Směrnice pro dlouhodobou ochranu multimediálních dat

Klodner, Michal; Antoš, David; Berka, Roman; Získal, Bohuš
2021

Návrh směrnice pro příslušný odbor Ministerstva kultury vytvořený v rámci projektu „Laterna magika. Historie a současnost, dokumentace, uchování a zpřístupnění“ DG16P02H005

Směrnice pro dlouhodobou ochranu multimediálních dat

1. Úvodní ustanovení 3

2. Použitá terminologie 3

3. Referenční standardy a zmiňované koncepty 4

4. Cíle, potřeby dlouhodobé ochrany multimediálních dat v daném kontextu 5

5. Rámec, zaměření a rozsah aplikovatelnosti směrnice 5

6. Definice rolí 6

7. Identifikace procesů členěná podle typů činností a rolí spolupracujících depozitářů 7
- 7.1. Parametry procesů 7
- 7.2. Příprava Archivního informačního balíčku na straně primárního repozitáře 7
- 7.3. Přenos Archivního informačního balíčku 8
- 7.4. Dlouhodobé uchovávání Archivního informačního balíčku 10
- 7.5. Zpřístupnění Informačního obsahu 12

8. Ověření a aplikace směrnice 13

Použité zdroje 14

Autoři:
Bohuš Získal
David Antoš
Michal Klodner
Roman Berka

1. Úvodní ustanovení

Směrnice popisuje procesy a zodpovědnosti při přípravě multimediálních dat pro dlouhodobé uchovávání, při jejich bezpečném a efektivním přenosu do institucí provozujících systémy pro jejich dlouhodobé uchovávání, a jejich případné zpřístupnění na straně těchto institucí, vše způsobem zajišťujícím nezbytnou koordinaci a vedoucím k minimalizaci možných rizik. Směrnice je vytvořena na základě ověřených postupů a odpovídajících platných standardů, s cílem nastavit výše uvedené procesy tak, aby byly aplikovatelné v podmínkách českých paměťových institucí a dalších relevantních subjektů a umožňovaly bezpečné sdílení a dlouhodobé uchovávání dat v rámci domácí i zahraniční spolupráce. Směrnice z důvodu širší aplikovatelnosti nezmiňuje konkrétní technologie ani vhodné nástroje pro realizaci jednotlivých operací, popisuje však způsoby, jak technologie a nástroje vybírat a provozovat s ohledem na charakter popisovaných procesů.

2. Použitá terminologie

Použitá terminologie je převzata nebo vychází z českých překladů odpovídajících norem (např. ČSN ISO 14721:2014) a navazujících metodik, a dále z Terminologické databáze knihovnictví a informační vědy (TDKIV). Anglické ekvivalenty jsou případně uvedeny v závorkách.

*Archivní informační balíček, AIP (Archival Information Packag*e) – soubor dat určený pro dlouhodobou archivaci

Bitová ochrana dat – zajištění neporušenosti dat až na úroveň jednotlivých bitů, odpovídá logické ochraně dat

Informace o neporušenosti (Fixity Information) – informace, která dokumentuje mechanismus zajišťující, ze objekt s informačním obsahem nebyl změněn, např. metoda kontrolního součet pro soubor

Informace o přístupových právech (Access Rights Information) – informace, zda a jakým skupinám uživatelů je Informační obsah přístupný, tato informace je uložena v PDI

Informace o uchovávání, PDI (Preservation Description Information) – informace nezbytná pro adekvátní uchovávání informačního obsahu

Informační obsah (Content Information) – samotný obsah, který nese primární informace určené k dlouhodobému uchovávání, je součást balíčku AIP (např. archivované video)

Kontrolní součet (Fixity) – doplňková informace vytvořená z primárního datového objektu, která slouží k ověření, že datový objekt nebyl porušen (např. při přenosu)

Logická ochrana dat – činnosti vedoucí k ochraně informačního obsahu včetně umožnění jeho zpřístupnění a prezentace

Popis balíčku (Package Description) – informace o struktuře a obsahu AIP, která umožňuje, aby se komponenty AIP daly vyhledat v daném archivním systému

Pravidla pro uchovávání – soubor pravidel zachycující závazky a záměry instituce v oblastech vztahujících se k uchovávání obsahu (např. bezpečnosti).

Primární repozitář – instituce zodpovídající za celý proces uchovávání dat, s výjimkou činností zajišťovaných smluvním partnerem – sekundárním repozitářem

Sekundární repozitář – instituce zajišťující specificky určenou část procesů uchovávání dat, za něž přebírá plnou zodpovědnost ve smyslu požadavků normy ČSN ISO 16363

Výstupní informační balíček, DIP (Dissemination Information Package) – Informační balíček odvozený z jednoho nebo více AIP, který archiv posílá koncovému uživateli na základě jeho žádosti

Základní popisné informace (Descriptive Information) – základní soubor popisných informací, který se váže k informačnímu obsahu (např. jeho stručná charakteristika) a který dovoluje daný informační obsah v úložišti nalézt (např. nalézt konkrétní videozáznam)

3. Referenční standardy a zmiňované koncepty

ČSN ISO 14721 - Otevřený archivační informační systém - Referenční model

ČSN ISO 16363 - Audit a certifikace důvěryhodných digitálních úložišť

ČSN EN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací

Metodika logické ochrany digitálních dat

The Open Archives Initiative Protocol for Metadata Harvesting OAIS-IO

4. Cíle, potřeby dlouhodobé ochrany multimediálních dat v daném kontextu

Cílem dlouhodobé ochrany multimediálních dat je v co největší míře uchovat jejich původní informační obsah a zároveň umožnit jeho zpřístupnění. Dlouhodobá ochrana dat je komplexní proces, který zahrnuje jak technologické komponenty (nástroje na zpracování, správu, zpřístupnění, uchovávání multimediálního obsahu a odpovídající infrastrukturu), tak soubor činností vyžadující plánovaný, systematický a organizovaný přístup. Samotné technologie, bez ohledu na jejich rostoucí výkon a dostupnost, nemohou dlouhodobou ochranu informačního obsahu zajistit, proces jeho aktivní ochrany je (zatím) nevyhnutelný. Vzhledem k obecné formě, jakou jsou formulovány relevantní standardy v dané oblasti, vzniká potřeba popisu konkrétních postupů aplikovatelných v dané situaci, které lze použít bez hlubokých znalostí celé problematiky. Tato směrnice vznikla na základě požadavku definovat konkrétní doporučení pro paměťové instituce uchovávající audiovizuální obsah, které nemohou, nebo nechtějí (na základě strategického rozhodnutí), zajistit všechny činnosti spojené s dlouhodobou ochranou dat, a potřebují určité dílčí procesy, jmenovitě spojené s dlouhodobým uložením a zpřístupněním, realizovat ve spolupráci s dalším subjektem. Zároveň tato směrnice slouží pro instituce, které dokáží zajistit bitovou ochranu dat v dlouhodobém horizontu i jako službu pro partnery a v tomto případě nezajišťují samotnou správu informačních objektů.

5. Rámec, zaměření a rozsah aplikovatelnosti směrnice

Cílem směrnice je popsat vhodné postupy v souladu s mezinárodními standardy, ověřenou praxí, platným legislativním rámcem a s ohledem na aplikaci těchto postupů při spolupráci více institucí. Směrnice vychází z otevřeného referenčního archivační modelu podle normy ČSN ISO 14721 a požadavků na provozování důvěryhodného úložiště, vyplývajících z normy ČSN ISO 16363. Směrnice se zaměřuje na situaci, kdy je správa dat zajišťována spoluprací více institucí nebo jejich samostatných celků a dochází k rozdělení odpovědností za správu dat. Tento model distribuované ochrany a jeho kompatibilita s referenčním modelem OAIS je v literatuře popsán jako vnější OAIS-vnitřní OAIS model (OO-IO, Outer OAIS–Inner OAIS Model), a byl v praxi ověřen například v Dánsku (Zierau, 2017). Teoreticky je možné rozdělit zodpovědnosti mezi instituce v podstatě libovolně, pokud bude mezi spolupracujícími subjekty (institucemi) existovat oboustranně závazná dohoda o spolupráci definující odpovědnosti za všechny procesy nezbytné pro dlouhodobou ochranu dat. V této souvislosti jsou používány termíny Primární a Sekundární repozitář pro rozdělení a vymezení rolí spolupracujících institucí, které níže popsané soubory činností zajišťují.

Následující směrnice je určena pro situaci, kdy Primární repozitář zajišťuje všechny úkony kromě dlouhodobého uložení obsahu, u nějž přebírá zodpovědnost za všechny potřebné úkony (procesy) Sekundární repozitář. Zároveň směrnice pokrývá situaci, kdy sekundární repozitář může, současně s Primárním repozitářem a v omezeném rozsahu, zajišťovat zpřístupnění. Směrnice nevytváří nové postupy a zodpovědnosti nad rámec v úvodu uvedených norem, pro konkrétní postupy ochrany logických dat odkazuje na Metodiku logické ochrany digitálních dat (Hutař, 2018). Níže uvedená doporučení se týkají výhradně rozdělení postupů a zodpovědností mezi partnerské instituce. Tomuto konceptu odpovídá i vymezení rolí a zodpovědností za jednotlivé procesy, které je v této směrnici stanoveno pouze rámcově a musí být předmětem dohody mezi spolupracujícími institucemi (Primárním a Sekundárním repozitářem). Zásadním předmětem této dohody je rozdělení kompetencí pro vytváření, zavedení, aktualizaci a dodržování Pravidel pro uchovávání, kde každý repozitář musí mít jasně vymezené závazky. Celkovou zodpovědnost za konzistenci a kompletnost těchto pravidel nese Primární repozitář a udržuje je v souladu se svým strategickým plánem uchovávání. Oba repozitáře dále musí mít zavedeny odpovídající postupy v oblasti správy informačních systémů, například musí vést dokumentaci všech změn konfigurací a provozu konkrétního HW a SW. Je s výhodou, pokud mají repozitáře zavedeny relevantní postupy v souladu s požadavky normy ČSN EN ISO/IEC 27001.

Jak již bylo zmíněno v úvodním ustanovení, ve směrnici nejsou zmiňovány konkrétní příklady zařízení nebo nástrojů, jejich vychází z konkrétního případu a situace spolupracujících institucí a vyžaduje vyhodnocení řady parametrů (definovaných níže).

Směrnice nepokrývá veškeré procesy dlouhodobé ochrany dat, byla vytvořena jako doplněk dalších směrnic a metodik určených zejména pro paměťové instituce (např. směrnice pro procesy zpracování a katalogizace multimediálních dat).

6. Definice rolí

- *Správce uchovávání (na straně Primárního repozitáře)* – odpovídá za zajištění zpracování a správu Informačního obsahu na straně Primárního repozitáře a návaznosti na definované procesy na straně Sekundárního repozitáře

- *Správce přenosů* – odpovídá za zajištění přenosů Informačního obsahu mezi Primárním a Sekundárním repozitářem

- *Správce dlouhodobého úložiště (na straně Sekundárního repozitáře)* – odpovídá za zajištění zpracování a (zejména logické) ochrany Informačního obsahu určeného k dlouhodobému uložení, případně za zajištění přístupu k Informačnímu obsahu ve sjednaném rozsahu

- *Správce zpřístupnění* – zajišťuje zpřístupnění Informačního obsahu na straně Primárního repozitáře

7. Identifikace procesů členěná podle typů činností a rolí spolupracujících depozitářů

7.1. Parametry procesů

V následujících kapitolách jsou popsány jednotlivé procesy z hlediska jejich cílů a návazností v rámci komplexní problematiky dlouhodobé ochrany a zpřístupnění dat, zejména s ohledem na vhodný model spolupráce dvou subjektů – repozitářů a odpovídající vymezení odpovědností.

Pro správu procesů je třeba vyhodnotit a průběžně aktualizovat následující parametry:

- Velikost přenášených a ukládaných dat pro jednorázové a pravidelné operace
- Strukturu dat (velikosti a počty souborů)
- Požadavky na rychlost přenosu a zpracování
- Dostupné zdroje (lidské, finanční, technologické)
- Rizika pro dané uspořádání s ohledem na situaci a vztahy mezi poskytovateli/příjemci Informačního obsahu

7.2. Příprava Archivního informačního balíčku na straně primárního repozitáře

Primární repozitář zajišťuje veškeré operace potřebné pro vytvoření Archivního informačního balíčku (AIP) v souladu s požadavky normy ČSN ISO 14721, kdy jednotlivé procesy přípravy a zpracování Informačního obsahu nejsou předmětem této směrnice. Primární repozitář dále ručí za skutečnost, že AIP neobsahuje žádné potenciálně škodlivé struktury (např. spustitelný kód nesouvisející s daným informačním obsahem), data pochází ze známých zdrojů a/nebo byla pořízena a zpracována v rámci kontrolovaných procesů (např. v souladu s požadavky normy ČSN EN ISO/IEC 27001). Primární repozitář dále zajišťuje, aby s každým AIP byly propojeny základní popisné informace umožňující identifikaci jeho informačního obsahu, a tato vazba byla udržována bez ohledu na jeho umístění. Přenos a vkládání dat do systému Sekundárního repozitáře mohou být plně automatizovány, např. v případě, že dlouhodobé úložiště provozované sekundárním repozitářem umožňuje strojový přístup prostřednictvím API. Součástí dohody mezi Primárním a Sekundárním repozitářem musí být zodpovědnost za vytváření a uchovávání informace pro kontrolu neporušenosti dat.

Činnosti prováděné v rámci procesu přípravy dat (v návaznosti na sekundární repozitář) zahrnují:

- Plánování a vyhodnocování objemu a struktury dat určených k dlouhodobé archivaci

- Informování správce dlouhodobého úložiště o požadavcích na přenos a ukládání AIP (např. objemy dat)
- Vytvoření (případně převzetí a kontrola) validního Archivního Informačního balíčku (AIP) a navázaných Základních popisných informací
- Výpočet informace pro kontrolu integrity ve formátu dohodnutém se sekundárním repozitářem a jejich vložení do AIP (může být po dohodě zajišťováno i Sekundárním repozitářem)
- Zajištění jedinečné, jednoznačné a trvalé identifikace AIP
- V případě potřeby aktualizace (AIP) a/nebo navázaných Základních popisných informací
- Udržování vazby mezi (identifikátorem) AIP a Základními popisnými informacemi
- Udržování informací o trvalém uložení AIP v Sekundárním repozitáři, pokud k němu došlo
- Správa strojového přístupu k technologiím sekundárního repozitáře (je-li strojový přístup zaveden)

Předpoklady:
- Primární depozitář má vytvořena a aplikuje Pravidla pro uchovávání, má zavedeny všechny procesy potřebné pro vytváření AIP v souladu s těmito pravidly
- Jsou nastaveny vhodné komunikační kanály mezi repozitáři, určeny osoby zodpovědné za komunikaci a správu těchto kanálů
- Je dohodnut způsob řešení mimořádných požadavků, například jednorázové uložení velkého objemu dat

7.3. Přenos Archivního informačního balíčku

Způsob přenosu Informačního obsahu mezi Primárním a Sekundárním repozitářem je definován na základě vzájemné dohody obou institucí, zahrnující určení Správce přenosu, požadovaných parametrů přenosu a způsobu aktualizaci, odpovědností za jednotlivé procesy a definování komunikačních kanálů. Výběr vhodné technologie a způsobu přenosu vychází z vyhodnocení v úvodu zmíněných parametrů (velikost a struktura dat, požadavky na rychlost, rizika…) a je limitován dostupnými prostředky. Obecně nejsou preferována přenosná zařízení s výjimkou případu, kdy je třeba jednorázově přenést velký objem dat (např. desítky TB) a není možné zajistit síťové propojení obou lokalit s dostatečnou rychlostí přenosu dat. Míra zabezpečení přenosu je vždy kompromisem mezi technickou náročností a odpovídajícími riziky, za zajištění odpovídajícího zabezpečení je zodpovědný Správce přenosu. Prioritou pro přenos je zajištění binární shody odesílaných a přijímaných dat, tuto shodu je třeba následně ověřit například vhodnou metodou kontrolních součtů. Pro kontrolu binární shody po přenosu může být použita i informace o neporušenosti uložená v AIP. Přenos samotných AIP může být doplněn o přenos asociovaných Základních popisných informací, v tomto případě je nutné dohodnout formát a způsob jejich přenosu (obvykle v závislosti na systémech správy dat používaných oběma partnery). Proces přenosu může být zcela automatizován, vždy ale musí existovat záznam o provedení kontroly binární shody odesílaných a přijímaných dat. Za správu

technologií a monitoring přenosu je zodpovědný Správce přenosu určený v dohodě mezi Primárním a Sekundárním repozitářem.

Proces výběru a správy přenosových technologií zahrnuje následující činnosti:

- Plánování pořizování a obnovy technologií a aktualizace postupů v souladu se strategií společnosti, která přenosy zajišťuje
- Pravidelné vyhodnocování požadovaných parametrů přenosu
- Pravidelné vyhodnocování vlastností dostupných/používaných technologií
- Pravidelné vyhodnocování existujících metod a postupů (např. šifrování, kontrolní součty) s ohledem na požadavek zajištění neporušenosti přenášených dat, požadované parametry přenosu a dostupné zdroje
- Pravidelné vyhodnocování rizik spojených s použitím konkrétních technologií a postupů
- Výběr vhodné technologie a postupů s ohledem na vyhodnocené parametry a dostupné prostředky
- Pravidelné vyhodnocování dosahovaných parametrů přenosů a stavu používaných technologií
- Aktualizace technologií a/nebo metod na základě plánu, systémových požadavků (např. aktualizace systémových komponent) nebo změny požadovaných parametrů
- Dokumentace všech změn provedených na přenosových technologiích
- Informování o haváriích, výlukách a změnách, pokud mají dopad na proces přenosu dat

Proces přenosu dat zahrnuje následující činnosti/operace

- Vytvoření, aktualizace a dodržování postupů přenosu dat s ohledem na vlastnosti vybrané přenosové technologie
- Oznámení ukončení přenosu a případně předání doprovodných informací v dohodnutém formátu (lze oznamovat a předávat automaticky).
- Ověření kontrolní součtů na straně příjemce, potvrzení úspěšného přenosu.
- Opakování přenosu v případě porušení integrity dat
- Informování o případných neúspěšných přenosech nebo přenosech nedosahujících požadovaných parametrů

Předpoklady:

- Jsou vytvořeny vhodné komunikační kanály a/nebo systémové nástroje pro zahájení/ukončení přenosů a pro informování o technických omezeních a poruchách
- Je dohodnut rámec přenášených datových objemů a doby zpracování přenášených dat
- Jsou dohodnuty parametry přenosu (např. rychlost) a provádí se jejich aktualizace na základě potřeb obou institucí
- Existuje dohoda o konkrétních zodpovědnostech při správě přenosových technologií včetně zajištění prostředků na správu a obnovu technologií a/nebo pronájem služeb

7.4. Dlouhodobé uchovávání Archivního informačního balíčku

Činnosti zajišťující dlouhodobou ochranu Informačního obsahu zahrnují ochranu dat na logické a bitové úrovni. Tato směrnice předpokládá model, kdy plná zodpovědnost za dlouhodobou ochranu dat na bitové úrovni leží na Sekundárním repozitáři, za předpokladu, že Primární repozitář zajišťuje ochranu Informačního obsahu během všech procesů až do vytvoření Archivního informačního balíčku – AIP. Sekundární repozitář přebírá datový obsah v podobě AIP, v případě, že s AIP pracuje jako s obecným datovým objektem bez jakéhokoliv zásahu do jeho obsahu, lze chápat označení AIP jen jako určení původu. V oblasti logické ochrany je třeba určit rozdělení odpovědností při transformaci dat, například při potřebě převodu do jiného formátu či aktualizaci metadat. Dále je třeba dohodnout konkrétní způsob identifikace archivovaného obsahu (AIP) např. pomocí přiděleného unikátního identifikátoru, aby Primární repozitář mohl požádat Sekundární repozitář o vydání či aktualizaci konkrétního obsahu. Zde je rovněž potřebná shoda, zda, a případně v jaké míře Sekundární repozitář spravuje i Základní popis balíčku a umožňuje vyhledání AIP na základě jeho obsahu (viz sekce zpřístupnění Informačního obsahu). Správce dlouhodobého úložiště je zodpovědný za vytvoření a aktualizaci konkrétních postupů správy a bitové ochrany dat v souladu s Pravidly pro uchovávání, definujících zejména množství a způsob vytváření kopií uložených dat, způsob a frekvence ověřování integrity dat, proces identifikace rizik spojených s použitými technologiemi a s tím spojené plánování obnovy technologií a přesuny dat, způsob přesunu dat, způsob zpřístupnění a aktualizace AIP, havarijní plány a způsoby obnovy dat. V případě, že je požadováno, aby Sekundární repozitář na vyžádání předal data v jiné podobě než jako AIP, a/nebo jinému subjektu než Primárnímu repozitáři, je toto předání řešeno jako zpřístupnění (viz sekce zpřístupnění Informačního obsahu).

Proces výběru, správy a obnovy archivačníech technologií zahrnuje:

- Plánování pořizování a obnovy technologií a postupů v souladu s Pravidly pro uchovávání a strategií společnosti
- Výběr vhodné technologie a postupů spojených s procesem správy dat s ohledem na vyhodnocené parametry a dostupné prostředky
- Dokumentaci všech postupů ukládání a bitové ochrany dat
- Pravidelné vyhodnocování předpokládaných objemů a struktury ukládaných dat
- Pravidelné vyhodnocování rychlosti ukládání a přístupu k uloženým datům
- Pravidelné vyhodnocování parametrů dostupných technologií
- Pravidelné vyhodnocování existujících metod a postupů (např. kontrola neporušenosti dat) s ohledem na požadované objemy dat a dostupné technologie
- Pravidelné vyhodnocování rizik spojených s použitím konkrétních technologií a postupů, vytváření plánů na zmírňování těchto rizik a plánů řešení havarijních situací
- Pravidelné vyhodnocování dosahovaných parametrů zpracování, ukládání a zpřístupnění dat a stavu používaných technologií i s ohledem na jejich možné nahrazení

- Identifikace a vyhodnocení všech chyb a odchylek od předpokládaného provozu systému
- Identifikace a hodnocení rizik/přínosů dostupných aktualizací používaného software, výběr vhodných aktualizací
- Aktualizace technologií a/nebo metod na základě plánu, systémových požadavků (např. aktualizace komponent), zjištěných chyb nebo změny požadovaných parametrů s minimalizací dopadů na proces správy dat
- Informování o haváriích, výlukách a změnách, pokud mají přímý dopad na proces správy dat

Proces správy dat (bitové ochrany) zahrnuje následující činnosti:
- Vytvoření, pravidelná aktualizace a dodržování postupů pro ukládání, zpřístupňování, přenos a obnovu dat s ohledem na parametry, architekturu a lokalizaci vybraných technologií a plán jejich obnovy
- Vytvoření a aktualizace postupů spojených s manipulací s daty při přechodu na nové technologie a postupy s minimalizací rizik
- Přijetí AIP z přenosu nebo strojového přístupu (přes API) do systému Sekundárního repozitáře a předání (Primárnímu repozitáři) informace o identifikaci AIP v systému, pokud byla rozšířena o další atributy
- Vytvoření informace o neporušenosti (pokud nezajišťuje Primární repozitář) a její uložení do přijatého AIP, uložení informace do systému
- Vytvoření operativní (vnější) informace o neporušenosti pro každý archivovaný datový objekt, uložení informace do systému
- Pokud je pro identifikaci AIP v archivním úložišti a jeho eventuální provázání se základními popisnými informacemi (v závislosti na rozsahu přístupových služeb poskytovaných archivem) nutné tuto identifikaci rozšířit, nová identifikace je spravována a předávána primárnímu repozitáři
- Vytváření identických kopií AIP na více úložištích v souladu se schválenými postupy pro uchovávání
- Nahrazení všech kopií AIP aktualizovanou verzí dodanou primárním repozitářem (včetně aktualizace vnější informace o neporušenosti)
- Pravidelná kontrola (vnější) informace o neporušenosti v souladu se schválenými postupy pro uchovávání
- Proces obnovy dat a jejich uložení v souladu s pravidly pro uchovávání v případě havárie
- Monitorování všech kroků správy dat, záznam a vyhodnocení případných chyb

Předpoklady:
- Sekundární repozitář má vhodně nastavené rozhodovací a řídící procesy potřebné pro pořizování, zavádění, provozování nebo externí zajištění výše uvedených postupů
- Sekundární repozitář má strategii pro zajištění dostatečných zdrojů (lidských, finančních) nezbytných pro zajištění činností a technologií spojených s procesy dlouhodobého ukládání dat

- Sekundární repozitář má definované postupy pro fyzické zabezpečení úložišť – zamezení přístupu neoprávněným osobám, dále postupy zabezpečení přístupu k datům a SW komponentám systému
- Mezi sekundárním a primárním repozitářem je dohodnut rámec objemů a doby zpracování ukládaných dat a způsob jejich zpětného zpřístupnění

7.5. Zpřístupnění Informačního obsahu

Zpřístupněním Informačního obsahu není míněn přímý přístup uživatelů do dlouhodobého úložiště, z důvodu bezpečnosti je zpřístupnění Informačního obsahu vždy zprostředkované. Zpřístupnění Informačního obsahu nad rámec poskytování AIP primárnímu repozitáři musí být specificky definováno ve smlouvě mezi Primárním a Sekundárním repozitářem, kde musí být sjednány i právní podmínky případného poskytování obsahu Sekundárním repozitářem. Pro poskytování obsahu externím subjektům ve formě hodnověrných objektů je zapotřebí, aby Sekundární repozitář poskytoval obsah ve formě Výstupních informačních balíčků (DIP). Variantou je zpřístupnění základních popisných informací spolu s vybranými částmi DIP a informačním obsahem AIP v náhledové kvalitě. Obě varianty musí být realizovány v souladu s Pravidly pro zpřístupňování poskytovanými a kontrolovanými Správcem zpřístupnění primárního repozitáře. Z důvodu zajištění důvěryhodnosti obsahu poskytovaného v DIP balíčcích je doporučeno, aby sekundární repozitář při vytváření DIP neprováděl manipulace s informačním obsahem AIP ve smyslu zásahu do uložených informací (např. převod do jiného formátu, zkracování). Proces zpřístupnění může znamenat rozšíření Procesu výběru, správy a obnovy archivačních technologií ve smyslu jeho aplikace na technologie pro další zpracování dat, např. pro vytváření náhledových kopií informačního obsahu. Sekundární repozitář pro zpřístupnění může, po dohodě s primárním repozitářem, zveřejnit základní popisné informace a zajistit jejich fyzické provázání na konkrétní AIP, nebo může žádost o zpřístupnění přijmout prostřednictvím primárního repozitáře, který dodá identifikaci požadovaných AIP.

Proces zpřístupnění zahrnuje následující činnosti:

- Přebírání a dodržování pravidel pro zpřístupňování dat od Primárního repozitáře v rámci omezení sjednaných s Primárním repozitářem, pravidla zahrnují i možný obsah a podobu DIP
- Zavedení, zveřejnění a správa postupu, jakým uživatel (externí subjekt) komunikuje o zpřístupnění obsahu
- Vytvoření a správa odpovídajících komunikačních kanálů (např. webová stránka s formuláři)
- Přijímání žádosti o zpřístupnění konkrétního Informačního obsahu
- Identifikace jednotlivých AIP na základě konkrétní žádosti o přístup, vyhodnocení (v DIP) uložené Informace o přístupových právech.
- Vyhodnocení žádostí o přístup k Informačnímu obsahu v souladu s Pravidly pro zpřístupňování a omezeními danými pro konkrétní informační obsah

- Informování uživatelů o případném zamítnutí žádosti
- Získání AIP s požadovaným informačním obsahem z archivního systému, kontrola vnější a vnitřní (v AIP) uložené informace o neporušenosti
- Vytvoření DIP ze zdrojových AIP v souladu s požadavky a omezeními danými pro konkrétní Informační obsah
- Uložení informací s popisem konkrétního případu zpřístupnění spolu s aplikovaným procesem vytvoření DIP včetně identifikace zdrojových AIP
- V případě zveřejnění základních popisných informací Sekundárním repozitářem zajištění jejich pravidelné aktualizace ve spolupráci s Primárním repozitářem
- Příjem hlášení o chybách ve zpřístupněných datech, spolu se Správcem zpřístupnění identifikace a (pokud je to možné) odstranění problému, ve všech případech informování uživatele
- Monitorování všech kroků zpřístupnění, záznam a vyhodnocení případných chyb
- Pravidelná kontrola, zda jsou relevantní kroky procesu zpřístupnění realizovány v souladu s Pravidly pro zpřístupňování, reporty výsledků kontrol Správci zpřístupnění

Předpoklady:

- Sekundární repozitář má strategii pro zajištění dostatečných zdrojů (lidských, finančních) nezbytných pro zajištění činností a technologií spojených se zpřístupněním uložených datových objektů
- Sekundární repozitář má definované postupy zabezpečení úložišť – zamezení přístupu k datům neoprávněným osobám
- Je dohodnut rozsah, objem zpřístupňovaných dat, jsou akceptována Pravidla pro zpřístupňování dat v definované šíři

8. Ověření a aplikace směrnice

Postupy uvedené ve směrnici byly ověřeny v rámci realizace projektu „Laterna magika. Historie a současnost, dokumentace, uchování a zpřístupnění" DG16P02H005 financovaného z Programu na podporu aplikovaného výzkumu a experimentálního vývoje národní a kulturní identity na léta 2016 až 2022 (NAKI II). Instituce, které v rámci projektu tyto postupy ověřovaly, mají v daných oblastech zavedeny vlastní směrnice, které danou problematiku pokrývají a výše popsané principy byly uplatněny v daných procesech v souladu se zaměřením a rolemi jednotlivých institucí. Tuto směrnici lze uplatnit jako kompletní soubor postupů, které by měly být institucemi dodržovány. Jejich začlenění do konkrétního souboru vnitřních předpisů závisí na jeho formě a uspořádání, a tedy nepředpokládá, že je tato směrnice přejata v nezměněné podobě.

Použité zdroje

- HUTAŘ, J., PAVLÁSKOVÁ, E., HRUŠKA, Z., MIRANDA, A. a VAŠEK, Z., 2018. *Metodika logické ochrany digitálních dat*. Praha: Knihovna AV ČR.

- ZIERAU, E., 2017. *OAIS and Distributed Digital Preservation in Practice. An exploration of Danish and other use cases that contributed to the development of the Outer OAIS–Inner OAIS Model for Distributed Digital Preservation*. iPRESS 14th International Conference on Digital Preservation, Kyoto, Japan. Dostupné online http://doi.org/10.5281/zenodo.130884.