si takto přiblížili problémy, se kterými se užívání elektronické spisové služby v organizaci potýká, pojďme si ukázat příklad dobré praxe, z něhož je vidět, že jde tyto překážky překonat, když se chce. Ilustrovat to budeme na příkladu městského úřadu Červený Kostelec, který využívá informační systém Munis včetně elektronické spisové služby Munis ERMS již řadu let.

Město Červený Kostelec leží v Královéhradeckém kraji, zhruba 10 km na severovýchod od Náchoda (viz poloha města na Obr. 2). Město leží v nadmořské výšce přibližně od 315 m n. m. až po cca 598 m n. m. Podle posledního geomorfologického členění tvoří trojmezný bod mezi Broumovskou vrchovinou, Podorlickou pahorkatinou a Krkonošským podhůřím. V současnosti nese označení Červenokostelcká pahorkatina [2]. Pohled na město ilustruje Obr. 3.




*Obr. 2: Poloha města na území ČR.*

Městský úřad Červený Kostelec se skládá z osmi odborů a vedení města. Uvedené odbory jsou Správní odbor, Finanční odbor, Odbor výstavby a životního prostředí, Sociální odbor, Odbor rozvoje města, Majetkový odbor, Odbor informatiky a Odbor místního hospodářství. Výkonem přenesené působnosti je Červený Kostelec zařazen mezi obce s pověřeným obecním úřadem, tedy obec II. typu. Blíže viz [1].

Z modulů informačního systému Munis se na úřadě využívají moduly elektronická spisová služba Munis ERMS, Seznam obyvatel a volby, Katastr nemovitostí, Matrika, Munizar Plus, Legalizace a vidimace, Úřední deska a eDeska, Majetek, Účetnictví a rozpočet, Pokladna, Platební karty, Poplatky, Komunální odpad, Evidence hřbitova, Manažerská nadstavba, Výkazy DPH, Fakturace ASM a Bankovní služby ASM, Rozpočet Plus, Konektor na datových sklad a tím samozřejmě i vlastní Datový sklad Munis.


*Obr. 3: Město Červený Kostelec v průběhu ročních období, foto: Ing. Jaroslav Kordina.*

Na městském úřadě Červený Kostelec pracuje okolo 60 zaměstnanců. Všichni aktivně pracují s elektronickým systémem spisové služby, ať již napřímo, nebo prostřednictvím vazby realizované na základě principů stanovených národním standardem. Jedním z přístupů, který podporuje začlenění výkonu spisové služby do rutinních procesů, je snaha o jednotnost pravidel, což

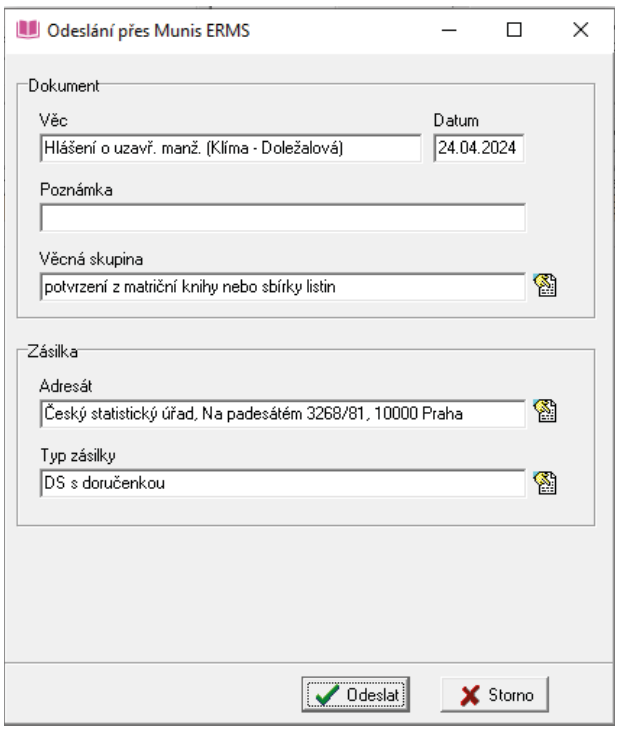
znamená, že všechny oprávněné úřední osoby, které smí podepisovat dokumenty v listinné podobě, mají zároveň token s kvalifikovaným certifikátem pro elektronický podpis, který jim umožňuje vytvářet kvalifikované elektronické podpisy v souladu s nařízením eIDAS a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Dalším důležitým prvkem je pravidelné proškolování a doškolování zaměstnanců, které většinou provádí přímo pracovníci dodavatele spisové služby.

Rozsah výkonu spisové služby ilustruje velmi dobře následující tabulka, která uvádí počty čísel jednacích za posledních pět let:

| Rok | Počet ČJ |
|---|---|
| 2020 | 7 724 |
| 2021 | 8 180 |
| 2022 | 10 203 |
| 2023 | 8 552 |
| 2024 | 7 499 |

*Tab. 1. Počet čísel jednacích za posledních pět let.*

Efektivní zapojení spisové služby do procesů je významně podpořeno také vhodnými vazbami, které jednak umožňují při výkonu konkrétních agend automatické zapojení spisové služby v podstatě na pozadí, tj. tak, že uživatel nemusí explicitně spisovou službu spouštět, a jednak zjednodušují celkovou tvorbu dokumentů. Do první zmíněné oblasti patří zejména vazba na agendy přestupků či stavebního úřadu dodávané společností VitaSW. Příkladem druhé oblasti může být vazba na modul Matrika, kde je vytvářeno hlášení pro Český statistický úřad (Obr. 4). Po vytvoření v modulu Matrika je hlášení automaticky zaevidováno ve spisové službě a následně odesláno přes datovou schránku. Byť se to může zdát jako drobnost, tak každé takové ulehčení práce znamená nejen vyšší komfort pro uživatele, ale také úsporu času, která se při opakovaných akcích pozitivně projeví na celkové výkonnosti úřadu.




*Obr. 4: Ukázka odeslání hlášení z modulu Matrika přes elektronickou spisovou službu Munis ERMS.*

V neposlední řadě je třeba vyzdvihnout trvalou a významnou podporu vedení, které si je vědomo důležitosti agendy spisové služby a jejího zapojení v elektronické podobě do celkové elektronizace a digitalizace úřadu. To znamená též zapojení portálového řešení, které je možné napojit na Datový sklad Munis, a z toho také plyne zodpovědný přístup úřadu k nabídce digitálních služeb de zákona č. 12/2020 Sb., o právu na digitální služby.

Díky kvalitnímu vedení spisové služby úřad již realizoval elektronická skartační řízení, v nichž jsme předali, jak vyřízené dokumenty, tak uzavřené spisy. Veškeré úkony, včetně generování SIP balíčků, proběhly bez jakýchkoli komplikací. Aplikace Spisovna, které je součástí elektronické spisové služby Munis ERMS, jasně a přehledně provede všemi kroky. I když se primárně skartační řízení zdá složité z důvodu více kroků a návaznosti Národního portálu, tak následně při dostatečné znalosti metodiky a správném zaškolení nepředstavuje provedení skartačního řízení zásadní problém. K tomu byla velmi přínosná nabídka společnosti Triada účastnit se školení přímo na počítačích (PC kurzu), které umožnilo praktické vyzkoušení celého procesu skartačního řízení přímo na počítači. K tomu společnost Triada nabízí také online kurzy na doplnění získaných dovedností.

Počty zařazených entit v jednotlivých skartačních řízení ukazuje Tab. 2. Poslední zmíněné řízení je ve fázi podaného skartačního návrhu a čekáme nyní na odpověď oblastního archivu.

| **Datum zahájení přípravy skartačního řízení** | **Počet vložených dokumentů** | **Počet vložených spisů** | **Stav řízení** |
|---|---|---|---|
| 17. 6. 2024 | 0 | 146 | Plně dokončeno |
| 10. 3. 2025 | 1795 | 0 | Podán skartační návrh |
| 24. 3. 2025 | 130 | 17 | Plně dokončeno |

*Tab. 2. Základní charakteristika provedených elektronických skartačních řízení*

Uživatelé práci v elektronické spisové službě Munis ERMS včetně aplikace Spisovna hodní pozitivně, což je také jeden z důležitých předpokladů celkového úspěchu v řádném vedení spisové služby na městském úřadě.

Literatura

[1] Oficiální webové stránky města Červený Kostelec, dostupné na https://www.cervenykostelec.cz/

[2] Wikipedia s heslem Červenokostelecká pahorkatina, dostupné na https://cs.wikipedia.org/wiki/%C4%8Cervenokosteleck%C3%A1_pahorkatina

[3] MINISTERSTVO VNITRA. Národní standard pro elektronické systémy spisové služby. Věstník Ministerstva vnitra, částka 42/2023.

[4] MINISTERSTVO VNITRA. Metodiky k výkonu spisové služby v elektronických systémech spisové služby, dostupné na https://mv.gov.cz/clanek/spisova-sluzba-metodiky.aspx.

# Co mělo být a není, aneb jak toho využít

Mgr. Ing. Václav Lukavský, ATS-TELCOM PRAHA, a.s.

*Moto:*

*I přes to, že dosud není zákon, mohou firmy bez problému zpracovávat bezpečnostní dokumentaci podle ještě stále platných předpisů a neudělají žádnou chybu.*

Tak jak již bylo mnohokrát konstatováno, ať již na odborných fórech nebo v mediálním prostoru, hrozby napadení kybernetickým útokem neustále rostou. A to nejen na kritickou infrastrukturu, ale i na všechny, mnohdy zdánlivě nezajímavé, ostatní části kybernetického prostoru.

Je proto zcela jednoznačně zřejmé, že všichni provozovatelé a uživatelé elektronických systémů musí svá aktiva účinně bránit. Jak jsme si již řekli na minulém ISSS, je zde několik úrovní zajištění kybernetické bezpečnosti, a nepochybně jednou z těchto úrovní je zpracování „bezpečnostních pravidel", což znamená vytvoření bezpečnostní dokumentace v souladu s požadavky státu jako celku a její následné rozpracování na konkrétní podmínky jednotlivých orgánů nebo organizací.

## Jaká jsou ta „bezpečnostní pravidla"

Pokud chce stát regulovat oblast kybernetické bezpečnosti, musí pro to vytvořit „**Návod k upotřebení**". Tímto návodem je myšlen nejen příslušný právní předpis (nový zákon o kybernetické bezpečnosti - NZKB) a jeho prováděcí vyhlášky, ale měly by být vytvořeny také příslušné vzorové dokumenty, sloužící k snazší orientaci v plnění zadávaných povinností. V této oblasti však již nelze, vzhledem k rozsáhlosti a komplexnosti opatření, ukládat povinnosti uzavřeně v intencích jednotlivých států, ale v rámci sjednocení „bezpečnostních pravidel" se musíme řídit nadnárodním právním předpisem. Tímto předpisem je směrnice evropského parlamentu a Rady (EU) 2022/2555, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), ze dne 14. prosince 2022. Z logiky věci nám vychází po krátkém propočtu, že před NIS 2 byla směrnice NIS 1. Takže z hlediska regulace se relativně neděje nic extra nového.

Až potud jsme všichni pouhými diváky a sledujeme, jak se nám ten legislativní proces vyvíjí. Ale pozor, až skončí proces národního rozpracování směrnice NIS 2 na právní předpis (NZKB) včetně prováděcích předpisů, bude již na pomyslném semaforu svítit nejméně oranžová s dodatkovou tabulkou „*Začíná být pozdě*".

## Tak jak se na toto mohu připravit?

Jednoduše. Nečekat na finální (platnou) verzi připravovaného NZKB, ale aktualizovat tam, kde je již bezpečnostní dokumentace zpracována, nebo zahájit přípravné práce na zpracování aktuální bezpečnostní dokumentace, a to vše za tichého, ale bedlivého dohledu stávajících, ale stále ještě platných právních předpisů.

Tam kde bude možné „se opřít" o platnou, funkční bezpečnostní dokumentaci, tam bude celý proces přechodu na nový zákon jednodušší, jelikož zákon není revolucí v oblasti kybernetické bezpečnosti, ale evolučním procesem s očekávanými změnami.

**POKUD BUDEME TAKTO POSTUPOVAT, URČITĚ NEBUDE NAŠE ČINNOST ZBYTEČNÁ, NAOPAK BUDEME MÍT VELMI DOBROU STARTOVACÍ POZICI NA PŘECHOD POD NOVÝ ZÁKON REFLEKTUJÍCÍ POŽADAVKY NIS 2.**

# „Chytré oči v terénu“ – Videopřenosy pro moderní krizové řízení

Ing. Olga Jedličková, Business Development & CFO, Smart Informatics s.r.o.

## Když sekundy rozhodují

Ve chvílích, kdy rozhodují sekundy, je každá informace klíčová. Ať už jde o hasiče zasahující u požáru, zdravotníky poskytující první pomoc, techniky řešící výpadek infrastruktury nebo policejní či armádní velení. Pro všechna tato nasazení je klíčové mít aktuální vizuální informace přímo z místa události. Tradiční hlasová komunikace a statické snímky často nestačí.

Možnost přenášet aktuální obraz z terénu v reálném čase znamená lepší rozhodování, koordinaci i bezpečnost. Společnost Smart Informatics přináší řešení postavené na technologii LiveU – původně vyvinuté pro televizní živé přenosy a zpravodajské vstupy, která se dnes uplatňuje také v podmínkách složek IZS, armády či telemedicíny. Technologie izraelské společnosti LiveU umožňuje spolehlivý a bezpečný přenos obrazu a zvuku odkudkoli – včetně náročných podmínek, kde není dostupná klasická síťová infrastruktura.

Moderní technologie tohoto typu mění způsob komunikace a spolupráce. Pomáhá rychleji se rozhodovat, předcházet rizikům, šetřit čas i zdroje. Připojení kamery na helmě, robopsu, dronu, videa z mobilního telefonu přímo k dispečinku znamená, že každý člen týmu – ať už je v terénu nebo na základně – vidí stejný obraz a může ihned reagovat. A co víc – přináší i nové možnosti vzdáleného školení, dokumentace, bezpečnostní analýzy nebo krizového rozhodování.

## Konektivita odkudkoli, kdykoli, za všech okolností

Základem systému je datový bonding – propojení různých typů konektivity (pevné připojení, 4G/5G od více operátorů, Wi-Fi, satelitní Starlink) do jednoho stabilního a širokopásmového datového toku. Díky tomu je možné dosáhnout vysoké kvality přenosu i v prostředích, kde klasická konektivita selhává. Technologie bondingu navíc zajišťuje automatické přepínání mezi sítěmi bez přerušení přenosu.

Klíčovým prvkem je patentovaný přenosový protokol LRT™ (LiveU Reliable Transport), speciálně navržený pro zvýšení spolehlivosti přenosu videa přes bezdrátové sítě, který umožňuje nízkou latenci, vysokou odolnost vůči výpadkům a šifrovaný přenos. Pro záchranáře nebo techniky v terénu to znamená, že jejich obraz i zvuk dorazí do dispečinku spolehlivě a téměř okamžitě.

## Kromě spolehlivosti přináší technologie LiveU další klíčové výhody:

- **Nízká latence:** LiveU minimalizuje zpoždění mezi pořízením záznamu a jeho přenosem, čímž poskytuje takřka okamžitý přehled o situaci. Díky latenci pod jednu sekundu lze živé přenosy sledovat na jednotné platformě na dispečinku i bezpečně na mobilních a přenosných zařízeních připojených k internetu. To je klíčové v rychle se měnících situacích, kde je okamžitá reakce zásadní.
- **Snadné použití:** Plug & go. Řešení je navrženo s důrazem na jednoduchost a rychlé nasazení. V kritických situacích je zásadní, aby bylo vybavení možné aktivovat rychle a bezchybně i méně technicky zkušeným personálem. Možnost vzdáleného zapnutí zařízení z dispečinku.
- **Živý přenos z jakéhokoli zdroje:** LiveU umožňuje spolehlivě přenášet video a data z různých zařízení – od bezpilotních prostředků (UAS), pozemních robotů (UGV), vrtulníků až po palubní kamery ve vozidlech. Enkodér LiveU lze snadno připojit ke zdroji a během několika kroků zahájit přenos zvuku i obrazu v reálném čase.

- **Mobilní konektivita pro vše:** Přenosné jednotky LiveU podporují nejen IP přenos videa, ale i dat a souborů, čímž představují komplexní řešení pro mobilní komunikaci v terénu.

## Terénní jednotka LU-REQON1 – Oči upřené na misi, ne na technologii

Nemusíte se starat o složité nastavení – stačí připojit libovolný video zdroj a okamžitě sdílet obraz. Ať už používáte dron, bezpečnostní kameru, robopsa s kamerou nebo vozidlo s osádkou či bez ní, jednoduše připojte jakékoli IP nebo HDMI zařízení k jednotce LU-REQON1™ a začněte přenášet obraz do zvoleného cílového místa. Jednotku lze také zapnout z dispečinku na dálku.

Lehká a přenosná jednotka váží pouhých 955 gramů a je navržena pro nasazení v pohybu. Součástí je taktická brašna kompatibilní se systémem MOLLE, díky čemuž je LU-REQON1™ připraven do jakékoliv akce.

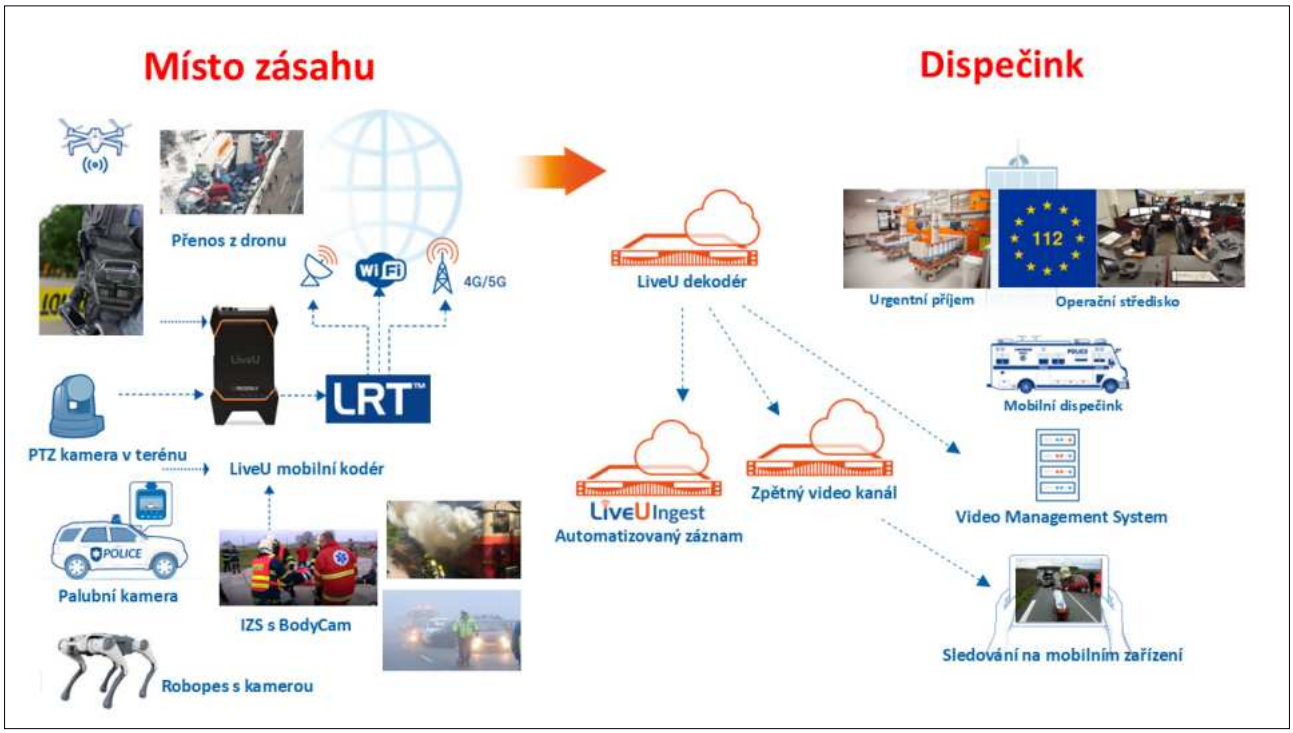

## Situační přehled v praxi: jak technologie LiveU pomáhá chránit lidi i infrastrukturu

Integrace mobilní přenosové technologie LiveU s autonomními drony výrazně zvyšuje situační přehled v reálném čase, a to jak při operacích zaměřených na ochranu obyvatelstva, tak v rámci pokročilých průmyslových scénářů. Následující příklady ilustrují praktické nasazení této kombinace.

## Ochrana obyvatelstva

- Dopravní nehody: Představme si hromadnou nehodu na dálnici. Dron vybavený technologií LiveU lze okamžitě vyslat k místu události a získat letecký pohled v reálném čase. První zasahující tak mohou rychleji vyhodnotit situaci, lokalizovat zraněné a naplánovat bezpečný a efektivní zásah. Rychlejší reakce u dopravních nehod zvyšuje šanci na přežití.
- Hlídky a bezpečnostní dohled: Dron lze nasadit k předběžné kontrole rizikového místa bez nutnosti okamžité fyzické přítomnosti policie. Díky leteckému přehledu lze zajistit tzv. overwatch a průzkum bez čekání na posily nebo vrtulník. Tím se výrazně snižuje riziko ohrožení zasahujících osob.

- Pátrání a záchrana: Při záchranných operacích ve složitém nebo rozsáhlém terénu dokážou drony nebo robopsi s přenosem přes LiveU rychle prohledat velké plochy. Obraz v reálném čase pomáhá lokalizovat pohřešované osoby, odhalit nebezpečné oblasti a koordinovat zásahové týmy.
- Požáry: Během požáru poskytuje dron s technologií LiveU hasičům nadzemní přehled o šíření požáru. Lze identifikovat ohniska, riziková místa i možné únikové cesty. Rychlejší situační přehled vede k rychlejšímu zásahu a nižším škodám.




## Civilní aplikace

- **Ostraha perimetru:** V průmyslových areálech nebo u kritické infrastruktury lze dron nebo robopsa s LiveU jednotkou využít k průběžnému dohledu nad areálem. Bezpečnostní týmy sledují obraz v reálném čase, identifikují neoprávněné vstupy a efektivně nasazují zásahové jednotky. Výsledkem je vyšší bezpečnost a rychlejší reakce na incidenty.
- **Inspekce infrastruktury:** Kontrola mostů, konstrukcí, potrubí, větrných elektráren, rozvoden je tradičně náročná a riziková pro člověka. Dron nebo robopes s kamerou, případně termokamerou a LiveU přenosem umožňuje automatizovanou inspekci ve vysokém rozlišení z různých úhlů. To zkracuje čas, zvyšuje kvalitu sběru dat a snižuje riziko pro techniky. Možnost nahrávání přenosu zároveň slouží k auditu nebo školení.
- **Monitoring davu:** Velké akce, jako koncerty, sportovní události nebo maratony, vyžadují neustálý dohled nad pohybem lidí a možnými riziky. Drony s LiveU poskytují organizátorům i bezpečnostním složkám letecký pohled v reálném čase, což umožňuje včas identifikovat problémová místa, reagovat na incidenty a zajistit celkovou bezpečnost akce.

## Technologie, která chrání a spojuje

Technologie LiveU se ukazuje jako spolehlivý nástroj pro přenos obrazu v reálném čase v kritických situacích. Vizuální přehled z terénu znamená rychlejší rozhodování, lepší koordinaci a vyšší bezpečnost pro zasahující týmy.

Díky přímému přenosu obrazu lze zásahy řídit s vyšší přesností a eliminovat rizika pro lidské životy. Tam, kde dříve musel do neznámého prostředí vstupovat člověk, dnes často stačí robopes nebo dron.

## ISSS 2025 – technologie LiveU v akci

Na konferenci ISSS 2025 bude možné vidět technologie LiveU v reálné ukázce. Na stánku Smart Informatics budou předvedeny výše uvedené příklady mobilních jednotek včetně robopsa nebo velitele zásahu s kamerou. Cílem je propojit moderní technologii s praktickými potřebami těch, kdo denně rozhodují o životech.

Zajímá vás, jak LiveU funguje v reálném světě? Přijďte si technologie vyzkoušet naživo na ISSS 2025 nebo nás kontaktujte pro ukázku ve vašem prostředí.

Ing. Olga Jedličková, olga.jedlickova@smarti.cz, tel: +420 724 188 791, www.smarti.cz

# Cyklistická budoucnost Královéhradeckého kraje: Strategie a sdílená mobilita

Ing. Martina Kubešová, Krajský úřad Královéhradeckého kraje

Královéhradecký kraj dlouhodobě systematicky podporuje rozvoj cyklistiky jako součást udržitelé regionální mobility. Tato podpora se nově netýká pouze výstavby infrastruktury, ale i zavádění moderní formy sdílené dopravy. Kromě investic do rozvoje sítě cyklostezek a cyklotras, které jsou realizovány prostřednictvím samostatného dotačního titulu, kraj v posledních dvou letech intenzivně podporuje také službu sdílených kol a elektrokol ve všech obcích na svém území.

Služba sdílených kol se stává důležitou součástí městské mobility ve středně velkých a menších městech České republiky. Královéhradecký kraj ve spolupráci s Nadačním fondem Škoda Auto patří mezi regiony, které podporují její rozvoj prostřednictvím dotačního programu a aktivní spoluprací s obcemi.

Z dat od poskytovatele služby společnosti nextbike Czech Republic vyplývá, že většina měst zaznamenala v roce 2024 výrazný nárůst počtu výpůjček oproti roku 2023. Největší relativní nárůst byl v Hořicích (+ 118 %) a ve Dvoře Králové nad Labem (+ 85 %). Absolutní špičku představuje Hradec Králové s téměř 170 tisíci výpůjčkami v loňském roce. V počtu výpůjček na osobu jsou v první desítce v rámci České republiky tři města z Královéhradeckého kraje – Trutnov, Jičín a Hradec Králové.

Na popularitě získávají také elektrická kola. Zatímco v roce 2023 byla elektrokola dostupná jen ve velmi omezeném počtu měst, následující rok se nabídka značně rozšířila (např. o Trutnov, Hradec Králové, Dvůr Králové nad Labem). V Trutnově bylo evidováno přes 19 500 výpůjček elektrokol za rok.

Podpora byla rovnoměrně rozdělena mezi menší i větší obce, což umožnilo vznik a rozšíření služeb i mimo krajská centra a vedle zavedených měst vstoupily do systému také obce jako Lánov, Dolní Dvůr nebo Albrechtice nad Orlicí.

Výsledky ukazují, že systém sdílených kol v Královéhradeckém kraji rychle expanduje. Významný růst počtu výpůjček, rozšiřování nabídky elektrokol a zapojování nových i menších obcí naznačují, že kombinace veřejné podpory a lokálního zájmu tvoří účinný model pro zavádění udržitelné městské mobility. Královéhradecký kraj s Nadačním fondem Škoda Auto chtějí pokračovat v pobídce tohoto trendu. Nadále se bude sledovat rozvoj služby a systematicky vyhodnocovat její přínosy z hlediska dopravního i vlivu na životní prostředí.

# Efektivní správa procesů informační a kybernetické bezpečnosti, kontinuity a systémů AI

Petr Krůček, jednatel a vedoucí konzultant, KRUCEK, s.r.o.

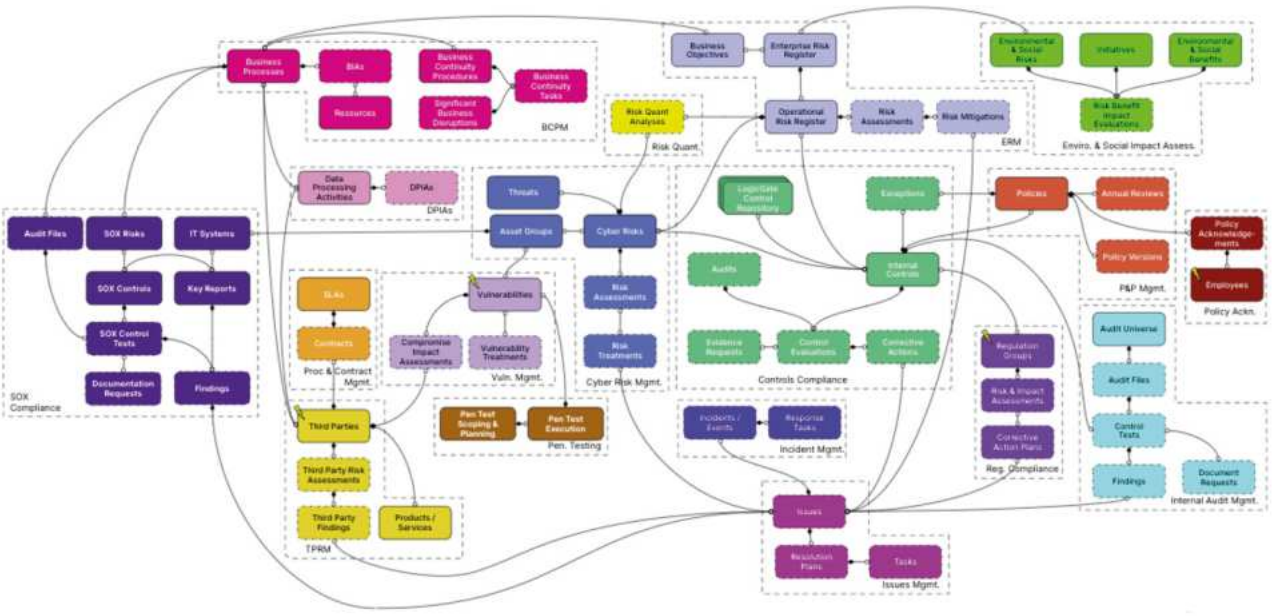
Organizace používají manažerské procesy, aby mohly dosahovat naplnění svých politik a cílů, zlepšovat svou výkonnost nebo zajistit soulad s předpisy v dynamickém a neustále se měnícím prostředí. Tyto manažerské procesy jsou podporovány více či méně formálními systémy managementu, které tvoří prvky jako je organizační struktura, zapojené osoby a jejich odpovědnosti, činnosti plánování a provoz.

Organizace při naplňování svých politik a cílů čelí mnoha výzvám, jako je rezistence ke změnám, nedostatek pracovníků či jejich kompetencí nebo stále rostoucí požadavky zákonů a předpisů. Nedostatky bývají příčinou mrhání času a potenciálu kvalifikovaných zaměstnanců, nesouladu s předpisy a v konečném důsledku incidentů s dopady na organizaci, jednotlivce nebo společnost.

Oblast informační a kybernetické bezpečnosti nebo umělé inteligence patří k dynamickým oborům s nedostatkem odborníků na manažerských i technických pozicích. Tento problém bude patrně ještě palčivější, například s ohledem na rozšíření působnosti směrnice kybernetické bezpečnosti NIS 2, nařízení EU o umělé inteligenci či směrnice o odolnosti kritických subjektů CER. Řešení spočívá v digitalizaci a automatizaci procesů, které umožní výrazné zvýšení produktivity a uvolní ruce odborníkům od rutinních činností.

## Soubor aplikací pro digitalizaci procesů systémů managementu a jejich integrace

Společnost KRUCEK představuje cloudové řešení s přizpůsobitelnými aplikacemi pro digitalizaci procesů správy a řízení, rizik a souladu s předpisy (GRC aplikace), které umožňuje propojovat tyto aplikace a vybudovat ucelená GRC řešení. Díky jednomu integrovanému pohledu je možné snadno agregovat a analyzovat data z jednotlivých oblastí.




*Obr. 1: Ucelený soubor navzájem propojených GRC aplikací*

Základní GRC aplikace pokrývají níže uvedené procesy a je na organizaci, aby se rozhodla, které bude používat a které ne.

- Management podnikových rizik
- Management kybernetických rizik
- Management rizik třetích stran
- Management kontrolních opatření
- Management incidentů
- Management problémů (neshod)
- Management politik a postupů a jejich šíření uživatelům
- Management modelů a aplikací umělé inteligence
- Management kontinuity činností
- Management ochrany osobních údajů
- Management interního auditu

Jak je naznačeno na obrázku 1, řešení umožňuje propojování aplikací v rámci platformy. Lze také využít nativní integraci s aplikacemi třetích stran, např. MS SharePoint, Power BI, Google Disk, Slack atp. nebo integraci s jinými aplikacemi prostřednictvím obecného aplikačního rozhraní (RESTful API s ověřením OAuth 2.0).

Kromě základních aplikací je možné efektivně vytvořit a provozovat řadu dalších řešení, například pro management rizik fyzické bezpečnosti, management výjimek nebo management aktiv, například produktů a služeb, procesů a činností, jakož i podpůrných aktiv.

## Uživatelské prostředí

Moderní uživatelské prostředí je pro uživatele velmi intuitivní a snadno ovladatelné. Uživatelé mají k dispozici prostředí převážně v českém jazyce.

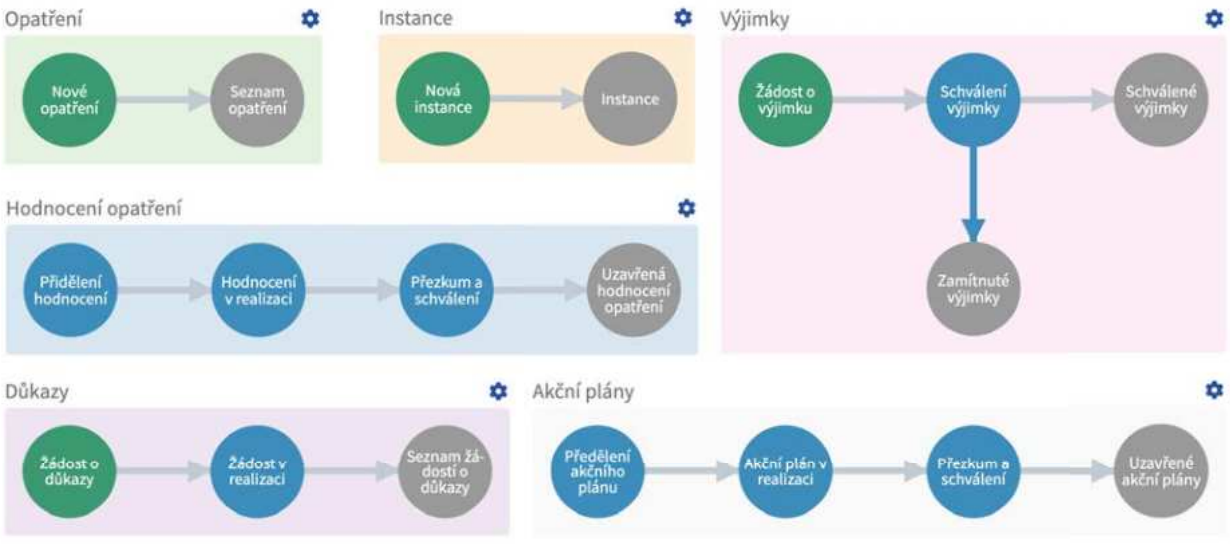
Platforma umožňuje sdílení informací v podobě tabulkových přehledů i grafů, které lze vhodně přizpůsobit různým uživatelským rolím. Pomocí informačních panelů a sestav může každý získat jasný přehled o stavu rizik nebo jiných agend. Každý aspekt lze přizpůsobit individuálním preferencím.


*Obr. 2: Informační panely s tabulkovými přehledy a grafy*

Řešení také podporuje automatizaci pracovních postupů, včetně zasílání notifikací v rámci aplikace nebo e-mailem, a to i opakovaně s nastavitelnou frekvencí, například v případě blížícího se data splnění úkolu, přidělení požadavku/úkolu uživateli, vzniku nového záznamu, provedení kroku v pracovním postupu atp.

## Administrátorské prostředí

Pro vytváření i správu aplikací není potřeba programování. Administrátorské prostředí umožňuje i netechnickým uživatelům vytvářet a udržovat aplikace mnohem snadněji než při použití tradičních metod vývoje aplikací.



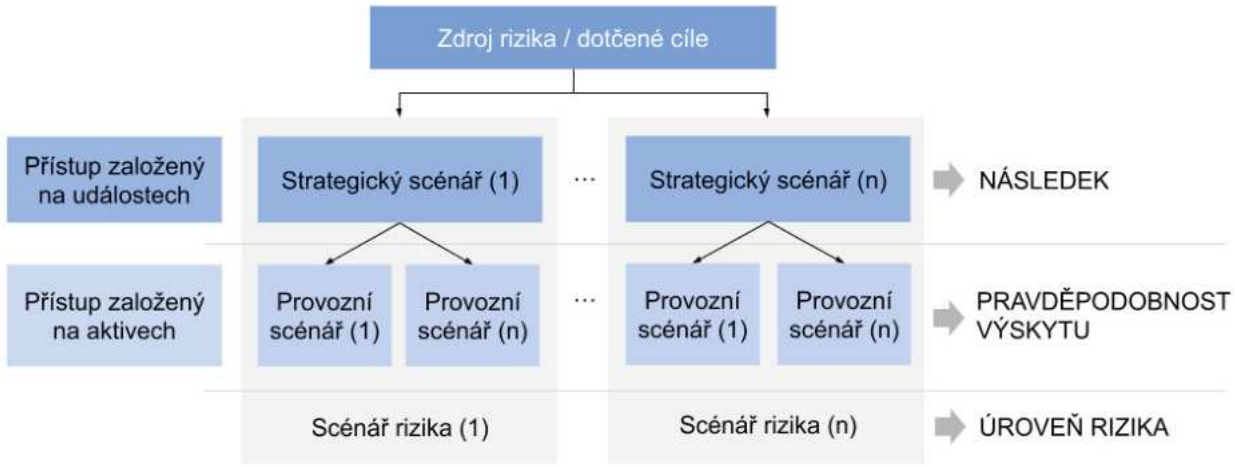

*Obr. 3: Pracovní postupy v administrativním prostředí – aplikace pro správu a kontrolu kontrolních opatření*

## Příklad použití – management rizik a kontrolních opatření kybernetické bezpečnosti

Flexibilita řešení je obrovská. Jako příklad může posloužit management rizik a kontrolních opatření kybernetické bezpečnosti. Obecně je možné aplikovat dva přístupy k managementu kybernetických rizik, a to přístup založený na událostech a přístup založený na aktivech.

- **Přístup založený na událostech**: Základní koncepce přístupu založeného na událostech spočívá v tom, že rizika lze posoudit prostřednictvím vyhodnocení obávaných událostí a jejich následků. Přístup založený na událostech může ustanovit scénáře na obecné úrovni (strategické scénáře), aniž by bylo nutné věnovat značné množství času podrobné identifikaci aktiv. To umožňuje organizaci zaměřit své úsilí při ošetření rizik na kritická rizika.
- **Přístup založený na aktivech**: Základní koncepce přístupu založeného na aktivech spočívá v tom, že rizika lze posoudit prostřednictvím aktiv, hrozeb a zranitelností. Pokud lze v rámci ISMS vyjmenovat všechny platné kombinace aktiv, hrozeb a zranitelností, pak by teoreticky měla být identifikována všechna rizika. Přístup založený na aktivech dokáže identifikovat hrozby a zranitelnosti specifické pro aktiva a umožňuje organizaci stanovit specifické ošetření rizik na podrobné úrovni.

V praxi se postupně prosazuje kombinace obou přístupů – přístup založený na událostech (strategické scénáře), na který navazuje přístup založený na aktivech, kdy se platné kombinace aktiv, hrozeb a zranitelností (provozní scénáře) uplatní pouze na relevantní strategické scénáře, nikoli na všechny možné kombinace. To umožňuje efektivní posouzení rizik a zaměření úsilí na ošetření významných rizik. Tento přístup je podporován normou ISO/IEC 27005:2022 i některými světově respektovanými metodikami.




*Obr. 4: Posuzování rizik na základě scénářů rizik, převzato z [2]*

Pro podporu uvedeného přístupu managementu rizik a opatření bude potřeba několik pracovních postupů (workflow):

- Evidence hlavních (primárních aktiv), jejich vazeb a významnosti
- Evidence třetích stran v ekosystému, jejich vazeb a významnosti
- Evidence podpůrných aktiv, jejich vazeb a významnosti
- Evidence původců rizik, jejich vazeb a významnosti
- Evidence kontrolních opatření, jejich vazeb a efektivity
- Proces posuzování rizik a jejich vazeb, včetně strategických a provozních scénářů
- Evidence akčních plánů pro ošetření rizik a jejich vazeb

Tyto základní pracovní postupy pro management rizik a kontrolních opatření lze doplnit o další, například evidenci instancí, ve kterých se aplikují příslušná kontrolní opatření, postup shromažďování a evidence důkazů o souladu realizace opatření v instancích, analýza dopadů na činnosti organizace (BIA) atd.

Jsou vaše procesy managementu rizik a kontrolních opatření odlišné? Nevadí. Aplikace lze snadno přizpůsobit individuálním požadavkům organizací.

Literatura

[1] ENISA, RISK MANAGEMENT STANDARDS Analysis of standardisation requirements in support of cybersecurity policy, březen 2022

[2] ISO/IEC 27005:2022 – Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti

# Právní pohled na kontejnerové datové formáty

Mgr. Tomáš Lechner, Ph.D., Vysoká škola ekonomická v Praze,
Národohospodářská fakulta, Katedra práva

## Úvod

Správní řád v § 37 stanoví, že podání je možno učinit písemně nebo ústně do protokolu anebo v elektronické podobě, přičemž pro elektronickou podobu nestanoví žádné specifické formální odlišnosti oproti podání v listinné podobě. Tedy podání musí obsahovat označení správního orgánu, jemuž je určeno, další náležitosti, které stanoví zákon, a podpis osoby, která je činí, bez ohledu na to, v jaké formě je činěno. Vlastní oddělení elektronické formy od písemné a ústní je odlišné oproti přístupu občanského zákoníku, který v § 562 odst. 1 stanoví, že písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Odlišnost těchto přístupů může být způsobena tím, že elektronická podoba může zachytit jak statický obsah v podobě písemné či obrazové, tak dynamický obsah v podobě zvuku či videa.

Podání v elektronické podobě má nejčastěji formu dokumentu, kterým je dle § 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě, každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena (detailně k tomuto pojmu viz [1]). V souvislosti s podáním v elektronické podobě se také objevuje pojem datová zpráva, která nyní není v českém právním řádu přímo definována, ale vyskytuje se v různých souvislostech. Např. § 19 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, říká, že dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky, úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky a dokumenty fyzických osob, podnikajících fyzických osob a právnických osob dodávané prostřednictvím datové schránky mají formu datové zprávy. Dříve datovou zprávu definoval § 2 písm d) zákona o elektronickém podpisu jako elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru. Tento předpis však byl v roce 2016 zrušen.

Nejnovějším pojmem týkajícím se vnitřní struktury elektronického dokumentu zavedeným vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby, je komponenta, kterou se rozumí dále nedělitelná část dokumentu, která je v digitální podobě. Komponentu již před tím zavedl národní standard po elektronické systémy spisové služby, který ji ve své nejnovější (již šesté) verzi definuje jako jednoznačně vymezený proud bitů tvořící datový soubor charakterizovaný zpravidla formátem datového souboru, běžně zpracovávaným programovými aplikacemi, které umožňují provádět správu souborů, složek a disků tak, aby k nim bylo možné uživatelsky srozumitelně přistupovat a s nimi samostatně manipulovat (správce souborů) [2].

K datovému formátu jako důležité charakteristice elektronického dokumentu se vyjadřuje např. § 64 zákona č. 499/2004 Sb., který mimo jiné stanoví, že v případě dokumentů v digitální podobě určení původci zajistí jejich příjem alespoň v datových formátech stanovených jako výstupní datové formáty nebo formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě. Příhodná definice datového formátu je uvedena v národním standardu [2]: „Datový formát je způsob kódování komponenty pro účely zpracování výpočetní technikou."

Od loňského roku lze prostřednictvím datových schránek doručovat elektronické dokumenty také ve vybraných kontejnerových datových formátech a otevírá se zde tak otázka, jak na tyto kontejnerové datové formáty pohlížet. V rámci tohoto příspěvku se pokusíme nad touto otázkou zamyslet z různých úhlů pohledu.

## Informační systém datových schránek a datové formáty

Informační systém datových schránek byl realizován v roce 2009 na základě zákona č. 300/2008 Sb. Blíže k tomuto stěžejnímu nástroji českého e-Governmentu viz např. [4] a [5]. Informační systém datových schránek přenáší datové zprávy, jejichž parametry jsou upřesněny jednak prováděcí vyhláškou č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, a jednak provozním řádem, který vydává správce tohoto systému, kterým je aktuálně Digitální a informační agentura [6]. V citované vyhlášce je stanoveno, že datová zpráva dodávaná do datové schránky může mít jen určité přípustné datové formáty. Podle přílohy č. 3 jde o následující datové formáty:

- PDF (Portable Document Format)
- PDF/A (Portable Document Format for the Long-term Archiving)
- XML (Extensible Markup Language Document)
- FO/ZFO (602XML Filler dokument)
- HTML/HTM (Hypertext Markup Language Document)
- ODT (Open Document Text)
- ODS (Open Document Spreadsheet)
- ODP (Open Document Presentation)
- TXT/CSV (prostý text)
- RTF (Rich Text Format)
- DOC/DOCX (MS Word Document)
- XLS/XSLX (MS Excel Spreadsheet)
- PPT/PPTX (MS PowerPoint Presentation)
- JPG/JPEG/JFIF (Joint Photographic Experts Group File Interchange Format)
- PNG (Portable Network Graphics)
- TIF/TIFF (Tagged Image File Format)
- GIF (Graphics Interchange Format)
- MPG/MPEG/MPEG1/MPEG2 (MPEG Phase 1 -ISO-IEC 11172/Phase 2 - ISO//ISO/IEC 13818),
- WAV (Waveform Audio Format)
- MP2/MP3 (MPEG-1 Audio Layer 2/Layer 3)
- ISDOC/ISDOCX (Information System Document) verze 5.2 a vyšší
- EDI (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů - EDI)
- DWG (AutoCAD DraWinG File Format) verze 2007 a vyšší
- SHP/DBF/SHX/PRJ/QIX/SBN/SBX (ESRI Shapefile)
- DGN (Bentley MicroStation Format) verze V7 a V8
- GML/GFS/XSD (Geography Markup Language Document)
- JSON (JavaScript Object Notation)
- MP4/M4A (MPEG-4 Audio ISO/IEC 14496)
- MP4/M4V/M4P (MPEG-4 Video ISO/IEC 14496)
- HEIC/HEIF (High Efficiency Image File)
- ZIP (ZIP File Format, specifikovaný v Info-ZIP Application Note 19970311)
- ASICS/SCS/ASICE/SCE (Associated Signature Containers Simple / Extended)

Pro poslední dva jmenované formáty platí další specifická omezení z toho důvodu, že jde právě o kontejnerové datové formáty, tedy takové datové formáty, které v sobě mohou obsahovat další komponenty. Tyto podmínky jmenovitě jsou:

- obsah datové zprávy není zašifrovaný,
- datovou zprávu tvoří alespoň jeden soubor ve formátu uvedeném výše,
- datovou zprávu netvoří soubor v jiném formátu než ve formátu uvedeném výše,
- datovou zprávu tvoří nejvýše 1 000 souborů a adresářů,
- maximální úroveň vnoření adresářů do sebe činí 4 a
- maximální velikost dekomprimovaného obsahu činí 3 GB.

## Datová zpráva a kontejnerový datový formát

Pokud přijmeme názvosloví vyhlášky č. 259/2012 Sb. a národního standardu, že nejmenší jednotkou, z níž se může skládat elektronický dokument je komponenta, pak můžeme mít trochu problém s tím, že i tato nejmenší jednotka vlastně nejmenší jednotkou být nemusí. Rozpor je také v samotné citované vyhlášce, která pro komponentu připouští datový formát PDF/A-3, k čemuž dodává, že PDF/A-3 je výstupním datovým formátem statických textových komponent a statických kombinovaných textových a obrazových komponent, neobsahuje-li komponentu v datovém formátu, který není výstupním datovým formátem, a komponent obsahující další komponenty. To tedy jednoznačně popírá definici dle vyhlášky o nedělitelnosti komponenty, avšak to není v rozporu s definicí zavedenou národním standardem.

Možná si tedy můžeme spíše vypomoci pojmem datová zpráva, který velmi důkladně rozebírá Stanovisko Nejvyššího soudu k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě (Plsn 1/2015) publikovaného pod č. 1/2017 ve Sbírce soudních rozhodnutí a stanovisek [3]. Zde se mimo jiné uvádí:

„Vzhledem k tomu, že elektronické dokumenty mají podobu datové zprávy, popřípadě že dokumenty jsou obsaženy v datové zprávě, lze na datovou zprávu pohlížet buď jen jako na elektronický dokument mající podobu datové zprávy, nebo také (v širším slova smyslu) též jako na elektronický nosič, tj. na obálku či kontejner, v nichž je obsažen samotný elektronický dokument jako příloha."

Datová zpráva v širším slova smyslu je tedy chápána jako kotejner, v nemž je obsažen dokument. Takovou datovou zprávou může být e-mail, datová zpráva přenášená informačním systémem datových schránek, nebo třeba SIP balíček, který slouží k přenosu dokumentu do národního digitálního archivu – viz [7]. Technicky vzato všechny tyto datové zprávy mají svůj datový formát, např. EML nebo ZFO.

Datová zpráva v užším slova smyslu je elektronickým dokumentem, jehož datový formát je posuzován pro padání vůči orgánům veřejné moci a můžeme na něj vztáhnout již jednou citované ustanovení § 64 zákona č. 499/2004 Sb., které říká, že určení původci zajistí příjem elektronických dokumentů alespoň v datových formátech stanovených jako výstupní datové formáty nebo formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě. Kromě toho veřejnoprávní původci musí upřesnit informace o provozu podatelny a o podmínkách přijímání dokumentů s tím, že podle § 2 odst. 3 písm. f) vyhlášky č. 259/2012 Sb. uvedou přehled dalších datových formátů dokumentů obsažených v datové zprávě, ve kterých veřejnoprávní původce přijímá dokumenty v digitální podobě, včetně jejich technických, popřípadě jiných parametrů.

Z výše uvedeného plyne, že daná vymezení se týkají stanovení datových formátů pro datovou zprávu v užším slova smyslu. Jinými slovy, původce nemusí mít uvedeno, že přijímá datový formát ZFO, aby tím dal najevo, že je přípustné podání prostřednictvím datových schránek. A naopak absence tohoto datového formátu mezi datovými formáty zveřejněnými dle § 2 odst. 3 písm. f) vyhlášky č. 259/2012 Sb. nemůže být použita jako odůvodnění pro nepřijetí datové zprávy podané prostřednictvím informačního systému datových schránek.

## Bestiář kontejnerových formátů

Pojďme si nyní udělat celkový přehled vybraných kontejnerových datových formátů, s nimiž se lze v současné praxi komunikace sekat. Následně se pokusíme je určitým způsobem kategorizovat.

- EML – datový formát elektronické pošty. Jeden z prvních kontejnerových datových formátů, kterým bylo možné činit podání vůči orgánu veřejné moci. Navíc podle původního zákona o elektronickém podpisu byl právě tento datový formát nositelem důkazu projevu vůle v podobě uznávaného elektronického podpisu – blíže viz [8]. Podle současné právní úpravy elektronického podpisu podle nařízení eIDAS a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, jen již tento formát „pouhou" obálkou a případným elektronickým podpisem musí být opatřena vložená příloha (datový soubor), tedy datová zpráva v užším slova smyslu (viz též [1]). Specifikem tohoto formátu je, že obsahuje dvě součásti, textovou část, kterou nelze chápat jen jako metadata, protože může mít vlastní písemný obsah, a přílohy. Z právního pohledu je textová část poněkud hůře uchopitelná, byť praktické využití elektronické pošty v neformální komunikaci je založeno zejména na ní. Komplikované je však jejich technické přiřazení k datovému formátu a, jak již bylo zmíněno dříve, nemůže být elektronicky podepsána uznávaným elektronickým podpisem podle aktuální právní úpravy. EML není výstupní datový formát dle vyhlášky č. 259/2012 Sb. EML nemůže být obsažen v datové zprávě přenášené informačním systémem datových schránek.
- ZFO – 602XML Filler dokument. Toto je obecný datovým formát založený na XML struktuře, jehož jednou z variant je také datová zpráva přenášená informačním systémem datových schránek. Obsah tedy závisí na konkrétní definici vlastního obsahu. Pokud je jím datová zpráva dle provozního řádu informačního systému datových schránek [6], pak je jedná o kontejnerový datový formát obsahující přílohy a specifická popisná metadata. Přílohy jsou datové zprávy v užším slova smyslu. ZFO není výstupní datový formát dle vyhlášky č. 259/2012 Sb., ale ZFO může být obsažen v datové zprávě přenášené informačním systémem datových schránek, a to dokonce bez specifického vymezení, tedy nejen jako datová zpráva odpovídající specifikaci dle provozního řádu informačního systému datových schránek [6].
- PDF/A-3 – Portable Document Format for the Long-term Archiving je datovým formátem, který variantně umožňuje přidání příloh. Tento formát tedy nemusí být vždy kontejnerovým datovým formátem. Vyhláška č. 194/2009 Sb. případnou „kontejnerovost" tohoto datového formátu ignoruje a neřeší pro ni žádné podmínky, což je přinejmenším udivující, když pro další datové formáty jako ZIP a ASICE tyto podmínky striktně stanoví. Naproti tomu vyhláška č. 259/2012 Sb. si je této případné „kontejnerovosti" tohoto datového formátu vědoma a z pohledu posouzení tohoto datového formátu jako výstupního datového formátu restriktivně uvádí, že PDF/A-3 je výstupním datovým formátem statických textových komponent a statických kombinovaných textových a obrazových komponent, neobsahuje-li komponentu v datovém formátu, který není výstupním datovým formátem, a komponentu obsahující další komponenty.
- ISDOCX – formát elektronické fakturace, který má charakter kontejneru spojujícího elektronickou fakturu ISDOC s přílohami. Jde vlastně o specifickou podmnožinu formátu ZIP, v němž je vložen alespoň jeden ISDOC a další přílohy. Přestože zde jde jednoznačně o kontejnerový formát, vyhláška č. 194/2009 Sb. tuto vlastnost přehlíží. Z pohledu vyhlášky č. 259/2012 Sb. není ISDOCX výstupním datovým formátem. Dodejme, že ISDOC, který již není kontejnerovým datovým formátem, výstupním datovým formátem je.
- ZIP – ZIP File Format, je datový formát soužící pro komprimování a spojování datových souborů. Kromě nich nenese žádná významná specifická metadata, obsahuje pouze technické charakteristiky sebe sama. ZIP není výstupní datový formát dle vyhlášky č. 259/2012 Sb. Od roku 2024 ZIP již může být za specifických podmínek (viz výše) obsažen v datové zprávě přenášené informačním systémem datových schránek.
- ASICE – Associated Signature Containers Extended. Jde o datový formát, který spojuje podepsaný datový soubor (podepsaná data) s elektronickým podpisem, nejlépe ve formátu CAdES podle nařízení eIDAS a k němu prováděcích předpisů. Technicky se vlastně jedná o určitou specifickou podmnožinu ZIP formátu. Proto asi není překvapující, že to není výstupní datový formát dle vyhlášky č. 259/2012 Sb. Od roku 2024 ASICE již může být za specifických podmínek (viz výše) obsažen v datové zprávě přenášené informačním systémem datových schránek.

Uvedený přehled vybraných kontejnerových datových formátů ukazuje, že jde skutečně o velmi různorodou skupinu datových formátů, které se liší ve všech možných parametrech. Některé mohou obsahovat sami o sobě významný obsah (EML, PDF/A-3),

některé obsahují specifická metadata (ZFO, EML) a některé jsou jen specifickým nebo obecným spojením datových souborů (ISDOCX, ZIP, ASICE).

## Kontejnerové datové formáty a národní standard

Přestože jde o takto pestrou skupinu, národní standard pro elektronické systémy spisové služby [2] k těmto formátům přistupuje, jako kdyby měly naprosto shodné vlastnosti. Již rozšířená definice komponenty tyto formáty uvádí jako rovnocenné příklady:

„Komponentou může být i metasoubor zahrnující společné uložení dat a metadat (datový kontejner, například PDF/A-3, ZFO, ZIP), z kterého lze – s pomocí k tomu určených programových aplikací – vyčlenit v něm zapouzdřené datové soubory, se kterými lze pracovat jako se samostatnými komponentami podle věty první."

Nicméně definice v citovaném předpisu není z tohoto pohledu přesná a odpovídá spíše jen datovým formátům ZIP, ISDOCX či ASICE, tedy těm, které spojují datové soubory, ale nic dalšího nepřidávají. Odkazovaná definice zní [2]: „Kontejnerové datové formáty jsou formáty komponent obsahující alespoň jednu další komponentu." Samozřejmě, že tato definici nevylučuje žádný kontejnerový datový, ale přehlíží skutečnost, že datový formát může anebo nemusí kromě dalších komponent zahrnovat i jiný obsah, který může mít různý význam.

Ke kontejnerovým formátům se vztahují požadavky 2.4.1, 2.4.2 a 2.4.3 národního standardu – viz následující obrázek.

***2.4 Kontejnerové datové formáty***

| Číslo | Požadavek |
|---|---|
| 2.4.1 | ESSL zajistí při příjmu doručeného dokumentu automatizované zpracování komponenty dokumentu v datovém formátu, který má charakter kontejneru, podle požadavků 2.4.3 a 2.4.4, a to alespoň pro formáty ASiC, FO/ZFO, EML, ISDOCX, ZIP, PDF/A. Povinnost automatického zpracování se nevztahuje na šifrované komponenty v datovém formátu, který má charakter kontejneru, a na již zpracované datové zprávy. |
| 2.4.2 | ESSL uchová kontejner doručeného dokumentu v nezměněné podobě jako samostatnou komponentu alespoň do okamžiku uzavření spisu. |
| 2.4.3 | ESSL při automatizovaném zpracování kontejneru zajistí vyjmutí všech komponent vnořených v první úrovni kontejneru a jejich uložení jako samostatných komponent. Pokud je vyjmutá komponenta v datovém formátu uvedeném v požadavku 2.4.1, proces automatického zpracování se opakuje. ESSL v případě selhání automatického zpracování kontejneru poskytne zpracovateli informaci o selhání. |

*Obr. 1. Požadavky národního standardu na kontejnerové datové formáty, převzato z [2].*

Národní standard se tak omezuje na funkčnost vyjmutí případných vložených komponent, aniž je zde jakkoliv zohledněna podmínka smyslu takového vyjmutí. Navíc dává povinnost uchování původního kontejneru, aniž jakkoliv řeší, zda je tento nezbytný, jako třeba PDF/A, nebo z pohledu posuzování obsahu podání bezpředmětný jako třeba ZIP, u něhož má uchování pouze určitý důkazní smysl.

## Jak posuzovat elektronický dokument z hlediska datového formátu

Elektronický dokument se tedy skládá alespoň z jedné komponenty, která oplývá vlastností v podobě datového formátu. Přesto již dvakrát zde citované ustanovení § 64 zákona č. 499/2004 Sb. hovoří o datovém formátu dokumentu. Podle citovaného Stanovisko Nejvyššího soudu k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě (Plsn 1/2015) publikovaného pod č. 1/2017 ve Sbírce soudních rozhodnutí a stanovisek [3] se tedy posuzuje datový formát datové zprávy v užším slova smyslu, tedy konkrétně např.

příloh elektronické pošty nebo obsahu datové zprávy přenášené informačním systémem datových schránek, což jsou podle citovaného stanoviska datové zprávy v širším slova smyslu. Nyní tu máme primárně položenou otázku, což když je formátem elektronického dokumentu kontejnerový datový formát. Jak takový formát posuzovat např. z hlediska přípustnosti pro podání?

Rozhodně zde není cílem podat černobílou odpověď, protože taková zřejmě neexistuje.

Již výše jsme si ukázali, jak jsou kontejnerové datové formáty různorodé a kritizovali jsme přístup národního standardu, který je – lidově řešeno – strká do jednoho pytle. V posuzování je třeba mít dále na paměti rozsudek Nejvyššího správního soudu ČJ 8 Afs 93/2020 ze dne 21. ledna 2021 [9], z něhož plyne, že i podáním v datovém formátu, které daný orgán veřejné moci nemá zveřejněný jako přípustný datový formát, je třeba se zabývat a dle dikce správního řádu případně poskytnout přiměřenou lhůtu k nápravě této vady podání. Nicméně jako datum podání se dle uvedeného rozsudku má aplikovat přijetí původní datové zprávy, byť byla v neakceptovaném datovém formátu.

A nyní si představme příklad, který je navíc podložený ustanovením § 23 odst. 9 vyhlášky č. 256/2012 Sb., kde se stanoví, že veřejnoprávní původce může pro výstup z elektronického systému spisové služby podle odstavce 1 písm. a) současně použít také jiný datový formát komponenty. Pokud tedy potřebuje jeden orgán veřejné moci jinému orgánu veřejné moci poslat třeba tabulku v datovém formátu XSLX (MS Excel Spreadsheet), měl by k tomu zároveň připojit stejnou tabulku konvertovanou do výstupního datového formátu PDF/A. Otázkou je, jak však pozná příjemce takové datové zprávy, že obsahy těchto komponent jsou totožné? Zřejmě by to mělo být uvedeno v průvodním dopise, např. „posílám vám tabulku k vyplnění a zároveň přikládám její shodnou podobu ve výstupním datovém formátu". A abychom to ještě zkomplikovali, tak to celé zabalíme do kontejneru ZIP. Nebo se rozhodneme obě přílohy vložit do datového souboru ve formátu PDF/A-3.

Komplikací v tomto ohledu si lze představit ještě mnoho. Nicméně zdá se, že v posuzování datových formátů z hlediska přípustnosti pro podání bychom měli primárně postupovat obdobně, jako z hlediska zkoumání elektronického podpisu. Podatelna by měla zaznamenat fakta a nikoliv rozhodovat, protože rozhodnutí závisí na mnoha okolnostech a detailech vlastního podání, které musí být schopen posoudit každý jednotlivý úředník.

## Závěr

Ukázali jsme, že definice týkající se vnitřní struktury dokumentů v elektronické podobě jsou v českém právním řádu stále poněkud nepřehledné a mnohdy i nesourodé, jako např. poslední definice komponenty v prováděcí vyhlášce č. 259/2012 Sb. Rozšíření používání kontejnerových datových formátů, které od počátku roku 2024 zavedla vyhláška č. 194/2009 Sb., k tomu přidává další komplikace posuzování přípustnosti datových formátů pro podání, se kterými je třeba se vypořádat a není možné je zcela automatizovat, jak se o to snaží některé požadavky národního standardu, které bohužel nerozlišují mezi různými variantami těchto specifických datových formátů.

Literatura

[1] KUNT, M., LECHNER, T. Spisová služba. 3. aktualizované vyd. Praha: Leges, 2022. 412 s. Praktik. ISBN 978-80-7502-616-3.

[2] MINISTERSTVO VNITRA. Národní standard pro elektronické systémy spisové služby. 6. verze. Věstník Ministerstva vnitra, částka 85/2024.

[3] Stanovisko Nejvyššího soudu k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě (Plsn 1/2015) publikovaného pod č. 1/2017 ve Sbírce soudních rozhodnutí a stanovisek. Dostupné na <http://www.nsoud.cz/JudikaturaNS_new/ns_web.nsf/0/70A637A6CC85DC0EC12580BB002F9CE5/$file/Plsn1-15-def.%20zn%C4%9Bn%C3%AD.docx>.

[4] SMEJKAL, V. Datové schránky v právním řádu ČR. Praha: ABF, a. s., 2009, 176 s. ISBN 978-80-86284-78-1.

[5] MATES, P., SMEJKAL, V. E-Government v České republice: Právní a technologické aspekty. 2., podstatně přepracované a rozšířené vydání. Praha: Leges, 2012.

[6] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. Provozní řád ISDS. Dostupné na <https://info.mojedatovaschranka.cz/info/cs/80.html>.

[7] KUNT, M., LECHNER, T., POKORNÝ, R. Skartační řízení elektronicky. Archivní časopis. 2020, roč. 70, č. 1, s. 52–73. ISSN 0004-0398.

[8] LECHNER, T. Elektronické dokumenty v právní praxi. Praha: Leges, 2013. 256 s. Praktik. ISBN 978-80-87576-41-0.

[9] Rozsudek Nejvyššího správního soudu ČJ 8 Afs 93/2020 ze dne 21. ledna 2021.
Dostupné na <https://vyhledavac.nssoud.cz/DokumentOriginal/Index/657600>.

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/14/2022.

# Umělá data jako nástroj bezpečného sdílení dat

Ing. Jiří Novák, Ph.D., JN Analytics s.r.o.

**Abstrakt**: S rostoucí potřebou sdílení dat napříč institucemi veřejné správy narážíme na limity ochrany osobních a citlivých údajů. Tradiční anonymizační techniky často nedokážou nabídnout dostatečnou rovnováhu mezi ochranou soukromí a užitečností dat. Příspěvek představuje přístup založený na využití umělých dat – dat, která neobsahují skutečné údaje, ale zachovávají statistické vlastnosti původních datových sad. Pouze data, u kterých zůstane zachována jejich logická struktura, lze totiž efektivně využít pro další analýzy. Umělá data jsou vytvářena s využitím nástrojů umělé inteligence (AI), díky čemuž je možné spojit ochranu dat s jejich praktickým využitím. Popsány jsou konkrétní příklady, jak lze umělá data využít jako efektivní nástroj bezpečného sdílení dat a jak mohou podpořit transparentnost, otevřená data i rozhodování ve veřejné správě – bez rizika ohrožení citlivých údajů.

**Klíčová slova**: důvěrnost, ochrana dat, umělá data, statistika, otevřená data

## Úvod

V digitální době roste poptávka po širší dostupnosti dat pro vědecký výzkum, analytickou činnost i řízení veřejné správy. Mikrodata, tedy podrobné údaje na úrovni jednotlivců, nabízejí unikátní pohled na socioekonomické procesy, ale jejich zveřejňování přináší riziko narušení důvěrnosti osobních údajů [1; 2]. Ochrana důvěrnosti proto představuje klíčovou výzvu: jak zajistit bezpečný přístup k datům a současně zachovat jejich analytickou hodnotu.

Tradiční anonymizační techniky čelí významným omezením, a proto se do popředí dostává moderní koncept **syntetických dat**, které v JN Analytics nazýváme **„Umělá data“**, jako inovativního nástroje ochrany důvěrnosti. Tento článek představí principy, metody i praktické zkušenosti s jejich využitím ve veřejné správě.

**Statistická ochrana důvěrnosti** *(Statistical Disclosure Control, SDC)* zahrnuje soubor metod, které minimalizují riziko identifikace jednotlivců nebo subjektů v publikovaných datech [1]. Rizika lze klasifikovat jako:

- **Identifikační riziko** *(identity disclosure)*, kdy je možné přiřadit údaj ke konkrétnímu subjektu,
- **Atribuční riziko** *(attribute disclosure)*, kdy je možné odvodit citlivou informaci o subjektu, aniž by byl přímo identifikován.

Současné právní předpisy, včetně GDPR a statistických kodexů, ukládají úřadům a veřejným institucím povinnost zajistit, aby zveřejňovaná data nebyla zneužitelná k identifikaci jednotlivců [2; 3].

K ochraně mikrodat existují různé strategie, jejichž volba závisí na charakteru dat, účelu zveřejnění a požadované úrovni ochrany důvěrnosti. Cílem vždy zůstává nalezení optimální rovnováhy mezi minimalizací rizika prozrazení a zachování maximální užitečnosti dat pro výzkum či řízení veřejné správy.

## 1. Tradiční metody ochrany a jejich limity

Historicky byly k ochraně důvěrnosti mikrodat využívány především dvě hlavní skupiny metod: neperturbační a perturbační [1; 2].

### 1.1. Neperturbační metody

Neperturbační metody se snaží omezit riziko prozrazení tím, že snižují detail zveřejňovaných dat, aniž by samotná data měnila. Typickými přístupy jsou:

- **Potlačení buněk** *(cell suppression)*: odstranění určitých hodnot či kategorií, zejména těch, které by mohly vést k identifikaci individuálních respondentů.
- **Globální překódování** *(global recoding)*: sloučení kategorií proměnných (např. věkové skupiny) do širších kategorií, čímž se snižuje možnost identifikace.

Výhodou neperturbačních metod je zachování původní struktury dat, ovšem na úkor podrobnosti a informační hodnoty [1].

### 1.2. Perturbační metody

Perturbační metody mění samotné hodnoty v datech, aby snížily riziko zpětné identifikace, přičemž se snaží minimalizovat dopad na statistickou užitečnost dat. Patří mezi ně například:

- **Výměna záznamů** *(record swapping)*: nahrazení určitých údajů jinými záznamy se stejnými charakteristikami.
- **Přidání náhodného šumu** *(adding random noise)*: mírná modifikace číselných hodnot přidáním náhodné odchylky.
- **PRAM** *(Post Randomization Method)*: náhodná změna kategoriálních hodnot podle definovaných pravděpodobnostních pravidel.

Perturbační techniky umožňují zachovat většinu datových vztahů, ale přinášejí určitou míru informační ztráty, kterou je třeba pečlivě hodnotit [1; 4].

**Omezení tradičních metod**

Tradiční metody, ať už perturbativní či neperturbativní, čelí v současnosti několika výzvám:

- **Zvyšující se schopnosti rekonstruovat data**: Pokročilé techniky datové analýzy a strojového učení zvyšují riziko zpětné identifikace i z relativně agregovaných dat [5].
- **Snížená užitečnost dat**: Čím více se data chrání, tím více klesá jejich analytická hodnota, což může omezovat možnosti vědeckého a veřejného využití.
- **Nemožnost efektivně chránit komplexní vícerozměrné struktury**: U dat s bohatou vnitřní strukturou (např. domácnosti, hierarchie) jsou klasické metody často nedostatečné.

V reakci na tyto výzvy roste zájem o nové přístupy k ochraně mikrodat, především o **syntetická data** jako efektivní a bezpečnou alternativu.

## 2. Syntetická data jako moderní nástroj ochrany

### 2.1. Definice syntetických dat

**Syntetická data** představují inovativní přístup k ochraně důvěrnosti mikrodat, který reaguje na limity tradičních anonymizačních technik. Základní myšlenkou je vytvoření **nového datového souboru**, který statisticky věrně napodobuje původní dataset, ale **neobsahuje skutečné individuální záznamy** [1; 3].

Rozlišujeme dva hlavní typy syntetických dat:

- **Plně syntetická data** *(fully synthetic data)*: všechna data jsou nově vygenerována modelem bez přímého využití skutečných hodnot [1].
- **Částečně syntetická data** *(partially synthetic data)*: pouze citlivé části dat jsou nahrazeny syntetickými hodnotami, zatímco ostatní údaje zůstávají původní [9].

V praxi, zejména v oblasti ochrany mikrodat ze sčítání lidu, se preferují **plně syntetická data** z důvodu maximalizace ochrany [2].

### 2.2. Výhody syntetických dat

Použití syntetických dat přináší několik zásadních výhod:

- **Minimalizace rizika prozrazení**: protože reálné údaje jsou nahrazeny simulovanými, riziko zpětné identifikace je zásadně sníženo.
- **Zachování analytické hodnoty**: při správné modelaci zachovávají syntetická data klíčové statistické vztahy v populaci, což umožňuje smysluplné analýzy [4].
- **Flexibilita použití**: syntetická data mohou být sdílena širšímu spektru uživatelů, včetně vědců, odborných pracovníků a veřejnosti, bez nutnosti přísných restrikcí.
- **Možnost simulace hypotetických scénářů**: díky generativní povaze lze vytvářet varianty dat pro testování různých scénářů a opatření.

### 2.3. Rizika a omezení

Přestože syntetická data přinášejí významné výhody, je třeba být si vědom určitých omezení:

- **Modelové zkreslení**: pokud model nezachytí dostatečně komplexně strukturu původních dat, může dojít k nepřesnostem [6].
- **Možné zbytkové riziko**: v případě nedostatečné variability syntetických dat by mohlo dojít k vytvoření záznamů velmi podobných skutečným respondentům.
- **Omezená použitelnost pro některé analýzy**: zejména pro analýzy extrémních hodnot nebo velmi specifických podskupin mohou být syntetická data méně vhodná.

Proto je klíčové pečlivě volit metodologii generování syntetických dat a vyhodnocovat jak míru ochrany, tak zachování užitečnosti dat [3; 4].

## 3. Tvorba syntetických mikrodat – metody

Generování syntetických mikrodat není náhodný proces, ale systematická činnost založená na sofistikovaných modelech, které zachycují strukturu, rozdělení a vzájemné vztahy původních dat [1; 2]. Volba správné metody je klíčová pro dosažení optimální rovnováhy mezi ochranou důvěrnosti a zachováním užitečnosti dat.

### 3.1. Proces tvorby syntetických dat

Obecně lze postup generování syntetických mikrodat rozdělit do následujících kroků:

1. **Analýza původního datasetu**
   - Identifikace klíčových proměnných a vztahů mezi nimi (např. socio- demografické charakteristiky, domácnosti, hierarchické struktury).

2. **Výběr vhodných modelů**
   - Pro každou proměnnou (nebo skupinu proměnných) je zvolen model, který nejlépe vystihuje její rozdělení a vztahy k ostatním proměnným.
3. **Trénování modelů na původních datech**
   - Modely se „učí" strukturu dat z původního datasetu.
4. **Generování syntetických záznamů**
   - Na základě naučených modelů jsou vytvořeny nové „umělé" záznamy.
5. **Vyhodnocení kvality syntetických dat**
   - Ověření zachování klíčových statistických charakteristik a minimalizace rizika identifikace.

### 3.2. Používané metody simulace

Pro tvorbu syntetických dat se dnes využívá široké spektrum nástrojů ze statistických metod, strojového učení a umělé inteligence [1; 2; 3]. Základní přístupy zahrnují:

- **Regresní modely**
  - Využívají se zejména pro simulaci spojitých proměnných a kategorizovaných výstupů na základě prediktorů.
  - Typickým příkladem je multinomická logistická regrese pro více kategoriální proměnné.
- **Modely imputace dat**
  - Používají se postupy, které předpovídají hodnoty na základě známých atributů.
  - Techniky jako „predictive mean matching" či bayesovská imputace se adaptují pro generování syntetických záznamů.
- **Klasifikační stromy a náhodné lesy**
  - Flexibilní nelineární metody vhodné pro komplexní závislosti mezi atributy.
  - Náhodné lesy *(Random Forests)* navíc poskytují robustnost vůči overfittingu [7].
- **Modely hlubokého učení** *(Deep Learning)*
  - Moderní pokročilé přístupy pro generování dat se opírají o hluboké neuronové sítě, např.:
    - **Generativní adversariální sítě (GAN)**: soutěživé modely „generátor–discriminator" umožňující vytvářet realistické syntetické datové sady [8].
    - **Variační automatické kodéry (VAE)**: metody umožňující generovat syntetická data na základě pravděpodobnostního zakódování vstupních charakteristik.
    - **Velké jazykové modely (LLM)**: nové přístupy využívající velké neuronové sítě, původně trénované na textových datech, nyní adaptované i na strukturovaná mikrodata.

## 4. Praktické zkušenosti a příklady využití

Implementace syntetických dat ve veřejné správě a oficiální statistice již probíhá v řadě zemí a institucí. Zkušenosti ukazují, že správně navržená syntetická data umožňují bezpečné sdílení informací, aniž by byla narušena důvěrnost jednotlivců [1; 3].

### 4.1. Česká republika – případová studie

V České republice se problematikou diseminace syntetických mikrodat zabývá Český statistický úřad (ČSÚ), zejména v souvislosti s mikrodaty ze **Sčítání lidu, domů a bytů 2011**.

Výzkum zaměřený na ochranu důvěrnosti mikrodat ze SLDB 2011 ukázal, že klasické anonymizační techniky (např. agregace, potlačení) nejsou dostačující při požadavku na vysokou míru využitelnosti dat pro vědecké účely [2].

Výsledky výzkumu [2] potvrdily, že simulace plně syntetických mikrodat, realizovaná pomocí moderních statistických a machine learning metod (logistická regrese, random forests, XGBoost), představuje **nejefektivnější řešení** z hlediska ochrany důvěrnosti při zachování analytické hodnoty dat.

ČSÚ využívá pro syntézu dat přístup, který kombinuje:

- replikaci struktury domácností,
- modelování kategoriálních a spojitých proměnných,
- vyhodnocování informační ztráty a užitečnosti nových datových souborů.

### 4.2. Mezinárodní praxe

Také v zahraničí roste využívání syntetických dat v rámci oficiální statistiky:

- **Spojené státy americké (US Census Bureau)**: V rámci projektů jako American Community Survey (ACS) byly vyvíjeny plně syntetické soubory pro veřejné použití *(Public Use Files)*, aby bylo možné zpřístupnit detaily demografických a ekonomických dat bez rizika identifikace jednotlivců [1].
- **Spojené království (ONS)**: Office for National Statistics pilotně testuje syntetická data pro výzkumné účely, především v oblasti socioekonomických údajů a zaměstnanosti.
- **Eurostat**: Podporuje výzkum a experimentální projekty zaměřené na využití syntetických dat pro evropské strukturální průzkumy, včetně projektů zaměřených na vývoj vhodných standardů kvality a validace syntetických souborů.
- **Rakousko (Statistik Austria)**: Statistik Austria implementuje syntetická data pro interní účely a výzkumné spolupráce v chráněných prostředích.

Tyto příklady ukazují, že syntetická data se stávají běžným nástrojem umožňujícím vyvážit potřebu otevřenosti dat a povinnost chránit důvěrnost informací.

## 5. Závěr

S rostoucím významem datového řízení ve veřejné správě a ve vědeckém výzkumu se zvyšuje i tlak na dostupnost podrobných mikrodat. Současně však zůstává prioritou ochrana důvěrnosti jednotlivců, na což reaguje obor statistické ochrany důvěrnosti mikrodat (SDC) [1; 3].

Tradiční anonymizační techniky, byť stále užitečné, čelí novým výzvám spojeným s rozvojem datových analytických nástrojů a strojového učení. Tyto technologie usnadňují zpětnou identifikaci jednotlivců i z agregovaných údajů, čímž narůstá riziko prozrazení [2].

Umělá data se proto ukazují jako moderní a perspektivní nástroj, který umožňuje:

- podstatně snížit riziko narušení důvěrnosti,
- zachovat vysokou analytickou hodnotu dat,
- flexibilně přizpůsobit rozsah a strukturu dat specifickým potřebám uživatelů,
- rozšířit přístup k datům pro vědeckou a veřejnou sféru bez nutnosti přísných bezpečnostních opatření.

Výzkumné i praktické projekty realizované v České republice a zahraničí potvrzují, že při správné volbě metod tvorby syntetických mikrodat – od tradičních statistických modelů až po nejmodernější nástroje hlubokého učení (GAN, VAE, LLM) – lze dosáhnout vysoké úrovně ochrany i užitečnosti současně [2; 4].

Do budoucna bude klíčové:

- **standardizovat postupy hodnocení kvality syntetických dat**,
- **vytvářet robustní validační rámce**,
- **zajistit transparentní komunikaci směrem k uživatelům dat**,
- **rozvíjet vzdělávání pracovníků veřejné správy** v oblasti práce se syntetickými daty.

Syntetická data, tak otevírají cestu k bezpečnější a zároveň otevřenější správě dat v moderní společnosti.

Použitá literatura

[1] Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E.S., Spicer, K., & de Wolf, P.-P. (2012). Statistical Disclosure Control. Wiley Series in Survey Methodology. Wiley.

[2] Novák, J. (2023). Modely statistické ochrany důvěrnosti mikrodat v populačních censech. Disertační práce, Vysoká škola ekonomická v Praze.

[3] United Nations Economic Commission for Europe (UNECE). (2022). Synthetic Data for Official Statistics: A Starter Guide. Geneva: United Nations.

[4] Templ, M. (2017). Simulation of Synthetic Data for Statistical Disclosure Control: Theory and Implementation. Journal of Official Statistics, 33(1), 153–174.

[5] Domingo-Ferrer, J., & Torra, V. (2001). A Quantitative Comparison of Disclosure Control Methods for Microdata. Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies, Elsevier Science.

[6] Novák, J. (2022). Statistická ochrana důvěrnosti pro mikrodata ze Sčítání lidu, domů a bytů 2011. RELIK 2022.

[7] Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32.

[8] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative Adversarial Nets. In Advances in Neural Information Processing Systems (NeurIPS).

[9] Rubin, D. B. (1993). Discussion: Statistical disclosure limitation. Journal of Official Statistics, 9, 462–468.

# Helios Pantheon pro úřad bez zbytečné administrativy

Miroslava Sedlářová, Asseco Solutions

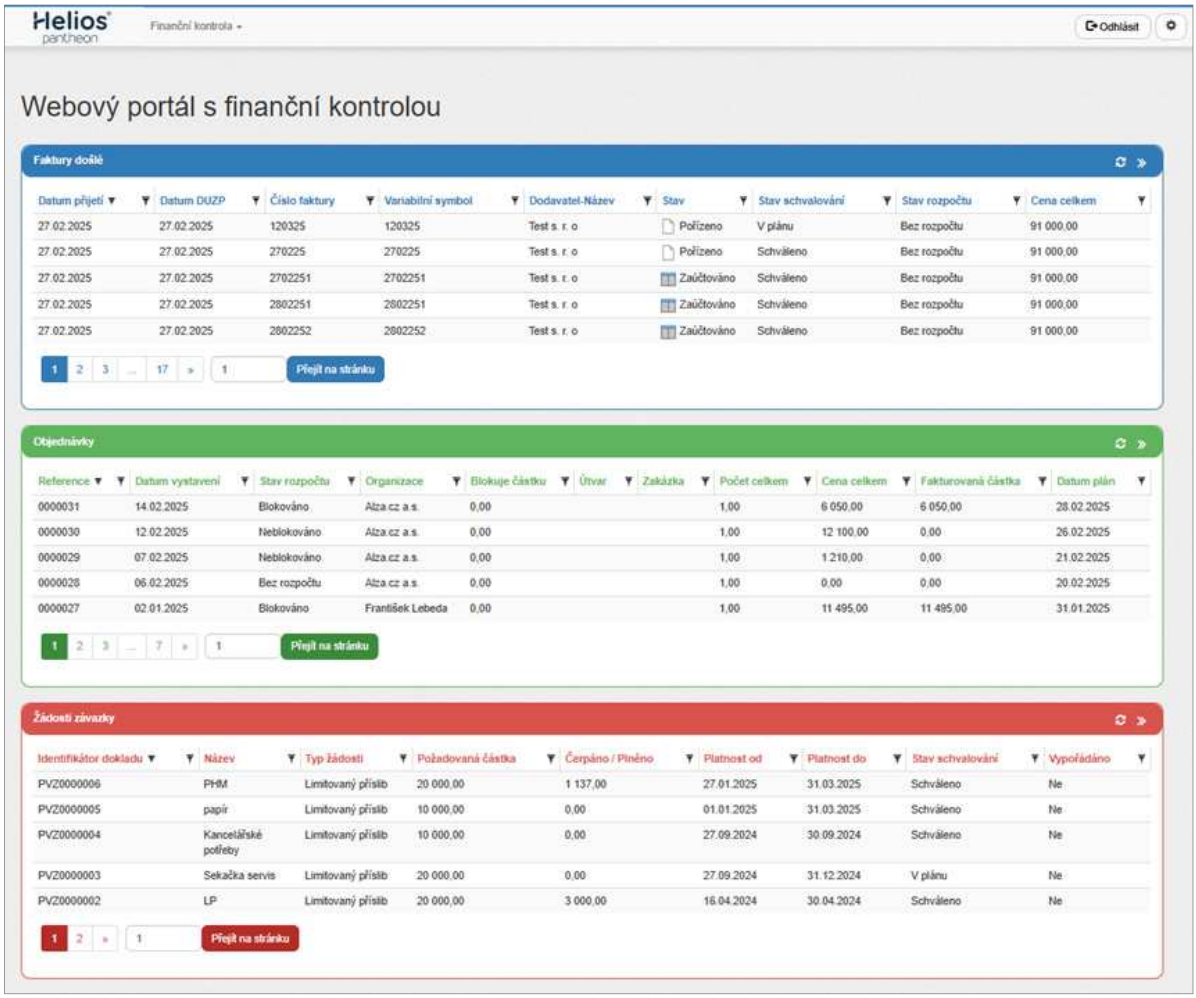
Moderní úřady se stále více spoléhají na digitální nástroje, které jim pomáhají efektivně řídit agendy, optimalizovat procesy a zajistit transparentní správu veřejných financí. Jedním z těchto nástrojů je **Helios Pantheon**, který si již získal důvěru řady úřadů.

**Jakou zpětnou vazbu od zákazníků zaznamenali naši kolegové?**

## Úřad pod kontrolou odkudkoliv

Miroslav Rouš, vedoucí realizace Helios Pantheon, potvrzuje, že moderní veřejná správa musí být flexibilní: *„Každý den vidím, jak důležité je mít data dostupná odkudkoliv a bez omezení. Webový portál Helios Pantheon umožňuje našim zákazníkům pracovat efektivněji, ať už jsou v kanceláři, na cestách nebo doma."*

Díky **centralizované platformě** mají úředníci i vedoucí pracovníci okamžitý přístup ke klíčovým informacím a mohou rychle reagovat na aktuální potřeby.



## Co od systému očekáváte? Helios Pantheon vám to nabízí!

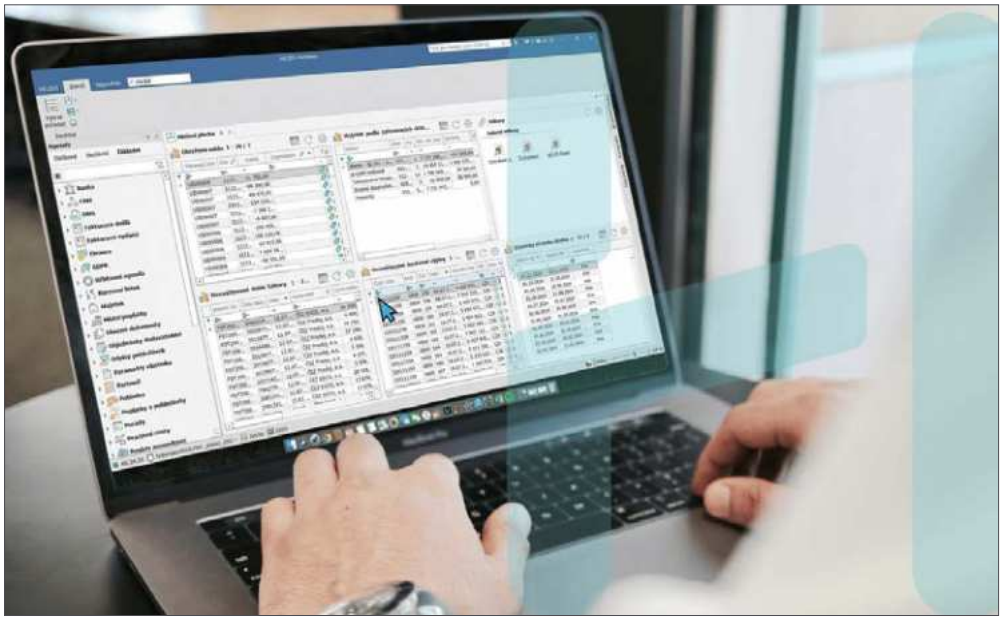
Pro mnoho úřadů znamená přechod na **Helios Pantheon** významnou úsporu času. Jednou z hlavních výhod je **automatizace procesů a odstranění zbytečné administrativy**. *„Už žádné opakované zadávání stejných dat, systém si je sám propojí napříč agendami, a tím šetří váš čas,"* dodává Rouš.

**Mějte finance pod kontrolou**: Helios Pantheon plně podporuje zákon č. 320/2001 Sb. o finanční kontrole, takže máte přehled o každé fázi schvalování výdajů a investic. Minimalizujte rizika neoprávněných výdajů a zajistěte transparentnost pro kontrolní orgány.

**Úspora času díky centralizaci dat**: Zapomeňte na opakované zadávání dat. Jednou zadané informace jsou automaticky sdíleny napříč agendami, což snižuje administrativní náročnost a zvyšuje efektivitu.

**Digitalizace dokumentů s kompletní auditní stopou**: Helios Pantheon vám umožní přehledně spravovat elektronické dokumenty a sledovat každý krok jejich oběhu, což usnadňuje zpětnou kontrolu a audit.

**Přizpůsobte si systém podle svých potřeb**: Moderní uživatelské rozhraní vám umožní přizpůsobit pracovní procesy tak, aby odpovídaly specifikům vaší instituce.



## Kybernetická bezpečnost je prioritou

V době rostoucích kybernetických hrozeb je ochrana dat klíčová. Helios Pantheon nabízí pokročilé bezpečnostní prvky:

- Komunikace šifrovaná protokolem HTTPS,
- Třívrstvá architektura pro minimalizaci rizik,
- Multifaktorová autentizace (MFA) pro bezpečné přihlášení,
- Komplexní řízení přístupů dle nařízení GDPR – tj. obecné nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679)

## Bezproblémová integrace s dalšími systémy

Helios Pantehon umožňuje vysokou mírou integrace s dalšími systémy. Ať už jde o spisovou službu **Spiska**, která je přímou součástí Pantheonu, nebo snadné napojení na důležité externí registry, jako jsou insolvenční rejstřík, ARES, ISZR, CSÚIS a další sektorové aplikace.

## Přínosy, které se projeví hned

Helios Pantheon nabízí nejen intuitivní ovládání, ale především moderní technologické nástroje, které efektivně pokrývají širokou škálu organizačních procesů. Například elektronické schvalování výdajů a investic umožňuje úřadům mít své finanční toky pod plnou kontrolou.

Díky propojení všech agend jsou informace snadno dostupné, což minimalizuje chybovost, snižuje časovou náročnost a výrazně zvyšuje pracovní efektivitu. Dokumenty jsou navíc sledovatelné po celou dobu svého „úředního putování," což zajišťuje transparentnost, lepší kontrolu a usnadňuje audity.

*„Úřady, které již na **Helios Pantheon** přešly, si pochvalují nejen snadné používání, ale především úsporu času a větší přehled nad důležitými procesy. Pokud hledáte řešení, které usnadní práci vašemu týmu, pomůže vám optimalizovat řízení agend a zároveň zajistí bezpečnost vašich dat, **Helios Pantheon** je určitě tou správnou volbou"*, doplňuje Miroslav Svoboda, obchodní manažer Helios pro veřejnou správu.

Podtrženo, sečteno: Helios Pantheon přináší uživatelům moderní nástroje pro organizaci procesů – od elektronického schvalování až po správu osobních údajů – a to vše s intuitivním ovládáním.

## Jednou vidět je lepší než stokrát slyšet...

Helios Pantheon – Neomezené možnosti pro fungující úřad on Vimeo

# Já píši vám – co mohu více? Současné přístupy k výběru archiválií a uchovávání e-mailové komunikace

Mgr. Zbyšek Stodůlka, Národní archiv

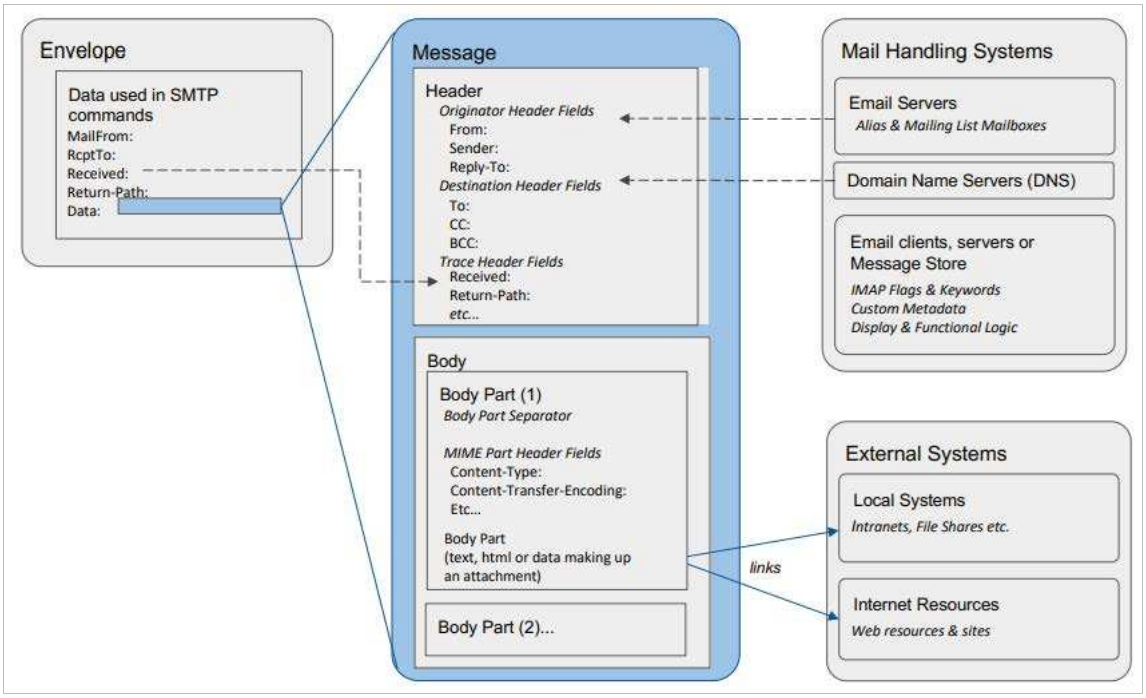
## Úvod

Podle odhadů dnes využívá e-mailovou komunikaci na 4.5 mld. lidí, tedy polovina světové populace, kteří každý den rozešlou 376.4 miliardy e-mailů. [1] E-mailová komunikace je s námi již více než padesát let, první pokusy probíhaly od 60. let 20. století. První e-mail obsahující oddělovač v podobě tzv. zavináče @ odeslal americký programátor Ray Tomlinson v roce 1971 v rámci sítě ARPANET, i když termíny jako elektronická pošta (electronic mail) a e-mail se začaly objevovat až později ve druhé polovině sedmdesátých let. Elektronická pošta se postupně stala součástí komerčního vývoje a standardizovaly se protokoly, které používáme dodnes. V roce 1982 byl vydán RFC 821 definující Simple Mail Transfer Protocol (SMTP) a RFC 822 pro formát zpráv, existovaly ale i jiné protokoly jako třeba X.400 nebo různá proprietární řešení jako známé Lotus Notes od IBM atd. Zasílání příloh bylo možné od roku 1992. Většího rozšíření se využívání elektronické pošty dočkalo až se zavedením první webové služby s názvem Hotmail a po akvizici společností Microsoft známé jako MSN Hotmail. Na aprílového 1. dubna 2004 spustila svůj freemailový server Gmail.com společnost Google. Z českých poskytovatelů byli na přelomu tisíciletí nejznámější Email.cz, Centrum.cz, Post.cz, Seznam.cz, Kiwwi.cz, Atlas.cz nebo třeba Katedrala.cz. [2]

## Akvizice a uchovávání

Vzhledem ke svému efemernímu charakteru a závislosti na použité technologii, se s ohledem na způsob využívání liší i strategie pro řádnou správu a případné dlouhodobé nebo i trvalé uložení. V průběhu doby se etablovaly několik hlavních formátů, se kterými se v oblasti archivace e-mailové komunikace pracuje:

| Formát | Otevřený/proprietární | Popis | Identifikace (PRONOM) |
|---|---|---|---|
| EML – Email Message Format | Otevřený | Jednotlivý e-mailový soubor | fmt/278 |
| MSG – Outlook Message Format | Binární (proprietární) | Jednotlivý e-mailový soubor ve formátu Microsoft Outlook | x-fmt/430 |
| MBOX – Mailbox File Format | Otevřený | Kontejner | fmt/720 |
| PST – Personal Storage Table | Binární (proprietární) | Archiv e-mailů a dat v Outlooku | x-fmt/248<br>x-fmt/249 |




*Obrázek č. 1: Datový model e-mailové zprávy (převzato z publikace Future of Email Archives 2018, s. 27) [3]*

V případě individuálního využívání doporučuje výzkumná zpráva Digital Preservation Coalition zohlednit následující kroky [4]:

1. Zjistěte, kde a jak jsou vaše e-mailové zprávy uloženy.
2. Odstraňte spam a nepoužitelné zprávy (např. oznámení ze seznamu), jakmile jsou přijaty.
3. Zajistěte, aby byla úložiště e-mailů synchronizována mezi zařízeními (tj. aby se odeslané zprávy ukládaly do stejného umístění na serveru).
4. Nakonfigurujte e-mailové klienty tak, aby uchovávali vzdálenou kopii všech odeslaných zpráv.
5. Oddělte staré zprávy ze své doručené pošty do samostatné složky „archiv" nebo „neaktuální", kde je méně pravděpodobné, že je smažete.
6. Pokud e-maily nebyly e-mailem zařazeny jako přijaté a odeslané, použijte filtry k vytvoření složek specifických pro projekt nebo téma.
7. Pokud je to možné, ukládejte všechny zprávy na server, nikoli do místních úložišť.
8. Mějte na paměti limity úložiště serveru.
9. Pochopte možnosti i omezení systémů vyhledávání e-mailů a složek.
10. Hromadné mazání a přenos provádějte s velkou opatrností.
11. Pokud je úložiště serveru neomezené, nebo prakticky ano, použijte jej jako střednědobý archiv.
12. Pokud je nutné zprávy ze serveru odebrat, exportujte a ukládejte zprávy ve formátu MBOX, PST nebo v jiném formátu a umístění, kde je lze procházet pomocí standardních nástrojů pro přístup k e-mailu. Pokud vaše organizace neposkytuje centralizovaný prostor pro takové soubory, může být nutné spolupracovat na jejich identifikaci.
13. Podnikněte několik jednoduchých kroků k zachování e-mailů. Pomocí cloudových e-mailových služeb, jako je Gmail nebo Outlook365, můžete stahovat a uchovávat e-maily a zjistit, jak lépe spravovat e-maily ve svých stávajících systémech.
14. Expertní tip #1: Prozkoumejte použití nástrojů pro osobní archivaci e-mailů k vytvoření osobních archivů e-mailů.
15. Expertní tip #2: Dlouhodobí uživatelé e-mailu mohou chtít identifikovat stará úložiště e-mailů ponechaná v počítačích

a zařízeních, poté je centralizovat na jednom místě a pomocí vhodných nástrojů je převést do formátu připraveného k uchování, jako je EML, MBOX nebo (méně ideálně) do proprietárního, ale a běžně používaného formátu PST.

Zatímco v případě osobního využití je na vlastní odpovědnosti zajištění odpovídajících nástrojů pro dlouhodobé uchovávání nebo zajištění přístupu k dané službě, je vhodné např. u akvizic pro trvalé uložení této e-mailové komunikace ve státním či jiném archivu již v předstihu komunikovat sladit výše uvedené kroky. Hranice mezi osobním a institucionálním využíváním e-mailové komunikace může být někdy velmi tenká, např. u akademických a výzkumných pracovníků nebo třeba politicky činných osob, které mohou působit napříč různými institucemi a při sdílení poznatků a zkušeností fakticky stírají hranice mezi profesní a soukromou sférou.

V případě institucí by měla být správa e-mailů součástí dobře definovaného systému správy dokumentů zohledňující dlouhodobou administrativní hodnotu, institucionální paměť nebo historickou hodnotu s formalizovanými pravidly výběru a přenosu do institucionalizovaných archivů. Jak však shrnuli v roce 2018 autoři výzkumné zprávy *The Future of Email Archives* i mnoho velkých organizací s dobrými zdroji se potýkalo s implementací politiky správy dokumentů zahrnující e-maily. V mnoha, ne-li ve většině organizací, se e-mail jen zřídka dostane z individuálních účtů uživatelů do obecného systému správy dokumentů. [5]

Značnou zásluhu na nastavení pravidel pro správu elektronických dokumentů, kam se e-maily ze své povahy také řadí, měl největší politický skandál 80. let, tzv. aféra Írán-Contras. Dotýkala se tehdejšího prezidenta Ronalda Reagana a jeho nejbližších spolupracovníků. Poradce pro národní bezpečnost admirál John Poindexter a jeho podřízený v Národní bezpečnostní radě (National Security Council) podplukovník. Oliver North realizovali utajený vývoz protitankových střel TOW do Íránu, který podléhal embargu a po islámské revoluci v roce 1979 deklaroval otevřeně nepřátelskou politikou vůči Spojeným státům včetně zadržování amerických diplomatů jako rukojmích. Ačkoli jedním z cílů bylo také navázání kontaktů s umírněnými íránskými politiky s cílem zprostředkovat propuštění amerických rukojmí zadržovaných libanonským hnutím Hizballáh, získané prostředky použila tato skupina k další utajené akci a to financování proti-sandinistických pravicových sil v Nikaragui. Když tato činnost vyplula v listopadu 1986 na povrch a bylo zřejmé, že nastane rozsáhlé vyšetřování, spolu s dalšími zaměstnanci Národní bezpečnostní rady účelově měnili a ničili dokumenty, které je usvědčovaly z nelegální činnosti. Jednalo se také o skoro 6000 e-mailových zpráv v rámci systému PROFS, které se však později podařilo obnovit ze zálohy a sloužily jako usvědčující materiál. Oliver North byl nakonec zproštěn obvinění na základě imunity, kdy spolupracoval s vyšetřovacími orgány na rozkrytí celého komplotu a John Pointdexter byl obvinění zproštěn v roce 1991 odvolacím soudem. [6]

Tento skandál odhalil nedostatky tehdy nastavené politiky správy dokumentů „vytiskni a zaeviduj" (print and file), kdy bylo zřejmé, že účastníci úmyslně tyto pravidla porušovali. Soudní spory vůči vládě se pak táhly ještě celá devadesátá léta, a to v podobě případu *Armstrong v. Executive Office of the President* a později *Public Citizen v. Carlin*. V prvním se podařilo prokázat žalobě v zájmu Národního bezpečnostního archivu (National Security Archive) podařilo prokázat, že elektronické dokumenty mají unikátní povahu a unikátní vlastnosti, které nejsou přenositelné v případě jejich převodu do analogového prostředí (metadata ke vzniku, oběhu atd.) a dosavadní politika jejich mazání s nástupem nové administrativy a spoléhání se na jejich vytištění a zaevidování, je chybná. V druhém případě, který se týkal mazání elektronických dokumentů poté, co byly převedeny a zaevidovány včetně metadat do evidence správy dokumentů v listinné nebo mikrofilmové podobě nakonec odvolací soud potvrdil. [7].

Tyto zkušenosti vzali do úvahy i autoři prvních verzí požadavků na správu dokumentů v elektronickém prostředí, tedy v elektronických systémech spisové služby. V americkém standardu DoD 5015.2 nalezneme jak definici elektronické poštovní zprávy: „*Dokument vytvořený nebo přijatý prostřednictvím systému elektronické pošty, včetně stručných poznámek, formálních nebo podstatných popisných dokumentů a jakýchkoli příloh, jako jsou textové a jiné elektronické dokumenty, které mohou být přenášeny se zprávou*", tak elektronického poštovního systému a v požadavku C2.2.4.1. „*Aplikace pro správu dokumentů by měla e-mailovými zprávami zacházet stejně jako s jakýmkoli jiným dokumentem a budou podléhat všem požadavkům tohoto standardu*". [8]

Nicméně po sérii skandálů rezonujících v tisku (např. k Internal Revenue Service, Centers for Medicare & Medicaid's Services a Environmental Protection Agency) a kongresových slyšení, ve kterých museli zástupci NARA reagovat na případy, kdy se s rozvojem e-mailové a jiné elektronické komunikace rostl počet případů jejich nedochování [9], což vyvolávalo otázky po nastavení a organizaci správy dokumentů, zejména s ohledem na transparentnost výkonu veřejné moci a práva občanů na kont-

rolu činnosti demokratických institucí (např. skrze aplikaci zákona o svobodném přístupu k informacím). Proto v roce 2010 zřídila NARA pracovní skupinu Správa e-mailů 2.0 (E-mail management 2.0), která postupně připravila metodologii Capstone. V té době zároveň připravila administrativa prezidenta Baracka Obamy rozsáhlou reformu správy dokumentů ve federálních institucích, která měla reflektovat otevřenost a odpovědnost federální správy, technologický rozvoj umožňující nové možnosti sdílení informací i efektivnější činnost a snížení výdajů díky standardizaci. Reformu zaštítilo Prezidentské memorandum o správě vládních dokumentů z 28. listopadu 2011, následované Směrnicí o vládních dokumentech (M-12-18) ze dne 24. srpna 2012. V oblasti elektronické komunikace byl federálním institucím stanoven cíl „do 31. prosince 2016 spravovat všechny e-mailové dokumenty v elektronickém formátu." V srpnu 2013 proto vydala NARA Bulletin 2013-02 „*Pokyny k novému přístupu ke správě e-mailů*" známý také jako „*Capstone Bulletin*". Strategie staví na principu definování stanovených pozic (tzv. Capstone Official), u kterých se uchovávají e-mailové účty a po 15–25 letech (nověji možno až po 30 letech) se předají do NARA [10]:

1. *Představený federální agentury, jako je ministr, komisař, administrátor, předseda nebo ekvivalent;*
2. *Hlavní asistenti představeného federální agentury (druhá úroveň managementu), jako jsou podsekretáři, asistenti tajemníků, asistenti komisařů a/nebo jejich ekvivalenty včetně důstojníků ozbrojených sil sloužící ve srovnatelných pozicích;*
3. *Zástupci všech funkcí v kategoriích 1 a 2 a/nebo jejich ekvivalent(y);*
4. *Asistenti personálu k těm v kategoriích 1 a 2, jako jsou speciální asistenti, důvěrní asistenti, vojáci atd.*
5. *Hlavní řídící funkce, jako je provozní ředitel, ředitel IT, ředitel pro řízení znalostí, technický ředitel a finanční ředitel a/nebo jejich ekvivalent(y);*
6. *Ředitelé významných programových kanceláří a/nebo jejich ekvivalent (y);*
7. *Hlavní regionální úředníci, jako jsou regionální správci a/nebo jejich ekvivalent (y);*
8. *Role nebo pozice, které agentuře běžně poskytují poradenství a dohled, včetně pozic v kategorie 1 až 3 a 5 až 7, včetně: generálních radních, náčelníků štábů, generálních inspektorů atd.;*
9. *Role a funkce výše nezastoupené a obsazené prezidentským jmenováním potvrzených Senátem a*
10. *Další role a pozice, které převážně vytvářejí dokumenty trvalé hodnoty týkající se kritických úkolů, funkcí nebo politických rozhodnutí a/nebo mají historický význam.* U ostatních zaměstnanců se mohou e-mailové účty smazat po sedmi letech, pokud nejsou potřeba déle a u administrativních a podpůrných činností po třech letech.

Přístup Capstone se záhy rozšířil a stal se etalonem nejen americké federální správy, ale také na úrovni jednotlivých amerických států. Implementovala jej v různé míře postupně řada zemí, jako jedni z prvních francouzská ministerstva a archivy, které již v roce 2013 rozsáhle zkoumaly, jakým způsobem realizovat správu e-mailů a jejich archivaci. Ministerstvo pro Evropu a zahraniční věci identifikovalo v rámci strategie Capstone kupříkladu přibližně 500 e-mailových účtů z 15.000, které spravovalo, zejména čelných představitelů a jejich zástupců. Úřad předsedy vlády se zaměřil na e-mailové účty přímých spolupracovníků premiéra a v rámci své vlastní činnosti na e-mailové účty nejvýše postavených úředníků, v menší míře také ze střední úrovně managementu. Aktivně tak úsek pro správu dokumentů (tzv. archivní mise) musí sledovat ukončení činnosti zaměstnanců, zejména po volbách. Tuto strategii doplňují ad hoc akvizice k vybraným událostem, jako byly např. účty pořadatelů Pařížského klimatického summitu 2015 nebo třeba zvládání pandemie COVID-19. Od roku 2014 tak došlo několika metodickými návody a doporučeními ke standardizaci přístupu v této oblasti, nyní podporované v rámci vládní strategie VITAM (Valeurs immatérielles transmises aux archives pour mémoire) jak metodicky, tak i softwarově pomocí nástroje ReSIP, jehož součástí je knihovna sedatools. Francouzský Národní archiv přijímá exporty účtů ve formátech .pst a .mbox, ze kterých tvoří balíček SIP. Dále vyžaduje, aby byly z těchto kontejnerů extrahovány zprávy ve formátech .eml a .txt a také přílohy, ze kterých se vytvoří pomocí nástroje ReSIP druhý SIP pro zpřístupnění. Aplikaci lze použít i pro další zpracování v podobě rozbalování příloh, mazání prázdných adresářů, adresářů obsahujících zprávy, které jsou považovány za soukromé, vizitky ve formátu VCF, loga ve formátu EMZ a soubory s příponou DAT. [11]

Implementace strategie Capstone v Evropě zrychlila i v návaznosti na průběh pandemie COVID-19, kdy veřejnost vice vystavila státní instituce a její představitele veřejné kontrole s ohledem na zásahy do občanských práv nebo s ohledem na výkon státní správy při zvládání následků pandemie. Kupříkladu Bersetova aféra ve Švýcarsku, spočívající v úniku informací o vládních proti-

covidových opatřeních do tisku, se snahou o zahlazení stop, nebo smazání e-mailů švédského hlavního epidemiologa Anderse Tegnella mělo dopad bylo mnohdy vnímáno jako selhání stávajících pravidel transparentního výkonu veřejné moci při správě dokumentů.

Evropský standard MoReq2, ze kterého byla odvozena v roce 2009 i česká implementace v podobě Národního standardu pro elektronické systémy spisové služby (VMV čá. 76/2009 (část II)), v kapitole 6.3 počítá se třemi variantami správy elektronické pošty. Výslovně si všímá problematického vztahu externího systému i možného problematického uživatelského chování: „*e-Mail se používá pro posílání dokumentů (ve formě zpráv a jako přílohy) uvnitř organizací a mezi nimi. Charakteristika softwaru pro správu e-mailů (zvláště nedostatek standardizace pro formáty vysvětlený nahoře) v kombinaci s uživatelskými přístupy vůči e-mailům, mohou činit funkčnost spisové služby obtížnou. Organizace musí být schopny zavést procedury a správu k: příjmu všech příchozích i odchozích e-mailů a příloh a/nebo příjmu e-mailů a příloh podle předdefinovaných pravidel a/nebo zajistit uživatelům možnost příjmu vybraných e-mailů nebo příloh. Každá organizace se musí rozhodnout, která z obou alternativ je nejvhodnějším kompromisem v následujících situacích: první možností je příjem jakýchkoli dočasných e-mailů i významných dokumentů; druhá možnost spoléhá na dobře nakonfigurovaná vhodná pravidla a filtry; třetí možnost vyžaduje, aby uživatelé posoudili význam prvků a existuje riziko, že ne všichni tak spolehlivě učiní. MoReq2 umožňuje ERMS podporovat všechny tři přístupy. Procedury a správa kontrol jsou mimo rozsah MoRequ2.*"

Klíčovým požadavkem se stal 6.3.2, který zní 6.3.2 „*ERMS musí podporovat příjem e-mailových zpráv integrovaným způsobem, tak aby příjem mohl provést uživatel v rámci působnosti aplikace elektronické pošty, tedy bez toho, že by uživatel musel přepnout režim na ERMS.*" A vysvětluje dále „*Úzká integrace je velmi důležitá pro efektivní využití ERMS. Uživatel by například měl být schopen provádět operace jako „táhni a pusť" z poštovního klienta do ERMS, nebo si zvolit z prostředí poštovního klienta příkaz „přijmout". Podstata tohoto požadavku tkví v tom, že uživatel nesmí být nucen přepnout do aplikace ERMS, aby mohl přijmout e-mailovou zprávu. MoReq rovněž dovoluje, ale nevyžaduje, příjem e-mailových zpráv jiným, ne tak těsně integrovaným způsobem.* [12]

Dle požadavku 6.3.3. ...musí být možné konfigurovat ERMS tak, aby v případě, kdy uživatel ERMS obdrží e-mailovou zprávu, reagoval ERMS jedním z následujících způsobů: automaticky zprávu přijme, pokud ještě nebyla přijata; rozhodne, zda e-mailovou zprávu přijme podle předem definovaných pravidel; nebyla-li e-mailová zpráva dosud přijata, automaticky informuje uživatele a nabídne mu možnost jejího přijetí; neprovede žádnou operaci.

Tehdejší Ministerstvo informatiky liberálně zakotvilo ve vyhlášce č. 496/2004 Sb., o elektronických podatelnách, povinnost orgánům veřejné moci přijímat datové zprávy prostřednictvím elektronické podatelny. Vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby, upravovala v § 2 odst. 1 povinnost předat dokument předaný původci mimo podatelnu bez zbytečného odkladu podatelně, zároveň v § 2 odst. 2 stanovila, že dokumenty, které z hlediska činnosti původce nemají úřední charakter, nepodléhají evidenci a charakteristiky takových dokumentů uvede původce ve spisovém řádu nebo jiném vnitřním předpisu.

Nová vyhláška č. 259/2012, o podrobnostech výkonu spisové služby, která nahradila i zrušenou vyhlášku o elektronických podatelnách, výslovně v § 5 odst. 1 poukazovala na situaci, kdy dochází ke komunikaci úředního charakteru na jiné elektronické adresy původce než je podatelna s tím, že pro něj vyplývá povinnost bezodkladně takový dokument označit a zaevidovat. V kontextu předchozí praxe se tak dělo namnoze přeposláním zprávy na adresu podatelny, která jej pak postoupila zpět prostřednictvím elektronického systému spisové služby namísto tehdy standardem MoReq doporučené integrace webového klienta s eSSL nebo třeba využitím funkce Drag&Drop, která ale povětšinou předpokládá práci s využitím dvou monitorů. Potvrzení, že dokumenty, které nemají úřední charakter, nepodléhají evidenci, se přesunula do znění § 9 odst. 3. Jakkoli není prostor v rámci tohoto příspěvku představit celou oblast judikatury týkající se doručování orgánům veřejné moci, je třeba poukázat na argumentaci v případě odmítnutí poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím s odkazem na skutečnost, že tato informace není součástí příslušného spisu. *Pokud je tedy povinnému subjektu doručena žádost o poskytnutí informací podle zákona o poskytnutí informací, musí, v souladu se zásadou dobré správy podle § 4 odst. 1 správního řádu, primárně vyvinout úsilí, aby nalezl požadovanou informaci a poskytl ji žadateli. Povinný subjekt tedy musí nejprve zkoumat, zda požadovanými informacemi fakticky disponuje, a to bez ohledu na to, jestli takovou povinnost má podle zákona o archivnictví a spisové službě či podle jakéhokoliv jiného právního předpisu. Pokud zjistí, že požadované informace má (i když je ze zákona shromažďovat nemusí), je povinen je žadateli poskytnout, nejedná-li se o výluky podle § 7 až 11 zákona o poskytnutí informací. Skutečnost, zda měl*

*povinný subjekt zákonem stanovenou povinnost danými údaji disponovat (například podle zákona o archivnictví a spisové službě nebo podle správního řádu), je relevantní až v okamžiku, kdy povinný subjekt po šetření zjistí, že požadované informace skutečně nemá, jelikož byly vymazány nebo odstraněny. V takovém případě má totiž podle výše citované judikatury Nejvyššího správního soudu povinnost je opět vytvořit.* Soud výslovně uvádí, že v daném případě doložení komunikace s externím subjektem měl povinný subjekt vyvinout „*nějakou aktivitu, například se dotázal příslušných úředních osob, které vedly správní řízení ve věci žalobce a které tak komunikovaly … a shromažďovaly příslušnou dokumentaci, pokusil se informace vyhledat ve svých interních databázích nebo e-mailových schránkách apod.*“ [13]

Jak správně konstatoval Národní úřad pro kybernetickou a informační bezpečnost, který od roku 2020 v rámci identifikace významných informačních systémů dle novelizované vyhlášky č. vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích od roku 2020, kam zařadil i elektronickou poštu: „*Kromě zákonem aprobovaného způsobu realizace správního podání nese elektronická pošta i další neopomenutelné prvky fungování orgánu veřejné moci, a to realizaci interních procesů souvisejících s výkonem jeho působnosti. Tyto interní procesy mohou nést důležité informace nebo osobní údaje a i přesto, že nejsou zachyceny podatelnou či spisovou službou, jsou pro fungování orgánu nepostradatelné. Aspekt ochrany elektronické pošty tak není myšlen pouze jako ochrana externí komunikace, ale i té interní, která mnohdy nese větší množství informací než samotný spis ke konkrétní věci.*“ [14]

Limity přístupu, který se spoléhá na zaevidování veškeré e-mailové komunikace ze strany zaměstnanců původce, navíc mnohdy ještě komplikovaným procesem skrze přeposílání na podatelnu, ukázal případ žádosti novináře, který žádal podle zákona č. 106/1999 Sb. o dokument prezentovaný na zasedání Rozpočtového výboru Poslanecké sněmovny ČR a dále o korespondenci mezi ministryní financí Alenou Schillerovou a tehdejším ředitelem Generálního finančního ředitelství Martinem Janečkem. V následné žalobě sice Ministerstvo financí uspělo s argumentací, že dokument není evidován v elektronickém systému spisové služby ministerstva a možnosti a oprávnění ministerstva nahlížet do e-mailové schránky ministryně financí a „e-mailová pošta mimo té, která je jako úřední zaváděna do spisové služby, nepodléhá povinné archivaci a nejedná se o informace, které by správní orgán prvního stupně měl, respektive musel mít k dispozici. Také se přiklonil k argumentaci žalované strany ve věci ochrany soukromí, kdy „*nelze přitom hovořit o odlišné povaze emailové schránky ministra oproti obecné ochraně soukromí zaměstnanců; ani ministra nelze vyloučit z ochrany soukromí, třebaže v konkrétním případě může mít jeho postavení na posouzení věci určitý vliv.*“ [15]

Poté, co Nejvyšší správní soud vrátil případ znovu k projednání, tentýž soud rozhodl znovu a tentokrát již ve prospěch argumentů žaloby s odůvodněním, že: „*…vlastní charakter požadované korespondence není pro odmítnutí jejího poskytnutí relevantní. Není tudíž rozhodné, zda žalobcem požadovaná informace byla jako úřední korespondence zaevidována ve spisové službě žalovaného prostřednictvím podatelna@mfcr.cz. či zda zůstala případně jako korespondence neúřední uložena ve správě samotné ministryně financí na adrese alena. schillerova@mfcr.cz. Provedeným dokazováním bylo zjištěno, že v rámci 20. schůze rozpočtového výboru Poslanecké sněmovny Parlamentu České republiky dne 20. 2. 2019 se ministryně financí opakovaně vyjádřila, že pracovníci finančních úřadů nejsou odměňováni v závislosti na výši doměřené daně… Ministryně byla finanční správou písemně ujištěna, že „podobná praxe se neděje“. Z uvedeného má soud za to, že žalobcem požadovaná korespondence ministryně financí týkající se tématu odměňování pracovníků finančních úřadů, jejíž existenci potvrdila na jednání rozpočtového výboru Poslanecké sněmovny, nemůže být hodnocena jako korespondence osobní a tedy neúřední. Nemůže proto obstát závěr žalovaného, že poskytnutí požadovaných informací odvisí od splnění povinnosti konkrétního pracovníka žalovaného zaevidovat úřední korespondenci do systému spisové služby. Soud přisvědčil žalobci i v tom, že poskytování informací požadovaného druhu, byť by korespondence proběhla přes e-mailovou adresu ministryně spravedlnosti alena.schillerova@mfcr.cz. což však ze sdělení o písemném ujištění explicitně nevyplývá, neboť druh písemné korespondence ministryně financí blíže nespecifikovala, lze výjimečně připustit, pokud v tom kterém posuzovaném případě dojde k provedení testu proporcionality práva žadatele na informace se zásahem do soukromí dotčené osoby (viz též rozsudek Nejvyššího správního soudu ze dne 30. 5. 2013, č. j. 4As 50/2012 -71.)*“. Soud však musel konstatovat, že rozhodnutí by bylo nevykonatelné, neboť „*v nyní posuzované věci existuje faktická překážka. V řízení před soudem totiž nebylo prokázáno ani osvědčeno, že informace v podobě písemného sdělení o žalobcem požadovaném obsahu existuje. Povinný subjekt tak nemohl poskytnout případnou e-mailovou korespondenci ministryně, která byla buď odstraněna, nebo průběžně smazána z důvodu omezené kapacity, přičemž je nutné zdůraznit, že ministerstvo obecně nemá povinnost vést e-mailovou korespondenci ministryně financí. Důvodem neposkytnutí informace je její faktická neexistence.*“ [16]

Soud velmi správně vystihl, i s ohledem na předchozí historický výklad, slabé místo současného přístupu, a to nedostatečnou záruku dochování dokumentu v případě, že spisová služba spoléhá na činnost zaměstnance v oblasti předání dokumentu k označení a evidenci. Je zřejmé, že e-mailová zpráva je dokument, přičemž v souladu s přílohou č. 2 zákona o archivnictví a spisové službě, budou podle obsahu vždy předloženy k výběru za archiválie mj. zakládací listiny, statuty, organizační řády a další dokumenty o organizační struktuře, vedení, správě, řízení, kontrole, činnosti a jejich výsledcích u orgánů zákonodárné, vládní a výkonné moci a orgánů územní samosprávy na všech stupních.

Jak jde vidět i z evropské praxe, kde je upravena problematika ochrany osobních údajů a soukromí více než v zámoří, je možné definovat postup pro výběr celých e-mailových účtů zaměstnanců původců s tím, že v rámci stanovené doby mohou před výběrem za archiváliii odstranit dokumenty osobní povahy. Takováto implementace strategie Capstone v prostředí české veřejné správy by mohla být koncipována na řídící stupně příslušných organizací, čímž by se do výčtu zahrnula administrativní podpora v podobě řízení kabinetů a kanceláří. Ze zahraniční praxe je zřejmé, že výčet aktérů cílí i na osoby v méně formálním vztahu k původcům (např. poradci a poradní orgány, odborné skupiny atd.), kteří mnohdy nejsou součástí spisové služby daného původce. S použitím soukromých e-mailů pro tuto činnost se může pojit i riziko v oblasti kybernetické bezpečnosti, proto může být jednodušší zřídit těmto osobám e-mailové účty institucionální, které pak budou podléhat stanoveným pravidlům. Formální akceptace pravidel pro nakládání a předání e-mailového účtu by mohlo být buď samostatně součástí spisového řádu původce nebo, jak je tomu i v zahraničí, součástí širšího pokynu k nakládání s e-mailovými a dalšími druhy komunikace včetně bezpečnostních požadavků atd.

## Výběr a zpracování

Vlastní provedení výběru archiválií může záviset na různém software a rozsahu prováděných uchovávacích opatřeních (migrace příloh atd.). Následující model poskytuje přehled, která metadata by měl archivář zahrnout z oblasti provenience a zpracování [17]:

**Kontext vytvoření e-mailu**

- Programy použité k vytvoření e-mailu (např. webové rozhraní Gmail nebo klient Microsoft Outlook)
- Použité platformy (výpočetní prostředí)
- Typ použití (pracovní, osobní, společný e-mailový účet s rodinou nebo organizací, mimoškolní činnost)
- Kdo účet používal (např. osoba nebo organizační jednotka složená z více osob)

**Kontext použití nebo správy dokumentů**

- Podrobnosti o účtu
- Název účtu / uživatelské jméno a právní / oficiální jméno
- Doba používání účtu
- Systém uspořádání (např. zda byly používány složky a jakým způsobem, zda byla složka „koš“ používána pro koncepty nebo pro revizi)

**Kontext uchovávání nebo archivní péče** *(mnohé z těchto činností mohou být zaznamenány jako události PREMIS)*

- Kdo materiály obdržel
- Jaké postupy byly použity k získání obsahu
- Jaké nástroje byly použity k inspekci, posouzení, inventarizaci, revizi a popisu materiálů
- Politiky uchovávání, které byly na materiály v průběhu času uplatněny (kdy, kým, za jakým účelem)

U osobních písemností nebo darovaných dokumentů externí organizace může být potřeba sledovat další metadata, například:

- Kritéria výběru
- E-mailové programy používané předávajícím
- Způsob, jakým archivář dokumenty převzal

**Vybrané nástroje pro podporu výběru a zpřístupňování e-mailové komunikace**

Následující přehled nekomerčních nástrojů, které slouží nejen v rámci aplikační praxe, ale jsou také součástí aktuálního výzkumu v dané oblasti. Je zřejmé, že v posledních letech dochází ke konsolidaci a integraci dostupných zdrojů do několika málo projektů, neboť se pro zpracování velkých textových zdrojů nabízí využití současného boomu nástrojů zpracování přirozeného jazyka (Natural Language Processing) včetně velkých jazykových modelů, deduplikace (zcelování vláken pro přehlednost a úsporu místa) atd.

ePADD (E-mail: Process, Appraise, Discover, Deliver)
Správa: konsorcium Stanford University, Harvard University a University of Manchester
Charakteristika: Aktuálně komunitně nejvíce podporovaná aplikace pro výběr, zpracování, uchovávání, a využívání sbírek e-mailových účtů využívaná od roku 2015 zejména v akademickém prostředí. Díky využití Java je multiplatformní. Zahrnuje i model a metody pro zpracování přirozeného jazyka (sémantické rozpoznávání), který umožňuje pokročilou indexaci a analýzu dat včetně případné anonymizace. Podporuje zpracování prostřednictvím formátu MBOX, případný převod je nutné realizovat komerčním softwarem Emailchemy.
Adresa: https://www.epaddproject.org

EMILiA
Správa: konsorcium Archiv der Max-Planck Gesellschaft a Freie Universität Berlin
Charakteristika: Moderní aplikace vyvíjená v etapách od roku 2024 s cílem poskytnout podporu výběru, zpracování i zpřístupňování sbírek e-mailových účtů. Využívá modelu zpracování přirozeného jazyka, rekonstrukci vláken k deduplikaci vícenásobného obsahu atd. Výstup pro digitální archivaci ve formátu BagIt.
Adresa: https://emilia-archiv.de

EA – PDF
Správa: konsorcium University of Illinois Library at the University of Illinois Urbana-Champaign a PDF/A Association
Charakteristika: Nejnovější výstup rozsáhlého amerického výzkumu, jehož cílem je poskytnout platformu vhodnou pro dlouhodobé uchovávání e-mailového obsahu s využitím současné technologie formátu PDF/A 3 a PDF/A 4, neboť uchovávání ve formátech jako MBOX, PST nebo EML vyžaduje buď využití e-mailových programů nebo transformaci, která není bezztrátová. K dispozici je i software Email2Pdf k tvorbě PDF/A souborů, které jsou v souladu s touto specifikací. Definuje následující profily [18]:

| | |
|---|---|
| PDF/mail-1s<br>„Single“ | Jedna e-mailová zpráva uchovaná jako jeden soubor EA-PDF, kde stránky představují vizuální reprezentaci pouze obsahu nebo kontextu daného e-mailu. Původní zdrojové e-mailové datové zdroje jsou vždy vloženy a jsou vloženy i další soubory, například přílohy e-mailů (pokud jsou k dispozici). |
| PDF/mail-1si<br>“Single, isolated” | Jedna e-mailová zpráva uchovaná jako jeden soubor EA-PDF, kde stránky představují vizuální znázornění obsahu nebo kontextu e-mailu, ale původní nezpracované zdrojové e-mailové datové zdroje nejsou vloženy. Mohou být vloženy další soubory (např. přílohy e-mailů). |

| | |
|---|---|
| PDF/mail-1m<br>„Multiple“ | Více e-mailů uchovávaných jako jeden soubor EA-PDF bez struktury složek, kde stránky v PDF jsou vizuální reprezentací obsahu nebo kontextu e-mailů. Původní nezpracované zdrojové e-mailové datové zdroje jsou vždy vloženy (věrně zachovány). |
| PDF/mail-1mi<br>“Multiple, isolated” | Více e-mailů uchovávaných jako jeden soubor EA-PDF bez struktury složek, kde stránky v PDF představují vizuální znázornění obsahu nebo kontextu e-mailů. Původní zdrojové e-mailové datové zdroje RAW vloženy nejsou, ale mohou být vloženy jiné soubory (např. přílohy e-mailů). |
| PDF/mail-1c<br>“Container” | „Strukturovaný kontejner“ EA-PDF pro jeden nebo více vložených souborů EA-PDF, z nichž každý může být libovolným jiným profilem PDF/mail-1. Soubory PDF/mail-1c mohou replikovat složité hierarchie složek, které se obvykle vyskytují v moderních e-mailových klientech, e-mailových formátech nebo souborových systémech. Kontejner jako soubor PDF/mail-1c neobsahuje stránky představující obsah zachovaných e-mailů – všechny reprezentace obsahu e-mailů ve formátu PDF jsou ve vložených souborech EA-PDF uložených v kolekci kontejnerových souborů PDF. Stránky v kontejnerovém PDF představují kontext kolekce. |
| PDF/mail-1ci<br>“Container, isolated” | „Strukturovaný kontejner“ EA-PDF pro jeden nebo více vložených souborů EA-PDF, z nichž každý může být libovolným jiným profilem PDF/mail-1. Soubory PDF/mail-1ci mohou replikovat složité hierarchie složek, které se obvykle vyskytují v moderních e-mailových klientech, e-mailových formátech nebo souborových systémech. Kontejner jako soubor PDF/mail-1ci neobsahuje stránky představující obsah uchovávaných e-mailů – veškerý obsah e-mailů je ve vložených souborech EA-PDF uložených v kolekci kontejnerových PDF. Stránky v kontejnerovém PDF představují kontext kolekce. Tento izolovaný profil označuje, že tento soubor EA-PDF neobsahuje úplnou sadu zachovaných původních nezpracovaných zdrojových e-mailových datových zdrojů pro všechny e-maily v kolekci, a proto není úplným formátem pro zachování. Může to být proto, že je zahrnut soubor PDF/mail-1{si, mi} nebo že samotný kontejner PDF/mail-1ci neobsahuje původní nezpracované zdrojové e-mailové datové zdroje. |

Adresa: https://pdfa.org/resource/ea-pdf; https://github.com/UIUCLibrary/ea-pdf

## Závěr

E-mailové komunikace do značné míry změnila za poslední tři desetiletí způsob výměny textového obsahu. I s ohledem na význam této komunikace, jeho jedinečnost a relativní ohrožení bylo nutné nalézt odpovídající strategie uchovávání tohoto digital-born obsahu. Je více než zřejmé, že spolehnutí se na evidenci této komunikace v prostředí elektronické správy dokumentů skrze její aktéry není dostatečným řešením a porušuje princip transparentního výkonu veřejné moci a kontroly činnosti demokratických institucí občany (např. skrze právo na svobodný přístup k informacím nebo skrze využívání dokumentů vybraných ve veřejném zájmu za archiválie. Řada evropských zemí nyní zavádí prvky strategie Capstone, tedy aktivní činnost původce a archivu na uchování e-mailové komunikace u představitelů veřejné moci. Uplatnění může nalézt i v kombinaci s akviziční činností archivů i v prostředí akademické a vědecké sféry či dalších oblastech. Díky dostupným nástrojům, které se rozvíjí jak komunitně, tak komerčně, se tak jedná o relativně metodicky uchopitelnou oblast, která má významnou informační hodnotu.

Literatura:

[1] THE RADICATI GROUP (2023). Email Statistics Report, 2023-2027. [cit. 2025-05-02]
Dostupné z https://www.radicati.com/wp/wp-content/uploads/2023/04/Email-Statistics-Report-2023-2027-Executive-Summary.pdf.

[2] IDNES.cz (2001). Test freemailů: Díl první – Email.cz [online]. 19. listopadu 2001 [cit. 2025-05-02]
Dostupné z: https://www.idnes.cz/technet/software/test-freemailu-dil-prvni-email-cz.A011119_0044486_software.

[3] TASK FORCE ON TECHNICAL APPROACHES FOR EMAIL ARCHIVES (2018). The Future of Email Archives. New York: Council on Library and Information Resources, s. 27. [cit. 2025-05-02] Dostupné z: https://www.clir.org/pubs/reports/pub175.

[4] PROM, Christopher J. (2019). Preserving Email (DPC Technology Watch Report). [cit. 2025-05-02]
Dostupné z http://doi.org/10.7207/twr19-01.

[5] TASK FORCE ON TECHNICAL APPROACHES FOR EMAIL ARCHIVES (2018), s. 11.

[6] WALLACE, David E. (2002). Implausible Deniability: The Politics of Documents in the Iran-Contra Affair and Its Investigations. In. Cox, Richard – Wallace, David E. (ed.): Archives and the Public Good. Accountability and Records in Modern Society. Westport, CT and London: Quorum Books, s. 91-114.

[7] WALLACE, David E. (2001). Electronic Records Management Defined by Court Case and Policy. Information Management Journal. Roč. 35, č. 1, s. 4-15.

[8] DEPARTMENT OF DEFENCE (2002). DoD 5015.02-STD. Design Criteria Standard for Electronic Records Management Software Aplication.

[9] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (2015). White Paper on The Capstone Approach and Capstone GRS (April 2015), s. 5an [cit. 2025-05-02]
Dostupné z: https://www.archives.gov/files/records-mgmt/email-management/final-capstone-white-paper.pdf.

[10] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (2023). GENERAL RECORDS SCHEDULE 6.1: Email and Other Electronic Messages Managed under a Capstone Approach, s. 20-22. [cit. 2025-05-02]
Dostupné z: https://www.archives.gov/files/records-mgmt/grs/grs06-1.pdf.

[11] VILLE Marion (2023). 2013 - 2023: a Review of Ten Years of Email Archiving in France. In: iPRES - 19th International Conference on Digital Preservation 2023: Conference Proceedings. [cit. 2025-05-02] Dostupné z: https://hdl.handle.net/2142/121102.

[12] DLM Forum (2008). MoReq 2. Modelové požadavky pro správu elektronických dokumentů., Bruxelles- Luxembourg: CECA-CEE-CEEA, s. 74-75. [cit. 2025-05-02]. Dostupné z: https://mv.gov.cz/sluzba/ViewFile.aspx?docid=21548245.

[13] NEJVYŠSÍ SPRÁVNÍ SOUD. 30. 5. 2019, č.j. 8 As 133/2017 – 56. [cit. 2025-05-02]. Dostupné z: https://www.nssoud.cz/stazeni-dokumentu?filepath=SOUDNI_VYKON/2017/0133_8As__1700056_20190619093755_20190624134032_prevedeno.pdf.

[14] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (2023). Průvodce identifikací významného informačního systému: podpůrný materiál, s. 27 [cit. 2025-05-02].
Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Pruvodce-identifikaci-VIS_v.

[15] MĚSTSKÝ SOUD V PRAZE. 20. 9. 2019, č.j. 11A 103/2019 – 25, s. 5-6. [cit. 2025-05-02]
Dostupné z: https://www.nssoud.cz/stazeni-dokumentu?filepath=EVIDENCNI_LIST/2019/11A_103_19_20191001130508_prevedeno.pdf.

[16] MĚSTSKÝ SOUD V PRAZE. 8. 10. 2020, č.j. 11A 103/2019 – 83, s. 6-7. [cit. 2025-05-02]
Dostupné z: https://www.mfcr.cz/assets/attachments/Zprava-Pr-001_2020_Rozsudek-c-j-11A-103-2019-83.pdf.

[17] TASK FORCE ON TECHNICAL APPROACHES FOR EMAIL ARCHIVES (2018), s. 48.

[18] PDF ASSOCIATION (2025). EA-PDF An archival email format based on PDF/A, s. 8-11. [cit. 2025-05-02]
Dostupné z: https://pdfa.org/download-area/specifications/EA-PDF-v1.pdf.

# Evropská peněženka digitální identity

Ing. Lenka Vaňková, Vysoká škola ekonomická v Praze,
Národohospodářská fakulta, Katedra práva

## Úvod

Od konce roku 2026 budou všechny státy EU muset nabídnout svým občanům, rezidentům a firmám alespoň jednu evropskou peněženku digitální identity. Veřejná správa je začne přijímat pro přístup k online službám, které vyžadují elektronickou identifikaci a ověření identity. Od konce roku 2027 vybrané soukromoprávní subjekty budou mít povinnost přijímat evropskou peněženku digitální identity podle požadavků uvedených v novém nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024 [21]. V současné době probíhají čtyři pilotní projekty na testování peněženek digitální identity EU, které financuje Evropská komise a na kterých se podílí jednotlivé členské státy EU, jakož i další nečlenské státy. Rozsáhlé pilotní projekty pomohou členským státům a dalším zúčastněným stranám připravit se na zavedení evropské peněženky digitální identity.

## Nástroj elektronické identifikace

Evropská peněženka digitální identity představuje moderní a inovativní způsob prokazování totožnosti nebo jiných informací online i osobně při jednání s úřady i soukromými firmami v celé EU a zajistí jejich držitelům bezpečný, důvěryhodný a jednoduchý přístup k různým veřejným i soukromým službám v celé EU. Občané navíc budou mít plnou kontrolu nad svými osobními údaji, protože každý uživatel je zároveň výhradním držitelem digitální peněženky, tudíž jen on sám rozhoduje, jaké údaje si do ní vloží a komu je zpřístupní. Princip digitálních peněženek je prostý a podobá se peněženkám fyzickým. Do evropské peněženky digitální identity si budou moci jejich uživatelé ukládat různé doklady a potvrzení z autorizovaných zdrojů v digitální podobě. Příkladem takových dokladů a potvrzení bude v budoucnu například mobilní řidičský průkaz, recept na léky nebo doklad o získané kvalifikaci. Výhodou je neomezená kapacita nebo schopnost prokázat se na jeden klik bez hledání konkrétní karty [1].

Používání digitální peněženky bude zcela dobrovolné, současné doklady a služby zůstanou. Uživatelé digitálních peněženek budou mít kontrolu nad svými údaji a pouze oni rozhodnou, co do peněženky vloží a které aspekty své identity a údajů budou sdílet se třetími stranami, což je zásadní přínos z pohledu bezpečnosti a ochrany soukromí. U některých služeb bude možné místo svého skutečného jména používat pseudonymy. Peněženky digitální identity EU budou k dispozici v celé EU pro přístup k veřejným a soukromým službám a budou dostupné pro všechny občany EU a firmy sídlící v EU, čímž se usnadní a zefektivní on-line interakce. Peněženka bude fungovat podle společných pravidel a umožní jak online, tak i prezenční (fyzickou) osobní identifikaci. Digitální peněženky EU budou licencovány s otevřeným zdrojovým kódem, což zajistí transparentnost a bezpečnost. Peněženky budou nabízet uživatelsky přívětivé rozhraní. Občané budou moci k registraci peněženek využívat vnitrostátní systémy elektronické identifikace, což zajistí hladký přechod na správu digitální identity. Tím, že poskytuje bezpečné a ověřitelné prostředky k prokázání totožnosti, může pomoci omezit krádeže totožnosti a související podvody, pokud jde o služby veřejné správy. Peněženky mohou snížit náklady spojené s procesy ověřování totožnosti tím, že je zjednoduší a automatizují. Přijetí peněženek identity může podnítit inovace, což povede k novým službám a produktům. Celkově může větší přijetí on-line transakcí, nové obchodní příležitosti a lepší přidělování zdrojů přispět k celkové hospodářské stabilitě a růstu [1], [5].

Peněženku vytváří poskytovatel národní peněženky digitální identity, kterého určí členský stát. Tento poskytovatel vyvine a zprovozní aplikaci, především v podobě mobilní aplikace nebo například i v podobě webové (cloudové) aplikace či jiných formách, ve stanoveném termínu a podle specifikací dohodnutých na úrovni EU. Uživatel si pak může peněženku stáhnout / aktivovat a začít ji používat [1].

## Právní základ

Nové nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se zřizuje rámec pro evropskou digitální identitu, vychází z nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (detailně viz [2], [3] a [4]). Toto nařízení, které je všeobecně známé pod zkratkou eIDAS, jež vychází z anglického „Electronic Identification and Services", sjednotilo zejména právní úpravu týkající se služeb vytvářejících důvěru pro elektronické transakce, kam spadá zejména elektronické podepisování a elektronické pečetění [6]. Stěžejním středobodem novelizace nařízení eIDAS je zavedení povinného vytvoření systémů pro elektronickou identifikaci všemi členskými státy a realizace tzv. evropské peněženky digitální identity. Podle citovaného předpisu má jít o produkt a službu, které uživateli umožní uchovávat údaje o totožnosti, pověření a atributy spojené s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, přičemž tyto služby budou dostupné jak pro veřejný, tak i soukromý sektor [7].

Peněženky digitální identity EU budou vycházet z vnitrostátních systémů, které již v některých členských státech existují. Nové nařízení stanoví, že digitální identity budou i nadále poskytovat členské státy. Evropská peněženka digitální identity vychází z tohoto základu, rozšiřuje funkce a použitelnost vnitrostátních elektronických průkazů totožnosti a zajišťuje vzájemné uznávání vnitrostátních peněženek ostatními členskými státy. [5].

V očekávání tohoto vývoje, neboť novelizace nařízení eIDAS byla připravována několik let, přistoupila Česká republika k vlastnímu projektu, který může být do jisté míry chápán jako národní trénink na evropskou peněženku digitální identity, která bude platná napříč celou Evropskou unií a bude obsahovat i další dokumenty a certifikáty [8]. Jde o vytvoření mobilní aplikace, která umožní uchovávat a používat digitální stejnopisy průkazů. Proto byl v samém začátku roku 2024 novelizován zákon č. 12/2020 Sb., o právu na digitální služby, a to zákonem č. 1/2024 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Otevřela se tak možnost vytváření digitálních stejnopisů průkazů a jejich ukládání v mobilní aplikaci. Pro tento nástroj se používá označení eDoklady [9].

## Evropská peněženka v ČR

Česká republika, stejně jako ostatní členské státy EU, musí zajistit vydání alespoň jedné evropské peněženky digitální identity. Tento závazek má být splněn do 24 měsíců od data, kdy vstoupily v platnost prováděcí akty stanovující technické detaily peněženek a souvisejícího ekosystému. S ohledem na skutečnost, že prováděcí akty byly již schváleny a publikovány, tak povinnost zajistit vydávání evropské peněženky digitální identity vychází na závěr roku 2026 [12].

Pověření k realizaci evropské peněženky digitální identity v České republice získala Digitální a informační agentura (dále DIA) formou koncese, tedy prostřednictvím soukromého poskytovatele pověřeného státem, na základě usnesení, které bylo schváleno na jednání vlády 26. března 2025 [10]. Koncesní model představuje formu veřejně-soukromé spolupráce, kde stát pověří soukromou firmu vývojem a provozem digitální peněženky výměnou za právo spravovat systém po dohodnutou dobu a realizovat komerční příjmy ze souvisejících činností. Stát si ponechává kontrolu nad právními, bezpečnostními a legislativními aspekty, zatímco soukromý poskytovatel nese náklady na vývoj, technickou správu, inovace a denní provoz [11]. Toto řešení kombinuje technologickou flexibilitu a schopnost inovovat, kterou přináší soukromý sektor, s kontrolou státu nad klíčovými bezpečnostními, právními a legislativními aspekty. V neposlední řadě je levnější [10].

DIA v současné době provádí nezbytné analytické a přípravné práce. Pro adaptaci právního řádu bude nutné novelizovat některé zákony, čímž se zajistí zohlednění nových požadavků eIDAS 2 v českém právním řádu. Konkrétně půjde zejména o zákon č. 250/2017 Sb., o elektronické identifikaci, a zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce [13].

## Pilotní projekty

V rámci čtyř velkých pilotních projektů, viz tabulka 1 (detailně viz [15], [16], [17] a [18]), které byly zahájeny v dubnu 2023, se před zavedením evropské peněženky digitální identity v členských státech testují její specifikace v širokém spektru případů použití.

Testování se zaměřuje na scénáře každodenního používání, jako je přístup k digitálním službám, platby, cestování a vzdělávání. Cílem je ověřit a získat zkušenosti, jak peněženka bude moci fungovat v těchto předpokládaných případech použití. Digitální a informační agentura se účastní dvou projektů LSP, jež vychází z anglického „Large Scale Pilots", a sice projektu POTENTIAL a projektu EWC.

| **Pilotní projekt** | | **Koordinátor** | **Členské státy** | **Instituce** |
|---|---|---|---|---|
| POTENTIAL | Pilots for European Digital Identity Wallet Consortium | Německo, Francie | 19 členských států + Ukrajina | 140 veřejných a soukromých institucí |
| EWC | EU Digital Identity Wallet Consortium | Švédsko | 19 členských států + Norsko a Spojené království | 77 veřejných a soukromých institucí |
| NOBID | Nordic-Baltic eID Wallet Consortium | Norsko | 4 členské státy + Norsko a Island | 20 veřejných a soukromých institucí |
| DC4EU | Digital Credentials for Europe Consortium | Španělsko | 20 členských států + Ukrajina, Norsko a Švýcarsko | 99 veřejných a soukromých institucí |

*Tab. 1: Pilotní projekty evropské peněženky digitální identity. Zdroj: tabulka vlastní konstrukce, data: [15], [16], [17] a [18].*

Projekt POTENTIAL (Pilots for European Digital Identity Wallet Consortium) podporuje inovace, spolupráci a růst v šesti odvětvích digitální identity – vládní služby, bankovnictví, telekomunikace, mobilní řidičské průkazy, elektronické podpisy a zdravotnictví [14], [20].

Projekt EWC (EU Digital Identity Wallet Consortium) je společným úsilím o využití přínosů navrhované digitální identity EU ve formě digitálních cestovních certifikátů ve všech členských státech. Evropská rada zaměstnanců má v úmyslu vycházet z aplikace referenční peněženky s cílem umožnit použití související s digitálními cestovními certifikáty [14], [20].

Projekt NOBID (Nordic-Baltic eID Wallet Consortium) je soubor severských a pobaltských zemí, které společně s Itálií a Německem pilotně používají peněženku digitální identity EU pro schvalování plateb za produkty a služby [14], [20].

Projekt DC4EU (Digital Credentials for Europe Consortium) poskytuje hmatatelnou podporu veřejnému a soukromému sektoru v oblasti vzdělávání a sociálního zabezpečení zaváděním nejmodernějších infrastruktur transevropských interoperabilních digitálních služeb a přístupem k nim a jejich začleněním do přeshraničního rámce pro důvěryhodnost [14], [20].

Pilotní projekty konkrétně zkoumají, jak může digitální peněženka poskytnout řešení v těchto 11 oblastech: 1. přístup k elektronickým službám veřejné správy, 2. založení bankovního účtu, 3. registrace předplacené SIM karty, 4. mobilní řidičský průkaz, 5. kvalifikovaný elektronický podpis, 6. elektronický recept, 7. digitální cestovní doklady, 8. příslušnost k určité organizaci, 9. autorizace plateb prostřednictvím peněženek, 10. vzdělání a odborná kvalifikace, 11. využití v rámci sociální oblasti včetně získání a sdílení Evropského průkazu zdravotního pojištění (detailně viz [19]) [14], [20].

Do pilotních projektů je zapojeno přes 300 subjektů, včetně soukromých společností a veřejných orgánů z 27 členských států, Norska, Islandu, Švýcarska, Spojeného království a Ukrajiny, podrobněji viz tabulka 2. Každý pilotní projekt je strukturován jako konsorcium, které spojuje odborné znalosti z veřejného i soukromého sektoru v rámci EU, přičemž spolufinancování je poskytováno z grantů Evropské komise. Tyto pilotní projekty by měly pokračovat až do konce roku 2025 [20].

| **Členské státy EU** | **Zapojení v pilotních projektech** | | | |
|---|---|---|---|---|
| | POTENTIAL | EWC | NOBID | DC4EU |
| Belgie | x | x | | x |
| Bulharsko | | x | | |
| Česko | x | x | | x |
| Dánsko | | x | x | x |
| Německo | x | x | x | x |
| Estonsko | x | x | | |
| Irsko | | | | x |
| Řecko | x | x | | x |
| Španělsko | x | x | | x |
| Francie | x | x | | x |
| Chorvatsko | | x | | |
| Itálie | x | x | x | x |
| Kypr | x | | | |
| Lotyšsko | | | | |
| Litva | x | | x | x |
| Lucembursko | x | x | | x |
| Maďarsko | x | x | | x |
| Malta | | | | x |
| Nizozemsko | x | x | | x |
| Rakousko | x | | | x |
| Polsko | x | x | | x |
| Portugalsko | x | x | | x |
| Rumunsko | | x | | x |
| Slovinsko | x | | | |
| Slovensko | x | | | |
| Finsko | x | x | | x |
| Švédsko | | x | | x |
| Státy mimo EU | | | | |
| Ukrajina | x | | | x |
| Norsko | | x | x | x |
| Island | | | x | |
| Švýcarsko | | | | x |
| Spojené království | | x | | |

*Tab. 2: Státy zapojené do pilotních projektů evropské peněženky digitální identity. Zdroj: tabulka vlastní konstrukce, data: [15], [16], [17] a [18].*

## Shrnutí

Revize nařízení eIDAS přináší několik významných změn, mezi které patří zavedení evropské peněženky digitální identity, která občanům umožní bezpečně ukládat, spravovat a ověřovat osobní údaje a elektronické doklady. Zavedení evropských peněženek digitální identity bude významným milníkem na cestě Evropy k digitalizaci [22].

Pilotní projekty důkladně testují peněženku digitální identity EU v celé řadě společných scénářů, s nimiž se Evropané setkávají ve svém každodenním životě. Česká republika se podílí na dvou pilotních projektech POTENTIAL a EWC. Více jak polovina členských států je zainteresována na třech pilotních projektech zároveň, Německo a Itálie se účastní všech čtyřech pilotních projektů.

Pověření k realizaci evropské peněženky digitální identity v České republice získala Digitální a informační agentura. Implementace evropské peněženky digitální identity bude náročným projektem, a to nejen technicky a organizačně, ale i finančně. Současně se ale jedná o nezbytný krok, který zajistí konkurenceschopnost České republiky v oblasti digitální transformace, umožní plnit závazky vůči Evropské unii a nabídnout občanům i podnikům moderní digitální služby [10].

Literatura

[1] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Co je evropská peněženka digitální identity a proč se zavádí* [online]. Dostupné z <https://www.eudiw.dia.gov.cz/evropska-penezenka/co-je-evropska-penezenka-digitalni-identity-a-proc-se-zavadi>.

[2] LECHNER, T. *Nařízení eIDAS a české adaptační zákony. Komentář.* 1. vyd. Praha: Wolters Kluwer ČR, 2023. 488 s. ISBN 978-80-7598-924-6.

[3] DUMORTIER, J. Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). In: *EU Regulation of E-Commerce*. Edward Elgar Publishing, 2017. s. 256-289.

[4] CUIJPERS, C. M. K. C., SCHROERS, J. eIDAS as guideline for the development of a pan European eID framework in FutureID. *Gesellschaft fur Informatik*, 2014, č. 7, s. 23–38.

[5] EVROPSKÁ KOMISE. *Nařízení o evropské digitální identitě (EUDI)* [online]. Dostupné z <https://digital-strategy.ec.europa.eu/cs/policies/eudi-regulation>.

[6] SMEJKAL, V., KODL, J., UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*, 2015, č. 11.

[7] VAŇKOVÁ, L., LECHNER, T. K čemu jsou užitečné eDoklady. *Odhadce a oceňování majetku. 2024*, roč. 30, č. 3-4, s. 77-85. ISSN 1213-8223.

[8] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *eDoklady v mobilu: Elektronické doklady v mobilním telefonu* [online]. Dostupné z <https://www.dia.gov.cz/co-delame/edoklady-v-mobilu/>.

[9] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *eDoklady* [online]. Dostupné z <https://edoklady.gov.cz/>.

[10] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Digitální a informační agentura získala pověření k realizaci evropské peněženky digitální identity v ČR formou koncese* [online]. Dostupné z <https://eudiw.dia.gov.cz/aktuality/digitalni-a-informacni-agentura-ziskala-povereni-k-realizaci-evropske-penezenky-digitalni-identity-v-cr-formou-koncese>.

[11] ADVOKÁTNÍ DENÍK. *Evropská digitální peněženka usnadní přístup k veřejným i soukromým službám* [online]. Dostupné z <https://advokatnidenik.cz/2025/03/28/evropska-digitalni-penezenka-usnadni-pristup-k-verejnym-i-soukromym-sluzbam/>.

[12] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Harmonogram realizace a zpřístupnění peněženky v ČR* [online]. Dostupné z <https://eudiw.dia.gov.cz/evropska-penezenka-stav-v-cr/harmonogram-realizace-a-zpristupneni-penezenky-v-cr-2>.

[13] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Plány do budoucna* [online]. Dostupné z <https://eudiw.dia.gov.cz/evropska-penezenka-stav-v-cr/plany-do-budoucna>.

[14] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Zapojení DIA v rámci Large Scale Pilots (LSP)* [online]. Dostupné z <https://eudiw.dia.gov.cz/evropska-penezenka-stav-v-cr/zapojeni-dia-v-ramci-large-scale-pilots-lsp>.

[15] POTENTIAL. (2023). Potential For European Digital Identity. Dostupné z <https://www.digital-identity-wallet.eu/>.

[16] DC4EU. (2025). Digital Credential for Europe Consortium. Dostupné z <https://www.dc4eu.eu/>.

[17] NOBID. (2025). Nordic-Baltic eID Wallet Consortium. Dostupné z <https://www.nobidconsortium.com/>.

[18] EWC. (2022-2025). EU Digital Identity Wallet Consortium. Dostupné z <https://eudiwalletconsortium.org/>.

[19] EUROPEAN COMMISSION. *The many use cases of EU Digital Identity Wallets* [online]. Dostupné z <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet>.

[20] EVROPSKÁ KOMISE. *Pilotní zavedení peněženky digitální identity EU* [online].
Dostupné z <https://digital-strategy.ec.europa.eu/cs/policies/eudi-wallet-implementation>.

[21] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Důležité milníky k procesu tvorby peněženky digitální identity – časová osa* [online]. Dostupné z <https://www.eudiw.dia.gov.cz/evropska-penezenka/dulezite-milniky-k-procesu-tvorby-penezenky-digitalni-identity-casova-osa>.

[22] DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *DIA – Evropská peněženka digitální identity* [online]. Dostupné z <https://eudiw.dia.gov.cz/>.

---

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/38/2021.

# AI Asistent pro Ředitelství silnic a dálnic: Digitalizace práce se směrnicemi na míru

Valdemar Závadský, Cloudfield

## Digitalizace jako klíč k efektivní správě

Efektivní práce s dokumenty je ve veřejné správě zásadní pro transparentní řízení procesů, právní jistotu a eliminaci chyb. Ředitelství silnic a dálnic s. p. (dále jen „ŘSD“), které spravuje rozsáhlou síť dálniční a silniční infrastruktury v České republice, pracuje s množstvím technických předpisů, interních i rezortních směrnic, metodických pokynů a dalších dokumentů určujících pravidla pro přípravu a realizaci staveb, správu majetku a administraci veřejných zakázek. Správné a rychlé dohledání relevantních informací je klíčové nejen pro efektivitu, ale i pro správnou aplikaci pravidel a zajištění souladu s platnými předpisy.

Přestože ŘSD disponuje systémem pro správu dokumentů s podporou různých verzí dokumentů, zaměstnanci naráželi na několik komplikací. Dokumenty existují v různých formátech a jejich vyhledávání bylo zdlouhavé. Právě zde sehrála roli naše expertíza – nejen jako dodavatele technologie, ale i jako konzultanta, který pomohl identifikovat problémy a navrhnout řešení na míru.

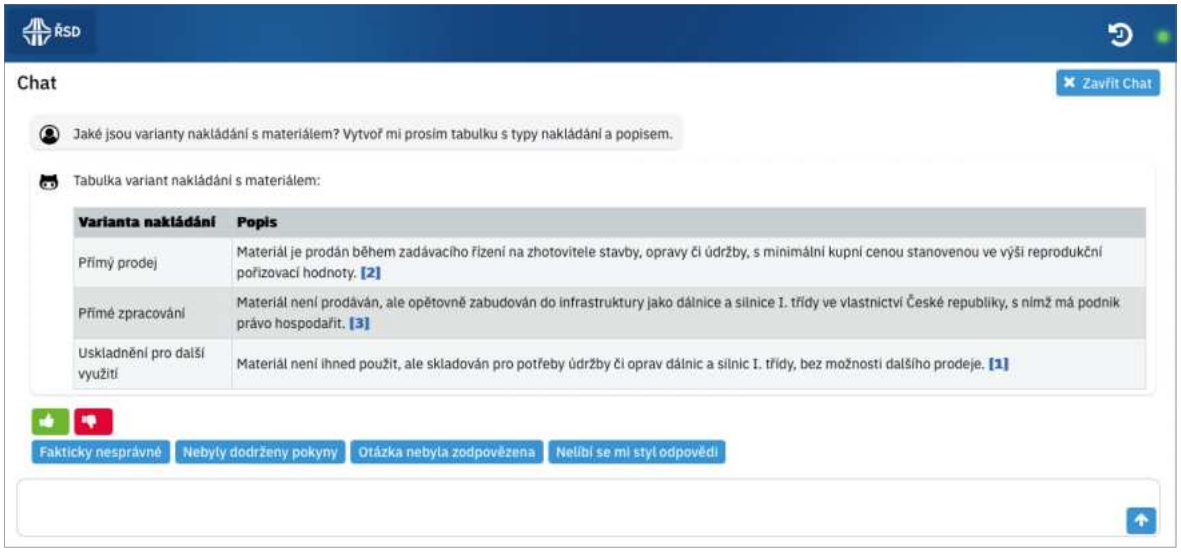
Mnoho organizací si není jistých, jak jim AI může pomoci v jejich každodenní práci. Proto jsme v rámci spolupráce s ŘSD využili naši interní **platformu DOC BRO** – nikoliv jako hotový produkt, ale jako sadu nástrojů a metodologií, které jsme přizpůsobili konkrétním potřebám klienta. Díky tomuto přístupu se podařilo navrhnout řešení, které nejen respektuje stávající IT infrastrukturu a postupy, ale zároveň efektivně využívá sílu umělé inteligence pro lepší přístup k informacím.

## Od výzev k řešení: AI jako nástroj pro snadnější práci se směrnicemi

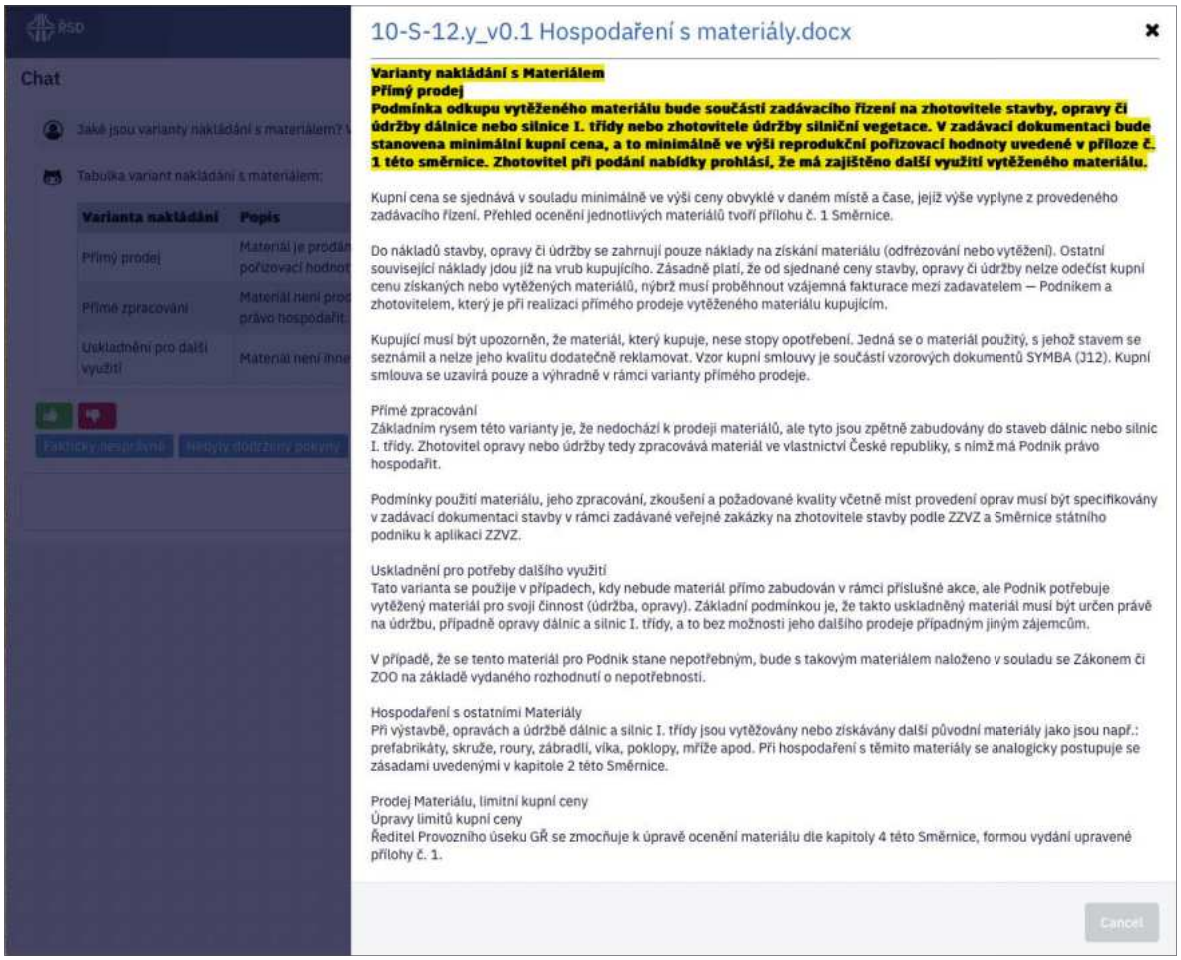
Před nasazením AI asistenta se zaměstnanci ŘSD potýkali s několika komplikacemi. Vyhledávání informací bylo časově náročné, s ohledem na velké množství dokumentů a jejich obsahu, s mnohdy složitými právními či technickými formulacemi, navíc uložených v různých formátech. Zaměstnanci potřebovali mít také jistotu, že pracují s aktuálními informacemi, ale zároveň mít možnost přistupovat i k historickým verzím předpisů.

Nové řešení tuto potřebu **plně respektovalo a zachovalo funkcionalitu správy verzí dokumentů**, která již byla v ŘSD zavedená. Klíčovým rozdílem však bylo **rozšíření těchto funkcionalit** o umělou inteligenci, která zajišťuje **významové vyhledávání, interpretaci obsahu a rychlejší zpřístupnění dokumentů.**

AI asistent umožňuje uživatelům klást otázky v přirozeném jazyce, na něž poskytuje odpovědi nejen na základě shody klíčových slov, ale také sémantické analýzy textu. To znamená, že zaměstnanci nemusí znát přesné formulace v dokumentech – stačí položit otázku, a systém jim nabídne nejen relevantní pasáže směrnic, ale i jejich shrnutí v kontextu daného dotazu.




Protože pracovník nese plnou odpovědnost za správnou aplikaci pravidel, AI asistent zároveň **umožňuje snadné ověření odpovědí pomocí referencí do původních dokumentů**. Každý výstup tedy obsahuje přímé odkazy na konkrétní směrnice nebo na související podklady, aby uživatelé měli jistotu, že interpretace je správná a že mohou důvěřovat uvedeným informacím.



Pokud je potřeba pracovat s dokumentem k určitému datu, AI automaticky zohlední jeho tehdejší platnost a nabídne odpovídající verzi.

## Technologická architektura: Přizpůsobení řešení na míru

Aby bylo řešení plně funkční v kontextu provozu ŘSD, bylo nezbytné jej **integrovat do stávající infrastruktury a zachovat kompatibilitu s existujícími systémy**. Zaměstnanci zůstali u svých původních účtů v **Azure Entra**, čímž bylo zajištěno, že přístup k dokumentům nadále odpovídá existujícím pravidlům oprávnění.

Celková architektura kombinuje **interní infrastrukturu ŘSD** s cloudovými službami v **Azure**, kde běží AI modely zpracovávající přirozený jazyk. Díky této hybridní koncepci organizace těží z výhod moderních AI technologií, aniž by byla závislá na kompletním přesunu dat do externího cloudu.

Významnou součástí implementace byla i **podpora optického rozpoznávání znaků (OCR)**, která umožňuje AI pracovat nejen s elektronickými dokumenty, ale i s naskenovanými materiály. To je zásadní pro práci s historickými nebo fyzickými dokumenty, které dosud nebylo možné snadno vyhledávat.

Důležitým aspektem bylo i **respektování znalostního kontextu**. Umělá inteligence byla konfigurována tak, aby rozuměla specifické terminologii a pravidlům platným pro silniční hospodářství. Tím se výrazně zvýšila relevance a přesnost odpovědí – AI nenabízí jen obecné informace, ale skutečně reflektuje konkrétní podmínky a potřeby ŘSD.

## Bezpečnost a kontrola nad řešením

Při práci s interními dokumenty hraje zásadní roli bezpečnost a kontrola nad daty. Ačkoliv je pro zpracování využíván jazykový model provozovaný v cloudovém prostředí, veškerá komunikace probíhá za přísných bezpečnostních podmínek. Data nejsou nikde ukládána, nejsou přístupná třetím stranám a nejsou využívána k tréninku jazykového modelu. Řešení bylo navrženo tak, aby ŘSD mělo plnou kontrolu nad výsledným systémem – včetně administrace, know-how a správy výstupů – a zároveň byla zajištěna maximální ochrana citlivých informací.

Veřejné instituce často čelí riziku dlouhodobé závislosti na externích dodavatelích softwaru, což může být problematické z hlediska financování, flexibility i bezpečnosti. **V našem přístupu jsme se této závislosti vyhnuli** – systémové know-how bylo předáno interním zaměstnancům ŘSD, kteří jsou schopni systém samostatně spravovat.

Zabezpečení přístupu k dokumentům je navíc připraveno pro řízení pomocí **role-based access control (RBAC)**. Tento systém řízení přístupových práv umožňuje nejen **omezit přístup k dokumentům podle oprávnění jednotlivých zaměstnanců**, ale zároveň **zohledňuje organizační strukturu**. To znamená, že například pracovníci jednotlivých regionů mají přednostní přístup k dokumentům relevantním pro jejich oblast, i když si mohou nahlédnout i do směrnic jiných regionů.

## AI jako transformační nástroj pro veřejnou správu

Nasazení AI asistenta v ŘSD představuje ukázkový příklad, jak může umělá inteligence **prakticky a efektivně pomoci veřejné správě**. Největší přidanou hodnotou není pouze technologie samotná, ale přístup, který umožnil **přesné přizpůsobení potřebám organizace**.

Díky propojení AI s existující správou dokumentů jsme dokázali **zachovat zavedené postupy**, a přitom je obohatit o nové možnosti, **které výrazně zrychlují a zpřesňují práci s vnitřními předpisy**.

# Řešení NIS2: Efektivní strategie pro zajištění bezpečnosti Vaší organizace

Michal Zedníček, Head of CyberSecurity Business Consulting, ALEF

NIS2 se stává symbolem současné éry, ačkoli ne vždy spravedlivě. Zaměňování cíle a prostředků je běžnou praxí, která přivádí NIS2 do popředí naší pozornosti. Jak se s tím vypořádat? Rychle a efektivně?

Můžeme vám nabídnout:

- Nejlépe hodnocený SIEM současnosti: Splunk SIEM formou služby, nebo dodaním produktu do vašeho prostředí
- Gap analýzu: Detailní zhodnocení a identifikaci nedostatků.
- Řízení aktiv a rizik: Efektivní řízení zdrojů a minimalizace rizik.
- Bezpečnostní dokumentaci: Komplexní dokumentaci zajišťující dodržení předpisů.
- Prevenci proti útokům: Aktivní ochranu a reakci v případě úspěchu útoku.
- Řízení kontinuity: Zajištění nepřerušeného chodu vaší organizace.
- Implementaci technické bezpečnostní architektury: Navrhnutí a nasazení technologických opatření.
- Vzdělávání zaměstnanců: Zvýšení povědomí a školení pro efektivní reakci na hrozby.

Další služby podle Vašich potřeb – jsme tu pro Vás.

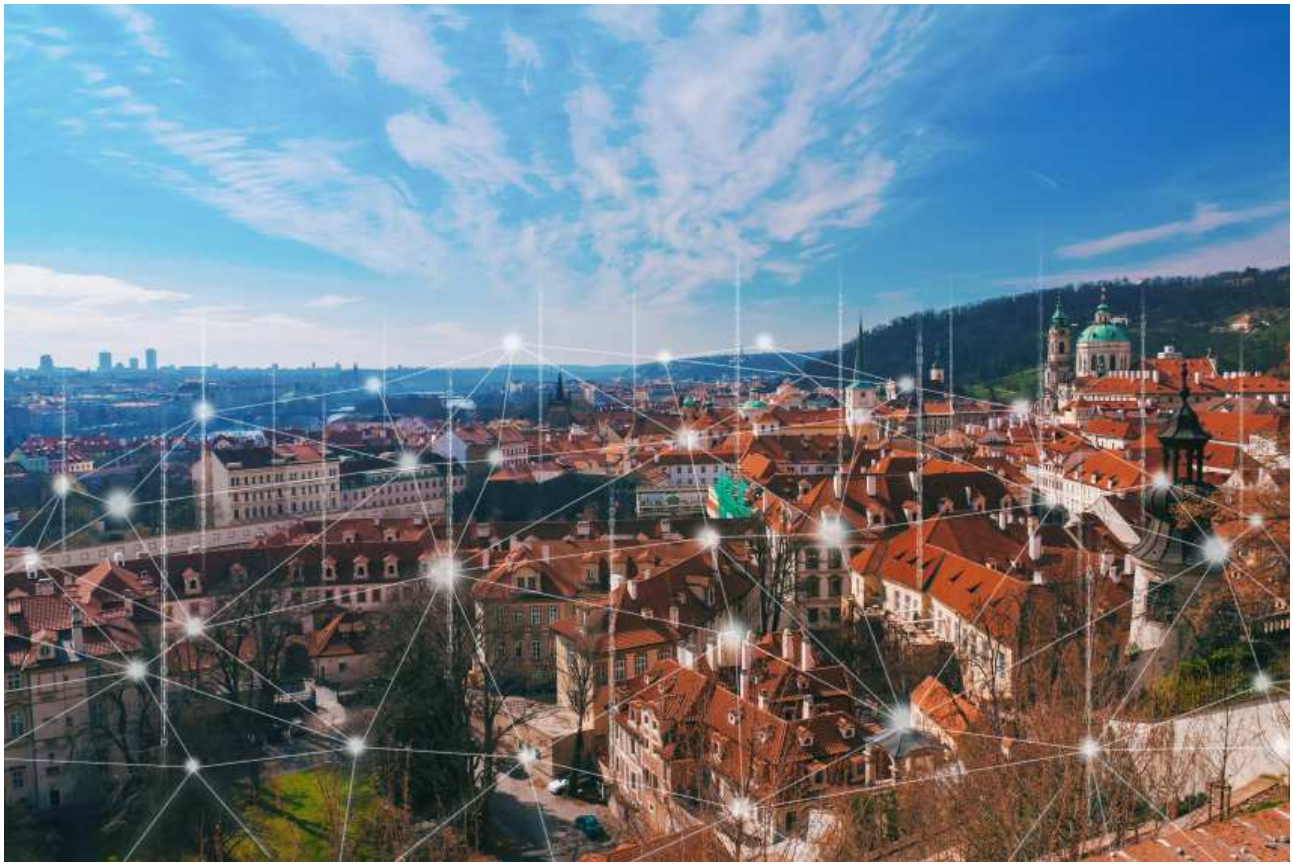
Zaměřujeme se na konzultační přístup s důrazem na porozumění Vašeho prostředí:

- Hodnocení zralosti prostředí: Posouzení bezpečnostního povědomí, procesní vyspělosti, technické odolnosti a přístupu bezpečnostních rolí.
- Vhodný postup implementace: Navrhnutí optimálního tempa zavádění procesů, úrovně vzdělávání, technické architektury a respekt k finančním možnostem organizace.

Naším cílem je vytvořit odolné prostředí s ohledem na Vaše zdroje a akceptovatelné riziko.

Zajímá Vás více? Domluvte si s námi nezávaznou hodinovou konzultaci. Během 60 minut Vám rádi přiblížíme, jakou hodnotu můžeme přinést Vaší organizaci.

# Zabezpečení sítě CETIN a dat našich zákazníků je pro nás stále tou nejvyšší prioritou



Provozujeme a vlastníme největší telekomunikační síť pokrývající celé území České republiky, prostřednictvím pevných a mobilních technologií pokrýváme 99,6 % populace. Naše síť zajišťuje kritickou informační infrastrukturu a díky špičkovým odborníkům a moderním technologiím **stanovujeme nejvyšší standardy kybernetické bezpečnosti**. Přivádíme do českých domácností nejvyspělejší optickou síť, stavíme 5G infrastrukturu a díky profesionálům v oboru máme možnost nabízet spolehlivé a bezpečné velkoobchodní telekomunikační služby.

Moderní kritické služby se stále více spoléhají na komplexní síťovou architekturu, včetně cloudového ukládání dat. To vede k nárůstu tzv. povrchovým útokům – citlivá data jsou distribuována na více místech. Proto je stále důležitější, aby jejich **přenos zajišťovala robustní, důvěryhodná a dostatečně kapacitní infrastruktura**, která je nepřetržitě monitorována nejmodernějšími obrannými nástroji.

## VÝHODY KRITICKÉ TELEKOMUNIKAČNÍ INFRASTRUKTURY PRO MĚSTA I OBCE

Protože vnímáme telekomunikační služby jako čtvrtou základní lidskou potřebu po vodě, elektřině a plynu, investujeme do modernizace telekomunikačních sítí měst i menších obcí v České republice.

V rámci zkvalitňování spolupráce se samosprávami provedla v prosinci roku 2024 společnost IPSOS nezávislý výzkum, který mapoval slabá místa při rozhodování i procesu realizace výstavby optické sítě v obcích. **93 % zástupců obcí potvrzuje**, že jsou spokojeni s komunikací se společností CETIN. **Dvě třetiny z nezasíťovaných obcí** plánují v příštích letech zavedení optické sítě.

Našimi robustními investicemi a spoluprací s místními samosprávami se snažíme zajistit, aby obyvatelé České republiky mohli využívat výhody rychlého a bezpečného internetu. Naší hlavní misí je být spolehlivým partnerem pro obce a jejich obyvatele, poskytovat nejvyšší standardy kybernetické bezpečnosti a podporovat digitální transformaci v celé zemi.

**www.cetin.cz**

# Novinky v inkoustovém kancelářském tisku

Společnost Epson doplňuje a inovuje své portfolio inkoustových kancelářských tiskáren. Na konci loňského roku uvedla tiskárnu formátu A4 WorkForce Pro EP-C800 a multifunkční zařízení EM-C800. Tato zařízení směřují do malých a středních kanceláří a představují alternativu menších laserových tiskáren s rychlostí tisku 25 A4 stran/min. Aktuální novinku v produktové řadě představují kompaktní multifunkční tiskárny AM-C400/C550, které nabízejí kancelářský tisk formátu A4 rychlostí 40/55 A4 stran/min. Dále také zařízení RIPS s vysokou kapacitou inkoustu EM-C8100/C8101 formátu A3 a rychlostí 25 A4/min. Tato zařízení doplňují řadu A3 tiskáren Workforce AM-C a Enterprise, která tak nabízí rychlosti tisku od 20 do 100 A4 stran/min.

Inkoustové tiskárny Epson používají osvědčené piezoelektrické hlavy PrecisionCore navržené na celou životnost zařízení bez nutnosti výměny. Při tisku se nevytváří škodlivý ozón a množství prachových částic je výrazně nižší než u laserových tiskáren, což umožňuje nasazení nejen v kancelářích, ale i v čistých provozech, jako jsou laboratoře či nemocnice. Tiskový proces je studený, tedy Heat-Free, neohřívá okolní prostředí a vyniká nízkou spotřebou energie. Spotřeba je výrazně nižší než u srovnatelných laserových tiskáren. Pokud tedy provozujete větší množství tiskáren, mohou úspory za energii představovat položku v řádu desítek tisíc korun za rok. Nižší spotřeba elektrické energie Heat-Free technologie má také enviromentální rozměr v podobě redukce množství $CO_2$.

Významná je u inkoustových zařízení také úspora času a pokud platí, že čas jsou peníze, každý kratší pracovní proces přináší finanční úsporu. Inkoustové tiskárny jsou mistrem v rychlosti tisku krátkých dokumentů do 3–5 stran, kterých je v dnešních kancelářích většina. To tyto tiskárny odlišuje od laserových tiskáren nejen stejné, ale i vyšší rychlostní kategorie, protože inkoustová tiskárna vytiskne 3–4stránkový dokument dříve, než se laserová stihne připravit (zahřát) před tiskem. Uživatel tak neztrácí čas při čekání na výtisk. Další časovou úsporu představují vysokokapacitní zásobníky inkoustu ať ve formě zásobníků až na 84 000 stran či dolévacích zásobníků EcoTank tiskáren, které není potřeba často měnit či doplňovat. Inkoustové tiskárny mají minimum vyměnitelného spotřebního materiálu v průběhu své životnosti, neztrácíte tak čas čekáním na servis a provedením pravidelné údržby. Inkoustové tiskárny Epson lze vzdáleně monitorovat prostřednictvím cloudového řešení Epson Remote Services, pomocí kterého může zajistit váš partner plynulé dodávky inkoustů, kontrolu stavu počítadel a případný servis bez zásahu uživatele či IT oddělení.

Při zvyšující se ceně dopravy představuje úsporu také logistika spotřebního materiálu a likvidace odpadu. Inkoustové tiskárny používají až o 90 % méně spotřebního materiálu a obalů než laserové tiskárny srovnatelné kategorie. Úspora v dopravě a při likvidaci odpadu je tedy nesporná.

Je jen na uživateli, zda si vybere výkonné tiskárny a multifunkční zařízení řady Epson WorkForce, anebo zařízení s inkoustovými zásobníky Epson EcoTank. Kancelářská zařízení Epson používají inkousty na bázi pigmentu, které se vyznačují výbornou barevností, ostrostí textu, světlostálostí pro archivní použití a odolností vůči vodě a zvýrazňovačům. K dispozici máme celou řadu zařízení, ze kterých si můžete vybrat na základě svých potřeb a požadavků na barvu, rychlost, softwarové vybavení, kompatibilitu se systémy řízení tisku, zásobu papíru a zpracování nestandardních materiálů.

**Informace o metodice srovnání naleznete na www.epson.cz/heat-free-technology**


EPSON®

# HP Workforce eXperience Platform: Zajištění výkonnosti a dostupnosti IT infrastruktury

V dnešní dynamické technologické éře, kdy jsou organizace stále více závislé na stabilní a efektivní IT infrastruktuře, se proaktivní správa a monitorování systémů stávají klíčovými faktory úspěchu.

Společnost HP v této oblasti již dříve nabízela a u zákazníků implementovala služby jako Proactive Insights a ActiveCare, které byly postavené na cloudové analytické platformě TechPulse. Nyní přichází s výrazným rozšířením funkcí, a to pod novým názvem **Workforce eXperience Platform (WXP)**, který reflektuje širší pokrytí nejen v oblasti správy hardwaru, ale i řízení celého ekosystému IT zařízení.

WXP je inovativní nástroj, který pomáhá organizacím zajistit vysokou dostupnost, výkon a bezpečnost jejich IT prostředí. Tento článek se zaměřuje na klíčové funkce, výhody a přínosy, které WXP moderním organizacím přináší.

## Co je HP WXP?

HP WXP je komplexní sada nástrojů pro správu a monitorování IT infrastruktury, která umožňuje organizacím předvídat a řešit problémy dříve, než se stanou kritickými. Tento nástroj je součástí širší nabídky služeb HP zaměřených na správu systémů a optimalizaci jejich výkonnosti. Hlavním cílem WXP je zjednodušení správy IT a minimalizace rizika výpadků či neplánovaných odstávek, které mohou negativně ovlivnit chod organizace.

## Hlavní funkce HP WXP

HP WXP nabízí širokou škálu funkcí, které pomáhají IT týmům efektivně monitorovat, spravovat a optimalizovat jejich infrastrukturu. Mezi hlavní funkce patří:

1. **Prediktivní analýza a monitoring**: HP WXP využívá pokročilou analýzu dat pro monitoring výkonu systémů v reálném čase a identifikaci potenciálních problémů dříve, než se stanou kritickými. IT specialisté tak mohou na rizika reagovat s předstihem a provádět opravy ještě před možným výpadkem nebo poklesem výkonu. Systém podporuje monitoring široké škály zařízení, včetně osobních počítačů, monitorů, dokovacích stanic, tiskáren a audio-video vybavení konferenčních místností.
2. **Automatické aktualizace a opravy**: Na základě analýzy systém doporučuje a provádí automatizované aktualizace hardwaru i softwaru, čímž zajišťuje jejich aktuálnost a bezpečnost. Tato funkcionalita pomáhá minimalizovat bezpečnostní rizika a zvyšuje celkovou spolehlivost infrastruktury.
3. **Pokročilé reporty a přehledy**: HP WXP generuje detailní reporty poskytující přehled o výkonu, zdraví a dostupnosti IT prostředí. Reporty lze přizpůsobit specifickým potřebám organizace a využít je jako klíčový nástroj pro rozhodování a optimalizaci systémů.
4. **Integrace s dalšími nástroji a platformami**: HP WXP je navrženo tak, aby bylo kompatibilní s různými IT nástroji pro správu a monitorování, což zajišťuje komplexní a centralizovanou správu systémů v organizaci.
5. **Nepřetržitá podpora a vzdálená diagnostika**: HP nabízí 24/7 podporu, která pomáhá organizacím rychle řešit jakékoli vzniklé problémy. Vzdálená diagnostika umožňuje technikům analyzovat systémové potíže bez nutnosti fyzické přítomnosti na místě, což šetří čas i náklady.
6. **Správa majetku (Asset management)**: WXP poskytuje detailní informace o instalovaných zařízeních, jejich výkonu, době užívání, servisním pokrytí a kompatibilitě s novými softwarovými systémy i bezpečnostními standardy.

7. **Analýza uživatelské spokojenosti (User Sentiment Analysis)**: IT oddělení mohou prostřednictvím cílených kampaní získávat zpětnou vazbu od uživatelů na prováděné změny a porovnávat ji s výsledky monitoringu a analytických výstupů.

## Přínosy pro organizace

HP WXP přináší organizacím řadu výhod, mezi které patří:

1. **Zvýšení dostupnosti a snížení rizika výpadků**: Prediktivní analýza a monitoring umožňují včasné odhalení problémů, čímž se minimalizuje riziko neplánovaných odstávek. To zajišťuje nepřerušený provoz organizace.
2. **Optimalizace nákladů: Díky automatickým aktualizacím** a preventivním opatřením lze snížit náklady na opravy a údržbu. IT týmy se tak mohou více soustředit na inovace a strategický rozvoj namísto řešení problémů, kterým bylo možné předejít.
3. **Zlepšení bezpečnosti**: Automatizované aktualizace a opravy minimalizují bezpečnostní hrozby a zajišťují, že všechny systémy jsou chráněny proti známým kybernetickým útokům.
4. **Zjednodušení správy**: Centralizovaný přístup k monitorování a správě systémů umožňuje IT týmům efektivněji řídit celou infrastrukturu a usnadňuje koordinaci mezi jednotlivými odděleními.
5. **Zlepšení výkonu systémů**: Detailní přehledy a reporty umožňují organizacím pravidelně optimalizovat výkon svých systémů a eliminovat slabiny, které by mohly negativně ovlivnit jejich efektivitu.

## Závěr

HP WXP je pokročilý nástroj pro proaktivní správu a monitorování IT infrastruktury, který organizacím pomáhá zajistit vysokou dostupnost, výkon a bezpečnost. Díky prediktivní analýze, automatizovaným aktualizacím a pokročilému reportování mohou organizace včas identifikovat problémy a minimalizovat rizika spojená s výpadky. Tím zvyšují efektivitu, snižují náklady a zjednodušují správu své IT infrastruktury. **HP WXP je klíčovým řešením pro organizace, které chtějí optimalizovat svůj IT ekosystém a zaměřit se na prevenci problémů namísto jejich reaktivního řešení.**

# IT z pohledu byznysu
# byznys z pohledu IT


Předplatné, ceny inzerce, ediční plán
a další informace o časopisu IT Systems najdete na

**www.SystemOnLine.cz**

# Umělá data
## jako nástroj bezpečného sdílení dat

V dnešní době, kdy je ochrana soukromí důležitější než kdy dříve a zároveň roste poptávka po širším sdílení dat, přinášejí umělá data revoluční řešení.

Moderní technologie generování umělých dat umožňují organizacím využívat hodnotu dat, aniž by ohrozily citlivé informace jednotlivců nebo firem.

### Co jsou umělá data?

Umělá data jsou pečlivě vytvořené datové sady, které zachovávají statistické vlastnosti původních dat, ale neobsahují žádné skutečné údaje. Jsou ideální náhradou reálných dat pro analýzy, vývoj, testování i otevřené sdílení.

### Proč?

> Moderní anonymizace
> Flexibilita v generování dat
> Bezpečná náhrada reálných dat
> Ochrana soukromí s minimálním rizikem
> Podpora spolupráce a bezpečné sdílení dat

### Kde?

> *Státní správa*: Efektivní sdílení dat mezi úřady při zachování ochrany soukromí občanů.

> *Akademie*: Bezpečný přístup studentů a výzkumníků k realistickým datům.

> *Byznys*: Vývoj inovativních produktů bez rizika úniku citlivých informací.

### Budoucnost je v bezpečných datech

Umělá data otevírají nové možnosti využití dat bez zbytečných rizik. Umožňují spolupráci a inovace bez rizika ztráty důvěry.

JN ANALYTICS

*Odemkněte potenciál svých dat – bezpečně a bez obav.*

# Datová centra K-net

**Kam bezpečně ukládat data? Čemu dát přednost – veřejnému cloudu velkých provozovatelů nebo vybudování vlastního datového centra? To jsou otázky, které začaly v K-netu rezonovat již před patnácti lety. K-net se rozhodl jít vlastní cestou.**

### Může datové centrum K-net vůbec konkurovat velkým provozovatelům cloudových řešení?

My se samozřejmě nemůžeme srovnávat s cloudy světových hráčů. A také nikomu nemůžeme říkat, aby do veřejného cloudu nechodil. Spousta firem upřednostňuje uložení dat a jejich zálohování v cloudech nadnárodních firem a má pro to dobrý důvod – levné základní předpřipravené služby. Ty může využít jak nadnárodní subjekt s vlastním velkým IT oddělením, tak malá organizace, kde ekonomika hraje prim a není potřeba poradenství spojené s jedinečností konkrétních IT řešení. Ale pro české subjekty, které potřebují postihnout jedinečnost svého prostředí při rozumných ekonomických výdajích a mít data uložena na konkrétním místě u českého partnera, a to nemusí být samozřejmě jenom K-net, může být místní datové centrum velmi dobrá volba. V našem posledním realizovaném datovém centru v Olešnici jsme vše připravili tak, aby i naše datové centrum mělo všechny potřebné atributy, aby bylo koncipováno chytře a pokud možno co nejzeleněji.

### Co to znamená „co nejzeleněji“?

To znamená, aby opravdu mělo co nejmenší dopad na energetickou spotřebu zdrojů a na životní prostředí.

### Může datové centrum K-net poskytovat certifikované služby pro veřejnou správu?

Ano, naše datové centrum splňuje certifikaci pro provoz eGovernment Cloudu, včetně jeho potřebných bezpečnostních úrovní. Provozovaná datová centra, tedy i data v nich se nacházejí na území České republiky.

### Máte datová centra v Praze, Brně a Olešnici, tedy na geograficky oddělených lokalitách. Považujete to z hlediska práce s daty klientů za důležité?

Ano. Nejkratší vzdálenost mezi lokalitami je cca 50 km mezi Brnem a Olešnicí na Vysočině. Má to i tu výhodu, že mezi nimi jsou trochu kopečky, takže v případě šíření řekněme nějaké vlny, ať už uměle vyvolané nebo z hlediska nějaké přírodní katastrofy, jsou místa pěkně oddělená. Pro nás to byl úplně zásadní důvod, abychom pro naše klienty měli bezpečná místa, kde můžeme mít data nebo kopie dat, o která se staráme a máme za ně spoluzodpovědnost.

### Představte si následující situaci: Jsem firma a vybírám si cloud, do kterého chci uložit svá data. Proč byste mi doporučil právě K-net?

Protože jsme blízko, protože mluvíme česky, protože používáme nejmodernější technologie, protože jsme schopni daleko lépe posoudit rozsah úlohy, protože jsme schopni využívat i jiné zdroje tady v České republice.

Hlavní výhodou Cloudového centra K-net je jeho nekompromisní bezpečnost, vysoká dostupnost a přístup k odbornému týmu. Na rozdíl od veřejného cloudu, kde je přístup k odborníkům omezený a často finančně náročný, K-net nabízí přímou podporu a konzultace s našimi specialisty. Tím zajišťujeme, že vaše data jsou nejen bezpečně uložena, ale také neustále chráněna a spravována s maximální péčí. S K-net získáte partnera, který se postará o všechny aspekty vašeho IT včetně kybernetické bezpečnosti, což vám umožní soustředit se na to, co je pro vás nejdůležitější – poskytování služeb veřejnosti.

# Královéhradecké tržiště: Nový impuls pro místní producenty a veřejné stravování

Královéhradecký kraj spouští **objednávkový portál pro veřejná stravovací zařízení a místní producenty**, který má za cíl propojit regionální výrobce potravin s těmi, kdo vaří ve školních jídelnách, nemocnicích nebo dalších veřejných institucích. Projekt s názvem **Královéhradecké tržiště** přináší moderní, jednoduchý a přehledný způsob, jak zkrátit dodavatelské řetězce a posílit **lokální soběstačnost v oblasti potravin**.

## Co je cílem tržiště?

Hlavní motivací kraje je **podpora místních producentů**, využití regionálních surovin a **zvýšení kvality stravování ve veřejných zařízeních**. Tržiště navazuje i na principy projektu **Skutečně zdravá škola**, který zdůrazňuje význam čerstvých a lokálních surovin pro zdravé stravování dětí.

Královéhradecký kraj má co nabídnout – množství kvalitních producentů, farmářů i malých výrobců. Nový portál jim otevírá cestu k institucím, které by jinak často volily velkoobchodní dodavatele.

## Kdo se může zapojit?

Projekt je určen nejen pro **školy, školky a nemocnice**, ale i pro jiné instituce zajišťující veřejné stravování a restaurace, které volí cestu využití sezónních a lokálních surovin. Na druhé straně se tržiště otevírá **všem registrovaným producentům a potravinářům** z Královéhradeckého kraje, případně i krajů sousedních.

Královéhradecký kraj

# Řešení pro moderní eGovernment od Monet+

Zakázkový vývoj informačních systémů, software pro výrobu a personalizaci dokladů či konzultace a návrh řešení. To vše jsou kompetence zlínské firmy Monet+.

## Identitní řešení pro moderní stát

Technologie Monet+ propojují občany s veřejnými službami a zajišťují bezpečný přístup k citlivým datům pro moderní eGovernment na úrovni vysoká. K dodávaným systémům poskytujeme profesionální servis a průběžný rozvoj dle specifických požadavků. Naše řešení zajišťují bezpečnou identifikaci uživatelů, ověření jejich identity a vytváření elektronických podpisů. Díky tomu umožňujeme důvěryhodnou digitální komunikaci mezi občany, firmami a státem.

## Digitalizace osobních dokladů

Dodáváme řešení pro výrobu, personalizaci, vydávání a akceptaci národních elektronických dokladů, včetně obslužných systémů a uživatelských aplikací. Digitalizujeme původní agendy a zjednodušujeme práci úředníkům. Stojíme za projekty, jako jsou elektronické občanské průkazy, elektronické cestovní pasy, povolení k pobytu, digitální tachograf či řidičské průkazy. Díky našim technologiím již bylo vydáno přes 31 000 000 osobních dokladů.

## Zakázkový vývoj informačních systémů

Jsme český software house se specializací na aplikovanou kryptografii a infrastrukturu veřejných klíčů (PKI). Díky našemu expertnímu know-how navrhujeme a vyvíjíme zakázkové informační systémy a aplikace určené pro podporu občanů i veřejné správy.

## Ochrana přístupů do systémů a prostor s ProID

Nástroje ProID jsou samostatnou produktovou řadou, která představuje komplexní řešení Workforce Security – bezpečné pracovní identity zaměstnanců. Jedná se o ucelené produktové řešení, obsahující uživatelské nástroje a metody (čipové karty, mobilní aplikace a obslužný software) pro bezpečné multifaktorové přihlašování do počítačů, systémů a VPN. Toto přihlašování je například vyžadováno i novou evropskou směrnicí NIS 2.

**Více o nás naleznete na webech www.monetplus.cz a www.proid.cz.**

**Zaujala vás naše řešení? Navštivte náš stánek č. 54 (v přízemí u vchodu do VIP zóny).**

MARBES

www.marbes.cz

# Návod, jak získat 1. místo v soutěži

# EGOVERNMENT THE BEST 2024

## Case Study projektu Koordinované stanovisko pro Magistrát Hl. města Prahy.

### O projektu

Zákazník: **Magistrát Hlavního města Prahy**
Dodavatel: **Marbes s.r.o.**
Téma: **Řízení procesu vyjadřování a schvalování za použití standardů eGovernmentu**

### Důležité je zadání a motiv

Hlavním motivem změny zastaralá aplikace s nižším standardem podpory a možnostmi rozvoje. Výzvou projektu bylo samotné nasazení aplikace se zcela novým mechanismem schvalování a moderním vizuálem. To znamenalo přesvědčit koncové uživatele o nutnosti přechodu do 21. století. Další výzvou byla migrace dat z původní aplikace a čištění zastaralých a chybných dat.

### O co v projektu šlo?

Aplikace Koordinovaného stanoviska usnadňuje tvorbu souhrnných dokumentů, koordinovaných stanovisek a vyjádření, na kterých se podílí více zpracovatelů (odborů, oddělení či referentů). Skvěle se hodí pro tvorbu závazných koordinovaných stanovisek či jednotných environmentálních stanovisek. Usnadňuje plánování a hlídání termínů s přehledy pro koordinátora, vedoucího i referenta. Důležité je napojení na systém základních registrů pro verifikaci dat.

### Slovo zákazníka

**Ředitel odboru informatických činností Mgr. Jiří Károly:**

*„Projekt koordinovaného stanoviska byl dodán včas, řádně a bez větších problémů. Implementovaná aplikace pomáhá pracovníkům napříč odbory MHMP, a i proto je připravován její významný rozvoj v rámci úřadu.“*

### Výsledky, přínosy, poznatky a doporučení

**5 měsíců od 11/23 do 03/24**
Délka projektu

**12 konzultantů a expertů magistrátu**
Projektový tým

**40 lidí ve 2 odborech magistrátu**
Základní počet uživatelů

**Java aplikační server, Oracle databáze a webový klient**
Na čem to běží

**tisíce ročně**
Počet žádostí

**desítky tisíc dokumentů**
Migrace

**základní skupinou 40 expertů**
Počet uživatelů

**klíčová je spolupráce se zákazníkem v oblasti analýzy a přípravy dat**
Doporučení

### Závěr

Aplikace zjednodušila a zpřehlednila celý proces vyjadřování, který lze použít v mnoha procesech úřadu. Zásadním usnadněním je užití typizovaných šablon, které v sobě obsahuje procesy, texty, osoby k vyjádření, předvyplňové údaje, kontrola ze základních registrů.

# Pohodlné řešení správy identit od Orchitech

**Získejte kontrolu nad přístupy vašich uživatelů a vyřešte požadavky nového zákona o kybernetické bezpečnosti. S naším IDM budou mít všichni přesně ty přístupy, které potřebují, a žádné jiné.**

Pracovníci odborů informatiky tráví zbytečně mnoho času zakládáním účtů v jednotlivých systémech, řešením problémů s hesly, auditem přístupů nebo přidělováním oprávnění, místo aby se věnovali klíčovým prioritám organizace. Procesy spojené s nástupem/odchodem zaměstnanců a jejich přístupy jsou na nich zcela závislé.

## Řešením je zavedení IDM, které přináší:

- automatické řízení změn v oblasti správy uživatelů a jejich oprávnění
- průkazná workflow (personální, schvalovací a systémová)
- intuitivní rozhraní pro uživatelský self-service
- eliminaci manuálních chyb (chybné či duplicitní zadání)
- přehledný reporting identit a jejich oprávnění
- napojení na všechny aplikace, které organizace používá včetně manuálně řízených systémů

Pokud vaše organizace čelí podobným výzvám, je zavedení tohoto systému cestou ke zvýšení efektivity, bezpečnosti a přehlednosti správy identit.

Přečtěte si více o našich implementacích.

Kontaktujte nás a zjistěte, jak vám můžeme pomoci.

## O Orchitechu

Orchitech nabízí řešení v oblasti správy identit a řízení přístupů, která pomáhají odborům IT:

- efektivně spravovat a zabezpečovat identity zaměstnanců i externích pracovníků
- automatizovat rutinní činnosti
- šetřit čas a náklady
- díky okamžitému přehledu eliminovat stres z auditu

Řešení od Orchitechu zajišťují soulad s legislativními požadavky, včetně GDPR, NIS2, nového kybernetického zákona a dalších. Orchitech působí na trhu více než 15 let a realizoval více než 100 projektů pro přibližně 50 klientů z veřejného i soukromého sektoru.

https://orchi.tech/ +420 216 216 850 info@orchitech.cz

orchitech

# WEDOS na ISSS: Globální ochrana před kyberútoky

Společnost WEDOS patří mezi tradiční účastníky konference ISSS v Hradci Králové a i letos zde představí své nejnovější aktivity v oblasti kybernetické bezpečnosti. Nově zde vystupujeme jménem společnosti **WEDOS Sàrl** – evropské technologické firmy se sídlem v Lucembursku, která se zaměřuje výhradně na vývoj a provoz bezpečnostních řešení pro globální trh.

WEDOS Sàrl vznikla jako samostatná entita oddělením od WEDOS Internet, a.s. – jednoho z největších poskytovatelů hostingových služeb ve střední Evropě. Tento krok byl strategickým rozhodnutím, které reflektuje naši rostoucí specializaci a cíl: **expanzi v oblasti kybernetické bezpečnosti na mezinárodní úroveň**.

Naše úsilí bylo začátkem tohoto roku oceněno v soutěži **CACIO IT Projekt roku**, kde jsme získali cenu za projekt **WEDOS Global Protection** – Inovativní řešení s celosvětovým dosahem, zaměřené na ochranu proti DDoS útokům. Do soutěže nás nominovala společnost **Hewlett Packard Enterprise (HPE)**, náš dlouholetý technologický partner a dodavatel serverové infrastruktury.

## Kyberútoky jako každodenní realita

Kybernetické útoky dnes ohrožují prakticky každou organizaci bez ohledu na velikost nebo obor. Zvláště nebezpečné jsou tzv. **DDoS útoky**, které zahlcují servery masivními vlnami falešných požadavků. Výsledkem může být zpomalení služeb nebo jejich úplné odstavení. I běžně dostupné nástroje mohou útočníkům umožnit způsobit značné škody během několika vteřin.

## Na jaké bázi funguje WEDOS Global Protection?

WEDOS Global Protection je postavený na kombinaci **globální DNS Anycast sítě** a **inteligentní bezpečnostní platformy WEDOS Protection**:

- **DNS Anycast** rozděluje provoz mezi více než 123 uzlů po celém světě. Zajišťuje rychlejší odezvu, rozkládá zátěž a zvyšuje odolnost vůči útokům.
- **WEDOS Protection** analyzuje a filtruje provoz v reálném čase, detekuje anomálie a blokuje škodlivé požadavky.

Celá infrastruktura je provozována výhradně naším týmem – bez využití třetích stran – což zajišťuje plnou kontrolu nad výkonem i bezpečností.

## Výsledky z praxe

Naše technologie se osvědčila např. během útoku v roce 2023, kdy objem škodlivého provozu přesáhl 500 Gbps. Služby všech chráněných klientů zůstaly dostupné, zatímco jiné systémy by čelily výrazným výpadkům. Mezi naše zákazníky dnes patří **nejen firmy**, ale i **univerzity**, **nemocnice**, **úřady** a **vládní instituce** po celém světě.

## Ochrana pro každého

Cílem WEDOS je poskytovat špičkovou kybernetickou ochranu všem organizacím – bez ohledu na jejich velikost či oblast působení. Díky férovým cenám, otevřenému přístupu a nonstop podpoře zpřístupňujeme robustní obranu všem, kteří ji potřebují.

Pokud vás naše řešení zaujalo, ozvěte se – rádi vám poradíme nebo připravíme vhodné zabezpečení na míru.

Kontakt: Markéta Průšová – marketa.prusova@wedos.com
Více na: **wedos.zone** | **wedos.protection** | **wedos.eu**

**Sborník 27. ročníku konference**
**ISSS**
**12.–13.5.**25
**Hradec**Králové
Editor: Kateřina Pánková
Vydavatel: TRIADA, spol. s r. o.
Rok vydání: 2025
ISBN: 978-80-907164-7-6