Operačný program
Efektívna
verejná správa

Európska únia
Európsky sociálny fond

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Výstup č. 1.1.8:

Štandardizácia dôveryhodných údajov

Realizačná zmluva o poskytnutí služieb a o dielo č. 445/2022

Projekt:

Zlepšenie využívania údajov vo verejnej správe

ITMS kód projektu:

314011S979

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Document review and approval

Revision history

Version	Author	Date	Revision
1.0	Ceľuchová Bošanská Bárdy Vančo	2.4.2023	
1.1	Ceľuchová Bošanská Bárdy Vančo	27.4.2023	Zapracovanie pripomienok

This document has been reviewed by

	Reviewer	Date reviewed
1		
2		
3		
4		
5		

This document has been approved by

	Subject matter experts Name	Signature	Date reviewed
1			
2			
3			
4			
5			

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Tento projekt je podporený z Európskeho sociálneho fondu.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

ZOZNAM SKRATIEK	
Skratka	**Význam**
AdES	Zdokonalený elektronické podpisy (Advanced Electronic Signature)
CA	Certifikačná autorita (Certification Authority)
CDEI	Centrum pre dátovú etiku a inováciu (Centre for Data Ethics and Innovation)
CIP	Centrálna integračná platforma
CMÚ	Centrálny model údajov
CRL	Zoznam zrušených certifikátov (Certificate Revocation List)
DCMS	Misterstvo pre digitálnu transformáciu, kultúru, médiá a šport (Department for Digital, Culture, Media and Sport of the United Kingdom)
DSS	Služba digitálneho podpisu (Digital Signature Service)
EDPB	Európsky výbor pre ochranu osobných údajov (European Data Protection Board)
eID	Elektronická identita
eIDAS	Nariadenie Európskej únie č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom európskom trhu.
GDPR	Všeobecné nariadenie o ochrane osobných údajov (General Data Protection Regulation)
HSM	Hardware Security Module
ICO	Úrad komisára pre informácie (Information Commissioner's Office)
IS CSRÚ	Informačný systém centrálnej správy referenčných údajov
IS VS	Informačný systém verejnej správy
JSON	JavaScript Object Notation
JSON-LD	JSON pre linkované údaje (JSON for Linking Data)
JWE	JSON Web Encryption
JWS	JSON Web Signature
JWT	JSON Web Token
mID	Mobilná identita
MIRRI SR	Ministerstvo investícii, regionálneho rozvoja a informatizácie

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

MOU	Manažment osobných údajov
MV SR	Ministerstvo vnútra SR
OCSP	Online Certificate Status Protocol
OVM	Orgán verejnej moci
PET	Technológie na zvýšenie súkromia (Privacy-enhancing Technologies)
PIMS	systémy na správu osobných informácií (Personal Information Management System)
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
RA	Registračná autorita
RDF	Resource Description Framework
SES	Jednoduchý elektronický podpisy (Simple Electronic Signature)
SvM	Slovensko v mobile
QES	Kvalifikovaný elektronický podpis (Qualified Electronic Signature)
TRUSTS	Trusted Secure Data Sharing Space
URI	Jednotný referencovateľný identifikátor
VC	Overiteľné poverenia (Verifiable Credentials)
W3C	World Wide Web Consortium
XML	Extensible Markup Language
ZKP	Zero-Knowledge Proofs

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Obsah

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

1 Úvod a zhrnutie

1.1 Kontext

Detailný výstup č. 1.1.8: Štandardizácia dôveryhodných údajov vznikol ako aktualizácia dostupných výstupov v téme zabezpečenia dôveryhodného zdieľania údajov.

Dokument bol pripravený v rámci projektu „Zlepšenie využívania údajov vo verejnej správe“. Tento projekt má ambíciu transformovať fungovanie inštitúcií verejnej správy tak, aby dokázali maximálne efektívne spravovať a zdieľať údaje, využívať údaje pre lepšie rozhodovanie na základe faktov a dôkazov, pre zlepšenie efektivity a adresnosti služieb na základe lepšieho využívania dát.

Projekt Zlepšenie využívania údajov vo verejnej správe realizuje Dátová kancelária verejnej správy ako špeciálna jednotka Ministerstva investícii, regionálneho rozvoja a informatizácie (ďalej aj MIRRI SR).

Výstupom dokumentu je návrh štandardov a metód pre zabezpečenie dôveryhodného zdieľania údajov, ktoré spravujú inštitúcie verejnej správy. Základnými nástrojmi dôveryhodného zdieľania údajov, ktoré popisujeme, sú:

- Informačný systém Centrálna správa referenčných údajov (IS CSRÚ), ktorý slúži predovšetkým na zdieľanie dôveryhodných údajov v rámci verejnej správy,
- Manažment osobných údajov (MOU), v ktorom získavajú občania a podnikatelia (dotknuté osoby a subjekty) dôveryhodné údaje, ktoré o nich verejná správa eviduje, cez IS CSRÚ, a môžu ich zdieľať tretím stranám.

Interoperabilita a integrita pri zdieľaní údajov je zabezpečovaná využitím transformácie podľa Centrálneho modelu údajov. MOU musí adresovať nasledujúce otázky, aby bolo zabezpečené dôveryhodné zdieľanie údajov pre tretie strany:

- Bezpečná autentifikácia používateľa,
- Ukladanie a ochrana osobných údajov v MOU,
- PKI a uloženie privátneho kľúča,
- Autorizácia osobných údajov,
- Zdieľanie overiteľných údajov.

Výstup vznikol ako realizácia aktivity číslo 1 Manažment kvality údajov a činnosti Návrh štandardného katalógu služieb pre kvalitu údajov. Zámerom je poskytnutie návodu na využitie dostupných nástrojov a služieb (služby pre zdieľanie údajov MOU). Zároveň analyzujeme najlepšiu prax pre dôveryhodné zdieľanie údajov.

Ambíciou Dátovej kancelárie verejnej správy je spustiť implementáciu konceptu „Data-driven state“ (teda štátu, ktorý funguje na základe využívania dát) do praxe v podmienkach verejnej správy na Slovensku. Zámer si vyžaduje výrazne zlepšenie využívania a spracovania údajov na analytické účely inštitúciami verejnej správy. Štát bude prijímať rozhodnutia na základe najlepších znalostí, ktoré sú k dispozícii. Takáto transformácia si vyžaduje nastavenie riadenia životného cyklu dát a zmenu spôsobu

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

rozhodovania. Koncept dôveryhodnosti údajov definuje dôležité aspekty manažmentu údajov, a to dátovú integritu a klasifikáciu a kategorizáciu údajov v informačných systémoch verejnej správy. Následne je možné navrhnúť mechanizmy pre zabezpečenie dôveryhodného zdieľania a budovanie dátového trhoviska ako súčasť spoločných európskych dátových priestorov[1].

1.2 Metodika realizácie výstupu:

Realizácia dokumentu pozostávala z nasledovných krokov:

- Definovanie konceptu dôveryhodných údajov a ich zdieľania.
- Zadefinovanie pojmov klasifikácia a kategorizácia údajov.
- Klasifikácia údajov v zmysle ich citlivosti.
- Následné prepojenie s možnosťou ich ďalšieho spracúvania a zaraďovania do kategórií údajov zadefinovaných v návrhu zákona o údajoch - ako referenčné, moje, otvorené údaje; možnosti využitia údajov v rámci analytického spracúvania dát, z hľadiska ich obsahu i požiadaviek na štandardy/prepojenie na Príručky/Metodické pokyny ako výstupy z iných aktivít.
- Identifikácia a výber štandardov pre zdieľanie citlivých dôveryhodných a overiteľných údajov v rámci Manažmentu osobných údajov.

[1] Zdroj: http://dataspaces.info/common-european-data-spaces/#page-content, Dátum referencie: 6.3.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

2 Koncept dôveryhodných údajov a ich zdieľania

2.1 Definovanie pojmov

Nasledovné vybrané pojmy a ich definície vyplývajú z nariadenia Európskeho parlamentu a Rady EÚ 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov („**Nariadenie**“ alebo „**GDPR**“) a zo zákona číslo 18/2018 Z. z. o ochrane osobných údajov („**Zákon**" alebo „**zákon o ochrane osobných údajov**“). Okrem pojmu osobný údaj, ktorý je definovaný v § 2 zákona o ochrane osobných údajov, sú ostatné pojmy definované v § 5 tohto zákona. Nariadenie tieto pojmy definuje v článku 4.

V súlade s princípom priamej aplikovateľnosti je Nariadenie priamo záväzné na celom území EÚ, vrátane Slovenskej republiky, pričom cieľom prijatia zákona o ochrane osobných údajov bolo najmä upraviť špecifické podmienky v oblastiach, v ktorých Nariadenie ponecháva členským štátom priestor na vlastnú vnútroštátnu úpravu. Zároveň aj tu platí zásada prednosti alebo nadradenosti práva EÚ zakotvená nielen v práve EÚ ale aj v Ústave SR, ktorá znamená, že v prípade rozporu medzi Nariadením a Zákonom, má Nariadenie prednosť a teda, že v takom prípade je nutné pri ochrane osobných údajov postupovať podľa ustanovení Nariadenia.

Spracúvanie osobných údajov - spracovateľská operácia s osobnými údajmi alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

Dotknutá osoba - každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Osobný údaj - údaj tykajúci sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Prevádzkovateľ - každý, kto vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene. Prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

Sprostredkovateľ - každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Príjemca - každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy ktorou je Slovenská republika

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

Informačný systém - akýkoľvek usporiadaný súbor údajov (akýchkoľvek, aj osobných), ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe.

Súhlas dotknutej osoby - je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov. Súhlas dotknutej osoby musí byť zároveň hodnoverne preukázateľný.

Porušenie ochrany osobných údajov - porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

Zodpovedná osoba - osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona o ochrane osobných údajov alebo GDPR.

Vnútropodnikové pravidlá - postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine.;

Kódex správania - súbor pravidiel ochrany osobných údajov dotknutej osoby, ktoré sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať. Jeho účelom je upresniť, konkretizovať dodržiavanie jednotlivých povinností podľa GDPR a zákona o ochrane osobných údajov týkajúcich sa spracúvania a ochrany osobných údajov s ohľadom na osobitné charakteristiky určitého odvetvia, pre ktoré konkrétny kódex správania bol schválený. Ku kódexom správania je možnosť pristúpiť a zaviazať sa ich dodržiavať dobrovoľne. V kódexoch správania sa nastavujú povinnosti prevádzkovateľov a sprostredkovateľov so zreteľom na riziko (a s ohľadom na osobitné charakteristiky určitého odvetvia), ktoré pravdepodobne vyplýva zo spracúvania osobných údajov, pokiaľ ide o práva fyzických osôb.

Pseudonymizácia - spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej alebo identifikovateľnej fyzickej osobe. Aj p seudonymizované údaje sú však naďalej považované za osobné údaje.

Log – záznam o tom, aké činnosti prebiehali alebo prebiehajú v automatizovanom informačnom systéme.

Ďalšie vybrané pojmy a ich definície vyplývajú z nariadenia Európskeho Parlamentu a Rady (EÚ) 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej ako „**nariadenie o elektronickej identifikácii a dôveryhodných službách**“ alebo „**eIDAS**“), ako aj zo zákona číslo 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej ako „**zákon o dôveryhodných službách**“):

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Dôveryhodná služba – elektronická služba spočívajúca vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.

Kvalifikovaná dôveryhodná služba – je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky stanovené eIDAS.

Poskytovateľ dôveryhodnej služby – fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb.

Kvalifikovaný poskytovateľ dôveryhodných služieb – je poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb, a ktorému orgán dohľadu udelil kvalifikovaný štatút.

2.1.1 Dôveryhodnosť údajov

Požiadavka na dôveryhodnosť údajov v informačných systémov vyplýva z Nariadenia, zo zákona o ochrane osobných údajov, ako aj z praktických očakávaní organizácii, ktoré osobné údaje spracúvajú a využívajú v rámci svojej činnosti. Dôveryhodnosť údajov je meraná súladom s jednak požiadavkami Nariadenia, zákona o ochrane osobných údajov a tiež očakávaniami organizácií, ktoré osobné údaje spracúvajú, aby toto spracúvanie mohlo dosahovať nimi stanovené ciele a účely, a v neposlednom rade aj v súlade s očakávaniami a oprávnenými záujmami dotknutých osôb, ktorých údaje sú v informačných systémoch rôznych organizácií spracúvané.

Dôveryhodnosť alebo integrita osobných údajov je kľúčovou vlastnosťou, ktorá má byť v rámci informačných systémov zabezpečená prostredníctvom legálnych a legitímne používaných nástrojov, opatrení postupov a procesov.

Súbor takýchto nástrojov, opatrení, postupov a procesov na zabezpečenie dôveryhodnosti osobných údajov v informačnom systéme by mal byť implementovaný v každej organizácii, ktorá spracúva osobné údaje, pričom by mal v prvom rade účinne reflektovať všetky požiadavky a povinnosti organizácie (napríklad prevádzkovateľa alebo sprostredkovateľa) vyplývajúce z Nariadenia a zákona o ochrane osobných údajov, ale aj požiadavky organizácie vyplývajúce z jej činnosti.

Práve tento súbor nástrojov, opatrení, postupov a procesov (Compliance program) by mal byť implementovaný a priebežne upravovaný tak, aby zabezpečoval vyššie uvedený súlad spracúvania osobných údajov v organizácii a prispieval ku konzistentnej ochrane osobných údajov.

Konzistentná úroveň ochrany osobných údajov je jedným z hlavných cieľov deklarovaných GDPR, ktoré vyžaduje, aby sa konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv a slobôd fyzických osôb pri spracúvaní osobných údajov zabezpečilo v rámci celej EÚ.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Cieľom GDPR je zaručiť konzistentnú úroveň ochrany fyzických osôb v celej Únii a zabrániť rozdielom, ktoré sú prekážkou voľného pohybu osobných údajov v rámci vnútorného trhu. Konzistentná ochrana osobných údajov poskytne:

- právnu istotu a transparentnosť hospodárskym subjektom,
- fyzickým osobám vo všetkých členských štátoch rovnakú úroveň právnej vymožiteľných práv.

Riadne fungovanie vnútorného trhu si vyžaduje, aby voľný pohyb osobných údajov v rámci EÚ nebol obmedzený ani zakázaný z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov a preto Nariadenie prevádzkovateľom a sprostredkovateľom:

- ukladá povinnosti a zodpovednosti, ktorých cieľom je zabezpečenie konzistentného monitorovania spracúvania osobných údajov,
- stanovuje rovnocenné sankcie vo všetkých členských štátoch,
- vytvára jednotné prostredie pre účinnú spoluprácu dozorných orgánov rozličných členských štátov.

S cieľom zabezpečiť konzistentné uplatňovanie Nariadenia v celej EÚ bol zriadený **mechanizmus konzistentnosti pre spoluprácu medzi dozornými orgánmi.** Mechanizmus konzistentnosti sa uplatňuje, keď má dozorný orgán v úmysle prijať opatrenie, ktoré má zakladať právne účinky v súvislosti so spracovateľskými operáciami, ktoré podstatne ovplyvňujú značný počet dotknutých osôb vo viacerých členských štátoch, ako aj vtedy, keď niektorý dozorný orgán alebo Európska komisia o to požiadajú.

Ďalším nástrojom pre zabezpečenie konzistentného fungovania vnútorného trhu EÚ je **jednotná digitálna brána** zriadená nariadením Európskeho parlamentu a Rady (EÚ) 2018/1724 o zriadení jednotnej digitálnej brány na poskytovanie prístupu k informáciám, postupom a asistenčným službám a službám riešenia problémov (známe ako nariadenie SDG). Jednotná digitálna brána by mala uľahčovať interakciu medzi občanmi resp. podnikmi a príslušnými orgánmi prostredníctvom online riešení, ktoré by mali minimalizovať prekážky na vnútornom trhu.

V záujme konzistentného uplatňovania pravidiel ochrany údajov v celej EÚ, ako aj v záujme implementácie mechanizmu konzistentnosti, bol zriadený **Európsky výbor pre ochranu osobných údajov** (European Data Protection Board – EDPB), ktorý:

a) prijíma všeobecné usmernenia na objasnenie podmienok európskych právnych predpisov o ochrane údajov,
b) poskytuje jednotný výklad práv a povinností vyplývajúcich z GDPR,
c) prijíma záväzné rozhodnutia voči vnútroštátnym dozorným orgánom v záujme zabezpečenia konzistentného uplatňovania,
d) poskytuje všeobecné usmernenia (vrátane usmernení, odporúčaní a najlepších postupov) na objasnenie Nariadenia,
e) poskytuje poradenstvo Európskej komisii v akejkoľvek veci týkajúcej sa ochrany osobných údajov a nových navrhovaných právnych predpisov v Európskej únii,
f) prijíma zistenia o konzistentnosti v cezhraničných prípadoch týkajúcich sa ochrany údajov a,

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

g) podporuje spoluprácu a účinnú výmenu informácií a najlepších postupov medzi vnútroštátnymi dozornými orgánmi.

Cieľ konzistentnej úrovne ochrany osobných údajov sa z popísanej inštitucionálnej úrovne má plynulo preniesť na organizácie, ktoré spracúvajú osobné údaje. Tieto organizácie pôsobiace ako prevádzkovatelia alebo sprostredkovatelia sú povinné v rámci svojej činnosti napĺňať cieľ konzistentnej ochrany údajov a prinášať ho do praktického života.

V prvom rade sú povinné dodržiavať nasledovné zásady spracúvania osobných údajov definované v prvej hlave zákona o ochrane osobných údajov (najmä § 6 až § 13), ako aj v článku 5 a článku 6 Nariadenia:

- **Zásada zákonnosti** – osobné údaje možno spracúvať len zákonným spôsobom, ktorý nebude znamenať porušenie základných práv dotknutej osoby, pričom spracúvanie je zákonné len vtedy, ak sa vykonáva na základe Zákonom stanovených právnych základov, napríklad na základe súhlasu dotknutej osoby so spracúvaním osobných údajov, alebo ak je spracúvanie nevyhnutné podľa osobitného právneho predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná; ak je nevyhnutné na plnenie zmluvy, ktorou je dotknutá osoba viazaná, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby; ak je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, na plnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany, to ale iba v prípade, že ich záujem neprevažuje nad záujmami alebo právami dotknutej osoby, najmä dieťaťa, ktoré si vyžadujú ochranu osobných údajov (tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh).
- **Zásada obmedzenia účelu** – osobné údaje môžu byť získavané len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú byť spracovávané takým spôsobom, ktorý by popieral tento účel alebo by s ním nebol zlučiteľný. Ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom, a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8 Zákona, sa nepovažuje za nezlučiteľné s pôvodným účelom.
- **Zásada minimalizácie osobných údajov** – osobné údaje musia byť spracúvané v primeranom, relevantnom a obmedzenom rozsahu, ktorý je nevyhnutný pre daný účel spracúvania, spracúvať teda možno len tie osobné údaje, ktoré majú viesť k naplneniu stanoveného účelu a žiadne iné.
- **Zásada správnosti** – spracúvané osobné údaje musia byť správne a podľa potreby aktualizované, teda aktuálne, musia sa prijať primerané a účinné opatrenia na zabezpečenie bezodkladného vymazania alebo opravy osobných údajov, ktoré sú z hľadiska účelu nesprávne.
- **Zásada minimalizácie uchovávania** – osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú, pričom osobné údaje sa môžu uchovávať aj dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, a to za podmienky, že sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8 Zákona.
- **Zásada integrity a dôvernosti** - osobné údaje musia byť spracúvané spôsobom, ktorý vďaka primeraným technickým a organizačným opatreniam zaručí primeranú

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou, výmazom alebo poškodením osobných údajov.

- **Zásada zodpovednosti** - prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie dozorného orgánu (napríklad Úradu na ochranu osobných údajov SR) preukázať.

Princípy dôveryhodnosti údajov

Dôveryhodný údajov je údaj, u ktorého je vysoká miera istoty, že nebol nejakým spôsobom narušený, poškodený alebo pokazený, že k nemu nemá prístup niekto na to neoprávnený, a že nedošlo k jeho neoprávnenej alebo neodôvodnenej zmene.

Dôveryhodnosť údajov je komplexná disciplína, ktorú ovplyvňuje to, ako sú údaje získavané, uchovávané, ako sa k nim pristupuje, aj to, ako sú používané.

Dôveryhodnosť údajov obsahuje mnoho znakov a elementov, ktoré vytvárajú zrozumiteľné prostredie vhodné na to, aby údaje v ňom mohli byť dôveryhodné. Toto prostredie je vytvárané primeraným množstvom štandardov, pravidiel, procesov a postupov, ktoré sú monitorované a dodržiavané osobami, ktoré sa majú o toto prostredie starať, ako aj užívateľmi alebo príjemcami údajov.

Z uvedených zásad spracúvania vyplýva detailnejšia definícia dôveryhodnosti osobných údajov, ide o nasledovné atribúty, ktoré musia byť splnené, aby mohli byť údaje považované za dôveryhodné:

- **Kvalita** (tomuto aspektu sa podrobnejšie venuje dokument 1.1.1 Štandardizácia dátovej kvality):

Kvalita je kľúčová vlastnosť údajov, ktoré majú byť považované za dôveryhodné, pričom v rámci hodnotenia kvality údajov sa sleduje, či sú údaje:

a) **Kompletné**, teda či sú k dispozícii všetky potrebné údaje, resp. údaje nevyhnutné pre naplnenie účelu spracúvania a zároveň údaje v datasete nesmú byť nadbytočné, spracúvané pre istotu alebo z iného nerelevantného dôvodu, údaje sú udržiavané vo svojej plnej forme a žiadne časti údajov nie sú filtrované, skomolené alebo stratené.

Príklad: ak sa vykonalo 50 testov, kompletné údaje by mali obsahovať informácie o všetkých 50 testoch, pričom výsledky testov, ktoré nedopadli dobre alebo podľa očakávaní, nie sú opomenuté alebo vymazané.

b) **Správne** alebo iným slovom platné pre ciele, ktoré má spracúvanie údajov plniť, pričom získané údaje by mali byť v súlade so zadefinovanou štruktúrou, údaje nesmú byť pozmenené alebo agregované spôsobom, ktorý by ovplyvnil ich analýzu.

Príklad: výsledky testov nie sú zaokrúhlené ani smerom nahor ani smerom nadol a kritéria testovania a jeho podmienky sú presne zdokumentované a zrozumiteľne popísané, pričom opakované testy by mali priniesť rovnaké výsledky.

c) **Aktuálne**, pravidelne kontrolované, či údaj nie je zastaraný, pričom v prípade zmien je vykonaná oprava, ktorá je v súlade s momentálnou realitou.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Príklad: ak dôjde k zmene priezviska, telefónneho čísla alebo čísla dokladu totožnosti v Registri fyzických osôb, dôjde k príslušnej zmene aj vo všetkých informačných systémoch, ktoré s týmito osobnými údajmi pracujú.

d) **Konzistentné**, to znamená, že údaje zostanú nezmenené bez ohľadu na to, ako, alebo ako často sa využijú alebo ako dlho sú uchovávané.

Príklad: údaje, ktoré sa rok nepoužijú, zostanú rovnaké aj po roku nevyužívania.

- **Bezpečnosť** (tomuto aspektu sa podrobnejšie venuje dokument 1.1.3 Štandardizácia pre bezpečnosť a ochranu údajov):

Bezpečnosť sa často zamieňa s integritou, ale v skutočnosti je bezpečnosť samostatnou kategóriou, ktorá prispieva k integrite alebo dôveryhodnosti údajov.

Bezpečnosť údajov predstavuje infraštruktúru, nástroje a pravidlá používané s cieľom zaistiť, že:

a) prístup k údajom dostanú výlučne oprávnení užívatelia,
b) údaje sú používané v súlade s určeným spôsobom,
c) údaje sú zabezpečené a chránené proti strate, krádeži alebo inému trestnému činu.

Narušenie dôveryhodnosti údajov môže spôsobiť nechcená alebo neočakávaná zmena údajov, ktorá sa udeje počas uchovávania, prístupu k nim alebo počas spracovávania, a je vnímaná ako zlyhanie alebo strata dôveryhodnosti údajov.

Prevádzkovateľ a sprostredkovateľ sú v zmysle zákona o ochrane osobných údajov povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie dôveryhodnosti údajov. Tieto opatrenia musia byť primerané spomínanému riziku ohrozenia práv fyzických osôb a môžu zahŕňať najmä:

- pseudonymizáciu a šifrovanie osobných údajov,
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
- proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Pri posudzovaní primeranej úrovne bezpečnosti je nutné prihliadať na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä:

- náhodné alebo nezákonné zničenie,
- strata, zmena alebo neoprávnené poskytnutie zdieľaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov,
- neoprávnený prístup k takýmto osobným údajom.

Súlad s požiadavkami uvedenými vyššie možno preukázať schváleným kódexom správania v zmysle zákona o ochrane osobných údajov.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

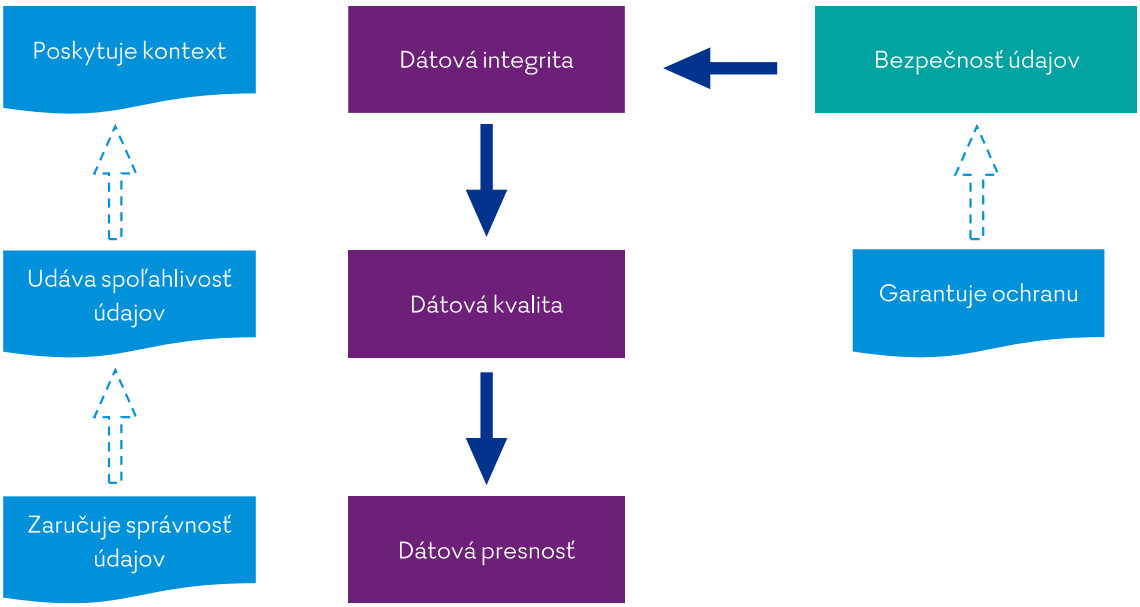
Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

2.1.2 Dátová integrita

Integrita údajov znamená, že údaje sú správne, presné, relevantné, kompletné a vhodné na účel, pre ktorý sú spracovávané. Integrita údajov tiež znamená vysokú mieru istoty, že údaje nie sú poškodené, že sú platné a majú k nim prístup výlučne osoby, ktoré sú na to oprávnené.

Z vyššie uvedeného je zrejmé, že integrita môže mať blízko, alebo môže byť zamieňaná za bezpečnosť údajov alebo kvalitu údajov, ale v skutočnosti ide o samostatné a obsahom odlišné pojmy.

Platí, že bezpečnosť údajov a kvalita údajov sú súčasťou širšieho pojmu integrity údajov. Vzťah týchto pojmov znázorňuje aj Obrázok 1. Pričom úroveň integrity údajov významným spôsobom prispieva k dôveryhodnosti alebo nedôveryhodnosti údajov a informačných systémov.



Obrázok 1: Schematické vysvetlenie vzťahov medzi pojmami bezpečnosť, integrita, kvalita a presnosť

Integrita údajov zahŕňa fyzickú integritu a logickú integritu:

- **Fyzická integrita** sa týka uchovávania (skladovania) a obnovovania údajov v rámci úložných systémov a zariadení, pamäťových zložkách a hardvéroch. Ide teda o integritu infraštruktúry, v ktorej sa údaje nachádzajú, ktorú ohrozujú najmä:
  - chyby a zlyhania hardvéru alebo dizajnu,
  - prirodzené opotrebenie (napríklad korózia),
  - zlyhanie energetických dodávok,
  - prírodné katastrofy,

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

- radiácia a environmentálne krízové situácie.

- **Logická integrita** sa týka najmä správnosti a relevantnosti dát v rámci určitého kontextu, kde je dôležité, či údaje dávajú zmysel alebo či neboli napríklad nečakane pozmenené, a to na základe:
  - konštrukčných chýb softvéru, ktoré robia softvér a údaje v ňom zraniteľnými, a ktoré môžu mať za následok reálne zlyhania softvéru,
  - (náhodného) ľudského pochybenia, ktoré zníži kvalitu dát alebo ich kompletnosť,
  - (úmyselného resp. vedomého) nezákonného počínania, ktorého výsledkom je narušenie systému a akékoľvek znehodnotenie údajov,
  - chýb v prenose údajov, ktorých následkom je strata, poškodenie, vymazanie alebo krádež údajov.

Prevádzkovatelia sú povinní voči týmto rizikám vykonať opatrenia na minimalizovanie rizík súvisiacich s vyššie uvedenými hrozbami a predchádzanie negatívnych dopadov, ktoré môžu pri nich nastať.

Tieto opatrenia musia byť účinné a podliehať pravidelnej kontrole a testovaniu počas celého životného cyklu údajov alebo informačných systémov, v ktorých sa údaje nachádzajú. Takýmito nástrojmi sú napríklad zálohovanie údajov, limitovanie prístupu k nim, pravidelná validácia údajov, používanie logov, používanie detekčných softvérov a podobne.

Úroveň integrity údajov sa meria úrovňou nasledovných schopností systémov, v ktorých sa údaje nachádzajú:

- **Obnovovanie a prístupnosť** – správne údaje, na správnom mieste a v správnom čase
- **Vysledovateľnosť** – každý úkon týkajúci sa údajov musí zanechať stopu (log), ktorú je možné v systéme sledovať
- **Spoľahlivosť a konzistentnosť** – údaje musia zodpovedať potrebám, pre ktoré boli získané.

Okrem partikulárnych záujmov organizácie, ktorá údaje akýmkoľvek spôsobom spracováva, je budovanie a ochrana integrity údajov dôležité tiež kvôli tomu, že integrita je nielen jednou z hlavných zásad spracovávania osobných údajov, ale premieta sa do nej množstvo povinností, ktoré prevádzkovateľovi alebo sprostredkovateľovi ukladá dodržiavať a plniť GDPR a zákon o ochrane osobných údajov, pričom nedodržiavanie týchto povinností so sebou prináša obrovské reputačné, ale aj finančné riziká v podobe vysokých pokút, ktoré sú dozorné orgány oprávnené ukladať.

2.1.3 Overiteľné údaje

Schopnosť preukázať integritu a pravosť zdieľaných údajov je kľúčovým prvkom pri vytváraní dôvery online. Vzhľadom na to, že spoločnosť produkuje veľké množstvo údajov a neustále ich zdieľa a presúva, je zložité nájsť riešenie, ktoré bude fungovať pre väčšinu používateľov rôznych online IT systémov v rôznych kontextoch.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Základným problémom, ktorý je potrebné riešiť, je, ako stanoviť autoritu pre zdieľaný dataset alebo jeho časť, a ako vytvoriť mechanizmy na presadenie dôvery v tieto autority v širokom kontexte. Vyriešenie tohto problému na principiálnej úrovni dodá všetkým dotknutým osobám a subjektom väčšiu dôveru v údaje, ktoré zdieľajú, a prijímateľom umožní pochopiť integritu a pravosť zdieľaných údajov.

Na označenie tejto problémovej oblasti budeme používať zastrešujúci pojem overiteľné údaje. Overiteľné údaje možno ďalej rozšíriť na tri kľúčové piliere:

1. Overiteľné údaje: zabezpečujú pravosť a integritu skutočných zdieľaných dátových prvkov, ktoré možno overiť.
2. Overiteľné vzťahy: týkajú sa možností kontrolovať a pochopiť prepojenia medzi rôznymi entitami, ako aj spôsob, akým sú jednotlivé entity reprezentované v údajoch.
3. Overiteľné procesy: opisujú možnosť overiť akýkoľvek elektronický proces, akým je napríklad zapísanie používateľa do informačného systému alebo správa účtu daňovníka (najmä s ohľadom na to, ako údaje umožňujú riadenie a udržiavanie procesu).

Overiteľné údaje sú najčastejšie implementované pomocou technológie „blockchain“[2] alebo aplikovaním štandardu W3C pre „Verifiable Credentials (VC)“[3], ktorý implementuje do praxe aj národný projekt „Manažment osobných údajov“ v rámci dátového programu Dátovej kancelárie[4]. Mechanizmus VC založený na štandarde W3C (Obrázok 2 a kapitola 4.2) sa používa v mnohých vzdelávacích inštitúciách na vystavenie overiteľných údajov o dosiahnutom vzdelaní a akademických výsledkoch, pričom autoritou pre vydanie týchto údajov sú samotné univerzity, na ktorých dotknuté osoby študovali[5]. Ďalším štandardom je Credential Transparency Language (CTDL) v Credential Engine[6], ktorý posytuje podrobnejší slovník na opis organizácií, zručností, pracovných pozícií a dokonca aj postupov („pathways“).

[2] Zdroj: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Verifiable+Credentials+Success+Stories, Dátum referencie: 24.04.2023

[3] Zdroj: https://www.w3.org/TR/vc-data-model/, Dátum referencie: 24.04.2023

[4] Zdroj: https://datalab.digital/cip-a-mou/manazment-osobnych-udajov/, Dátum referencie: 24.04.2023

[5] Zdroj: https://www.digitary.net/digitary-testimonials/, Dátum referencie: 24.04.2023

[6] Zdroj: https://credentialengine.org/, Dátum referencie: 24.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Obrázok 2: Mechanizmus VC pre overiteľné údaje podľa štandardu WC3[7]

2.1.4 Klasifikácia údajov

Klasifikácia údajov je rozhodujúcim krokom, ktorého cieľom je vniesť disciplínu do vzťahu medzi technologickým sektorom a používateľmi, ktorí sú na základe týchto údajov identifikovaní. Tento proces a jeho výsledok pomôže podnikom a organizáciám vyhodnotiť svoj zber údajov z pohľadu používateľov, ktorých údaje zhromažďujú. Tento proces zahŕňa priradenie úrovne dôvernosti a dôležitosti každému údaju v informačnom systéme. Toto je nevyhnutné pre riadenie prístupu a ochranu údajov v verejnej správe, ktorým sa podrobne venujeme v dokumentoch 1.1.3 Štandardizácia pre bezpečnosť a ochranu údajov a 1.1.5 Štandardizácia anonymizácie údajov.

Klasifikácia údajov je potrebná najmä na pomoc pri organizovaní a analýze informácií ako aj pri presadzované správnych politík v rámci manažmentu údajov. Klasifikácia údajov umožňuje porozumieť typom informácií, ktoré sa spracúvajú a ukladajú, takže je možné nájsť vzory a korelácie a získať užitočné poznatky. Pomáha tiež zlepšiť presnosť údajov a urýchliť analýzu údajov. Poznatky získané klasifikáciou údajov umožňujú prijať potrebné opatrenia napríklad na ochranu údajov na základe ich dôležitosti alebo citlivosti. Klasifikácia tiež uľahčuje súlad s predpismi a môže viesť k úsporám nákladov implementáciou vhodnej úrovne zabezpečenia pre všetky informácie.

V závislosti od citlivosti údajov a mieru zasahovania do súkromia existujú 2 úrovne dôvernosti: zverejniteľné a nezverejniteľné údaje, pričom nezverejniteľné sa ďalej delia na interné, dôverné a vyhradené (táto kategorizácia je definovaná aj v dokumente 1.1.5 Štandardizácia anonymizácie údajov a zosumarizovaná v tabuľke nižšie (Tabuľka 1)).

Evidujeme tri typy závažnosti údajov: kritické, údaje s vysokou a nízkou závažnosťou. Kritické údaje sú údaje, ktoré by mali byť chránené pred stratou alebo poškodením. Údaje vysokej závažnosti sú údaje, ktoré by mali byť chránené pred poškodením alebo

[7] Zdroj: Detailný návrh riešenia (DNR): Manažment osobných údajov, Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

zneužitím. Nízka závažnosť údajov znamená, že údaje nie sú chránené pred stratou alebo poškodením.

Tabuľka 1: Kategorizácia údajov z pohľadu ochrany súkromia - Sumár

Klasifikácia údajov	
Prístupy	1. Kategorizácia podľa obsahu – kontrola a interpretácia obsahu a hľadanie citlivých informácií; 2. Kategorizácia podľa kontextu – kontrola metadát a iných premenných. Hľadanie nepriamych indikátorov citlivých informácií; 3. Kategorizácia podľa používateľa – manuálna klasifikácia podľa úsudku skúseného používateľa. Jednotlivci, ktorí pracujú s dokumentmi, môžu určiť, ako sú citlivé – môžu tak urobiť pri vytváraní datasetu alebo dokumentu, po významnej úprave alebo kontrole alebo pred zverejnením.
Hlavné dve úrovne a podkategórie nezverejniteľných údajov	1. **Zverejniteľné údaje** – údaje, ktorých zverejnenie ako otvorené údaje neohrozuje fungovanie štátu, organizácie či podniku a jeho systémov, alebo neodhaľuje intelektuálne vlastníctvo, a preto ich je možné kedykoľvek zverejniť.; 2. **Nezverejniteľné údaje** - údaje, ktoré nie je vhodné zverejniť v žiadnom prípade, pretože zverejnenie nesie riziko okamžitého alebo neskoršieho pokusu o narušenie informačnej bezpečnosti. Pre nezverejniteľné údaje môže existovať podmienka, za splnenia ktorej sa stanú zverejniteľnými: 1. **Vyhradené údaje** – Osobné alebo iné údaje, ktoré podliehajú najprísnejším požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko pre organizáciu a zákazníkov v prípade nesprávnej manipulácie. 2. **Dôverné údaje** – Osobné alebo iné údaje, ktoré podliehajú prísnym požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko v prípade nesprávneho zaobchádzania. 3. **Interné údaje** - Údaje, ktoré sú zamestnancom a prípadným tretím stranám k dispozícii na základe zmluvy/dohody o (zachovaní) mlčanlivosti výlučne v dôsledku ich zamestnania v organizácii alebo prebiehajúceho projektu či poskytovania služby a ktoré nie sú kategorizované ako dôverné alebo obmedzené.
Úrovne závažnosti údajov	1. Údaje s nízkou závažnosťou – určené na verejné použitie. Napríklad obsah verejných webových stránok. 2. Údaje vysokou závažnosťou – určené len na interné použitie, ale ak by boli kompromitované alebo zničené, nemali by katastrofický dopad. Napríklad e-maily a dokumenty bez dôverných údajov. 3. Kritické údaje – ak by boli ohrozené alebo zničené, mali by katastrofálny dopad na organizáciu alebo jednotlivcov. Napríklad finančné záznamy, duševné vlastníctvo, autentifikačné údaje.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

V prípade ukladania a spracovania údajov v cloudových službách možno údaje klasifikovať z pohľadu ochrany súkromia a vzťahu medzi technológiou cloudu a ochranou používateľov, ako ukazuje nasledujúca Tabuľka 2.

Tabuľka 2: Príklad klasifikácie údajov: ICO usmernenie pre hodnotenie rizika cloudu (UK)

Príklad klasifikácie údajov: ICO usmernenie pre hodnotenie rizika cloudu (UK)	
Klasifikácia dát	**Usmernenie na používanie cloudových služieb tretích strán**
Normálne	Cloudové úložisko a služby sa môžu používať na základe základnej úrovne istoty, že integrita a dostupnosť údajov bude zachovaná.
Vyhradené	Cloudové úložisko a služby sa môžu používať pod prísnym uistením o bezpečnosti.
Vysoko vyhradené	Cloudové úložisko a služby pravdepodobne nie sú vhodné, pokiaľ nejde o špecializovanú a vysoko zabezpečenú službu.
Utajované	Cloudové úložisko a služby by sa za normálnych okolností nemali používať.
Zdroj: ICO. 1998. Guidance on the use of cloud computing. Odkaz	

2.1.5 Kategorizácia údajov vo všeobecnosti

Kategorizácia údajov je proces, ktorým sa údaje rozdeľujú do skupín podľa ich typu alebo účelu. Kategorizácia údajov je proces oddeľovania a organizovania údajov do príslušných skupín na základe ich spoločných charakteristík, ako je úroveň ich citlivosti, riziká, ktoré predstavujú atď. Najmä na ochranu citlivých údajov je potrebné ich lokalizovať, kategorizovať podľa úrovne citlivosti a presne označiť.

Ak sa to robí správne, Kategorizácia údajov uľahčuje a zefektívňuje používanie a ochranu údajov (viď dokument 1.1.3 Štandardizácia pre bezpečnosť a ochranu údajov). Tieto kategórie by mali byť súčasťou dátového katalógu, popísaného v dokumente 1.1:2 Štandardizácia pre modelovanie údajov. Tento proces kategorizácie sa však často prehliada, najmä ak organizácie nerozumejú jeho úplnému účelu, rozsahu a schopnostiam. Bežne používané kategórie údajov sú:

- **podľa charakteru údajov:**
  - Normatívne – upravujú, regulujú správanie či činnosti subjektov. Sú zvyčajne vo forme dokumentov, čiastočne vnútorne štruktúrovaných;
  - Kategorizačné – umožňujú zaradenie do jednej z konečnej množiny kategórií (číselníky, zoznamy, jednoznačné referencovateľné identifikátory, kritériá);
  - Evidenčné – údaje o subjektoch, objektoch, veciach, financiách či iných entitách vedené v informačných systémoch verejnej správy (registre, údaje v systémoch evidencií, údaje v ďalších IS VS);
  - Agendové – súvisiace s výkonom agend verejnej správy;

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

  - Informatívne – súvisiace s výkonom verejnej moci OVM;
  - Dokumentárne – napríklad spravodajstvo, monitoring cestnej dopravy;
  - Prevádzkové - súvisiace s prevádzkou danej inštitúcie, informačno-komunikačných technológií, kontrolných a riadiacich systémov, elektroniky;
  - Odvodené údaje – sú výsledkom spracovania údajov z ostatných domén;
  - Doménové – finančné, priestorové, vzdelávacie, vedecko-technické, zdravotné, kultúrne, podnikové;
  - Ostatné;
- **podľa vlastníctva údajov:**
  - Údaje verejnej správy Slovenskej republiky;
  - Údaje verejnej správy inej členskej krajiny EÚ;
  - Údaje fyzických osôb a právnických osôb;
  - Údaje bez vlastníckeho práva;
- **podľa pôvodu údajov / zdroja:**
  - Primárny zdroj;
  - Sekundárny zdroj;
  - Terciárny zdroj;
  - Referenčný zdroj;
- **podľa typu a formy;**
- **podľa úrovne strojového spracovania:**
  - Úroveň 0★ až 5★
- **podľa typu interoperability zverejnených dát:**
  - Katalógy – sú kolekcie spravovaných údajov o datasetoch vrátane metadát;
  - Datasety – sú kolekcie dát, publikovaných a spracovaných definovaných gestorom, prístupné na prezeranie alebo na stiahnutie v jednom alebo viacerých formátoch;
  - Distribúcia datasetu - reprezentuje špecifickú formu dostupného datasetu. Každý dataset môže byť dostupný v rôznych formách, pričom tieto formy môžu reprezentovať rôzne súborové formáty (XML, CSV, RDF, ...) rozličné prístupové aplikačné miesta (API, RSS) alebo verzie v čase.
- **z pohľadu ochrany súkromia (podľa citlivosti údajov):**
  - Vyhradené – osobné alebo iné údaje, ktoré podliehajú najprísnejším požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko pre organizáciu a zákazníkov v prípade nesprávnej manipulácie.;
  - Dôverné – osobné alebo iné údaje, ktoré podliehajú prísnym požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko v prípade nesprávneho zaobchádzania.;
  - Interné – údaje, ktoré sú zamestnancom a prípadným tretím stranám k dispozícii na základe zmluvy/dohody o (zachovaní) mlčanlivosti výlučne v dôsledku ich zamestnania v organizácii alebo prebiehajúceho projektu či poskytovania služby a ktoré nie sú kategorizované ako dôverné alebo obmedzené.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Tabuľka 3: Kategorizácia údajov vo všeobecnosti - Sumár

Kategorizácia údajov vo všeobecnosti	
Prístupy	1. Manuálny – Tradičná metóda kategorizácie údajov ľudským zásahom. 2. Automatizovaný – Technologické riešenia eliminujú riziká ľudského zásahu vrátane chýb a zároveň znižujú náklady (nepretržitá kategorizácia všetkých údajov). 3. Hybridné – ľudský zásah poskytuje kontext pre kategorizáciu údajov, zatiaľ čo nástroje umožňujú efektívnosť.
Hlavné typy	• podľa charakteru údajov; • podľa vlastníctva údajov; • podľa pôvodu údajov / zdroja; • podľa typu a formy; • podľa úrovne strojového spracovania; • podľa typu interoperability zverejnených dát; • podľa citlivosti údajov.

2.2 Zdieľanie údajov

Štátne orgány v rámci plnenia svojich úloh získavajú od občanov a podnikateľov množstvo dát vrátane osobných údajov, pričom sa opakujú situácie, keď orgány získavajú údaje, ktoré štát už predtým získal alebo nimi disponuje na inom základe.

Kľúčom k efektívnemu spracovávaniu nielen osobných údajov je namiesto ich duplicitného získavania ich zdieľanie, a to nie len v prostredí štátnej správy, ale aj mimo nej v rozsahu legislatívnych účelov. V prípade súhlasu dotknutej osoby alebo subjektu aj mimo týchto dvoch uvedených scenárov.

S týmto cieľom sú spojené rôznorodé úskalia, ktoré efektívne zdieľanie údajov komplikujú alebo priamo znemožňujú, a ktoré tvoria celé spektrum problémov s tým spojených, od dostupnosti, dôveryhodnosti a overiteľnosti údajov, cez technické a organizačné možnosti spojené s prevádzkou systémov obsahujúcich údaje, materiálne a personálne kapacity, až po integritu, bezpečnosť a dôvernosť spracovávania údajov, ktoré sú nevyhnutným predpokladom dôvery občanov a podnikateľov, ktorých osobné a iné citlivé údaje majú byť spracovávané.

Získavanie údajov

Základným predpokladom efektívneho, úspešného a užitočného spracovávania nielen osobných údajov je ich získanie, a to jednak v súlade so zákonom o ochrane osobných údajov, ako aj v súlade s účelmi a cieľmi spracovávania. V praxi sa ukazuje, že v rámci tohto štádia sa prevádzkovatelia informačných systémov stretávajú s nasledovnými problémami:

- **nedostupnosť údajov** plynúca z nedostupnosti zdrojov alebo nesprávnych metodík určujúcich zdroje údajov.
- **nedostatočná kvalita údajov**, na ktorú má často vplyv, že organizácie získavajú obrovské množstvá údajov, ktoré však nie sú správne, platné, zrozumiteľné, konzistentné, kompletné a podobne.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

- **nerelevantnosť údajov** nadväzuje na nedostatok pozornosti venovanej kvalite údajov a vyplýva z nesprávneho dizajnu a metód získavania údajov, ako aj manažmentu prístupu k údajom, ktorého výsledkom je, že oprávnené osoby pracujú so systémami obsahujúcimi aj množstvo údajov, ktoré nie sú potrebné resp. nevyhnutné na dosiahnutie účelu konkrétneho spracovávania údajov.

Organizačné, procesné a prevádzkové prekážky

Tieto prekážky majú významný vplyv na to, akým spôsobom sa dáta využívajú, ako ľahko alebo ťažko sa dajú v systéme vyhľadať, alebo objaviť, aby mohli byť využité na splnenie legitímnych cieľov a účelov. Ide o nasledujúce prekážky:

- **Organizačné prekážky,** spôsobené myslením a konaním v uzatvorených navzájom nekomunikujúcich silách, znemožňujú opätovné používanie dát a ich zdieľanie naprieč rôznymi organizáciami.
- **Procesné prekážky** zdieľania údajov spočívajú najmä v tom, že organizácie si často nie sú vedomé, akými údajmi disponujú, alebo nie sú schopné ich vytiahnuť z informačných systémov, zdieľať či zmysluplne využiť, aj keď by to bolo v záujme a v prospech dotknutých osôb a iných subjektov.
- **Prevádzkové prekážky** majú spoločného menovateľa, ktorým je nejednotnosť resp. neschopnosť vysporiadať sa s rozmanitosťou systémov a procesov, ktorá sa pretavuje do neschopnosti zdieľať údaje napríklad preto, že sú v rôznych formátoch, ktoré rôzne systémy nie sú schopné spracovať alebo čítať, ale aj preto, že v organizáciách vo všeobecnej rovine chýbajú kvalitné riadiace procesy.

Personálne a materiálne kapacity

Napriek tomu, že sa údaje stávajú v mnohých organizáciách najdôležitejším a najcennejším majetkom, zostávajú investície do kapacít, ktoré sa majú o tento majetok starať, na úrovni, ktorá nezodpovedá jeho významu („len 20,6 % vedúcich pracovníkov, teda sotva každý piaty, uviedlo, že v ich spoločnosti bola úspešné zavedená dátová kultúra, čo predstavuje 27 % pokles oproti 28,3 % spoločností, ktoré v roku 2019 uviedli, že už majú zavedenú dátovú kultúru.“)[8].

Kľúčové kapacity, ktoré je nevyhnutné rozvíjať aj v záujme efektívneho zdieľania dát, sa týkajú jednak ľudí, ktorí majú k dátam prístup a pracujú s nimi, a tiež technických a materiálnych podmienok, do ktorých sú informačné systémy a údaje zasadené. „V prieskume Harvard Business Review vedúci pracovníci skúmaných spoločností už piaty rok po sebe uviedli, že najväčšou prekážkou v súvislosti s dátovými iniciatívami nie sú technologické problémy, ale problémy so zmenou kultúry. V prieskume z roku 2021 92,2 % hlavných spoločností uviedlo, že naďalej zápasia s kultúrnymi výzvami týkajúcimi sa organizačného zosúladenia, biznis procesov, riadenia zmien, komunikácie, zručností zamestnancov a odporu alebo nedostatočného pochopenia pri umožňovaní zmien.“[9] Tieto problémy neobchádzajú ani verejný sektor, ktorý má navyše ešte nevýhody pri získavaní talentu oproti súkromnému sektoru, predovšetkým čo sa týka výšky platov a dynamiky pracovného prostredia. Pri budovaní kapacít musia lídri organizácií preukázať, že im ide o dlhodobý cieľ, musia sa držať týchto investícií a nestratiť

[8] Zdroj: https://hbr.org/2023/01/has-progress-on-data-analytics-and-ai-stalled-at-your-company, Dátum referencie: 24.04.2023

[9] Zdroj: https://hbr.org/2021/02/why-is-it-so-hard-to-become-a-data-driven-company, Dátum referencie: 24.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

trpezlivosť alebo neznížiť úsilie, keď sa výsledky nedostavia okamžite. Zároveň treba rýchlo demonštrovať hodnotu dátového programu prostredníctvom „rýchlych víťazstiev“ aj smerom k verejnosti, čím možno obhájiť investície a identifikovať ďalšie prípady použitia so zásadným pozitívnym vplyvom na rôzne agendy. Dlhodobý program budovania interných personálnych kapacít musí zahŕňať:

- **Digitálne zručnosti** zamerané napríklad na dátovú gramotnosť, komunikáciu a manažment,
- **Líderské schopnosti** zamerané na vedenie ľudí, ale napríklad konkrétne aj na zvládanie komplexných situácií a ťažkostí pri vedení projektov,
- **Analytické nástroje**, ktoré pomôžu zabezpečiť napríklad poskytovanie užitočných dát alebo prepájanie systémov za účelom opätovného využitia dát,
- **Zdieľané platformy** vlastnené štátom, ktoré umožnia dôveryhodné a bezpečné zdieľanie údajov naprieč štátnou správou a v prípade súhlasu dotknutej osoby či subjektu aj naprieč neštátnymi organizáciami.

Dôvera občanov a podnikateľov

Okrem vyššie popísaného konceptu dôveryhodnosti údajov (kapitola 2.1.1), kde otázka dôvery smeruje od užívateľa k údajom, ktoré má využívať, je veľmi dôležitým atribútom dôvera dotknutých osôb a subjektov, ktoré majú svoje údaje zveriť systému za účelom ich spracovávania.

V rámci získavania alebo upevňovania dôvery je nevyhnutné zamerať sa na etické a zodpovedné využívanie údajov, požiadavky na ochranu súkromia, transparentnosť a overiteľnosť spracovávania, stanovenie podmienok na výkon práva na údaje a manažment rizík spojených so spracovávaním údajov.

2.2.1 Legislatívny rámec

1. V podmienkach Slovenskej republiky je ohľadom zdieľania osobných údajov určujúci **Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**[10] **a Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov - GDPR)**[11], z ktorého národný zákon o ochrane osobných údajov vychádza. Oba legislatívne akty obsahujú podmienky platné pre akékoľvek legitímne spracovávanie osobných údajov, a to vrátane ich prenosu, prenosnosti a zdieľania.

V prípade zdieľania údajov je kľúčový súhlas dotknutej osoby s prípadným zdieľaním, transparentnosť informácií o zdieľaní spoločne s dodržiavaním základných zásad spracovávania osobných údajov a zabezpečením práv dotknutej osoby aj v prípade zdieľania jej údajov.

2. Reguláciu údajov, ktoré nemôžu byť považované za osobné údaje, zabezpečuje v európskom priestore **Smernica Európskeho parlamentu a Rady EÚ 2019/1024 o**

[10] Zdroj: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/, Dátum referencie: 24.04.2023

[11] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016R0679, Dátum referencie: 24.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

otvorených dátach a opakovanom použití informácií verejného sektora[12], ktorá je ďalším stavebným kameňom európskeho legislatívneho rámca vzťahujúceho sa na dáta.

V prípade informačných systémov, ktoré obsahujú zmiešané dáta, teda osobné údaje aj údaje, ktoré nie sú osobnými údajmi, ktoré nie je možné oddeliť, je nutné riadiť sa spomínaným všeobecným nariadením o ochrane údajov alebo zákonom o ochrane osobných údajov. Európska komisia tiež vydala **informatívne usmernenie** o interakcii medzi spomínanou smernicou o otvorených dátach a všeobecným nariadením o ochrane údajov (resp. zákonom o ochrane osobných údajov), ktoré vyjasňuje, ktoré pravidlá je potrebné dodržiavať pri spracovávaní zmiešaných informačných systémov.

Hlavným cieľom smernice o otvorených dátach je povolenie slobodného opätovného používania dát, ktoré majú k dispozícii orgány a inštitúcie verejného sektora. Dôvodom je podpora nových digitálnych produktov a služieb.

3. Do legislatívneho rámca týkajúceho sa dát môžeme zaradiť aj **legislatívu EÚ, ktorá reguluje zdieľanie dát nepriamo**. Ide o Smernicu Európskeho parlamentu a Rady 9/96/ES o právnej ochrane databáz[13], Smernicu Európskeho parlamentu a Rady (EÚ) 2019/790 o autorskom práve a právach súvisiacich s autorským právom na digitálnom jednotnom trhu[14], Smernicu Európskeho parlamentu a Rady (EÚ) 2016/943 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva)[15], Smernicu Európskeho parlamentu a Rady 2009/24/ES o právnej ochrane počítačových programov (kodifikované znenie)[16] a Smernicu Európskeho parlamentu a Rady 2005/29/ES o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu[17].

4. **Európska dátová stratégia** (European Data Strategy)[18] je takisto spôsobom regulovania dátových transakcií, konkrétne zdieľania dát, ich opätovného používania a ich dostupnosti. V tejto stratégii Európska komisia zdôrazňuje, že rozvoj dátových trhovísk je kľúčový nástroj pre naplnenie celého potenciálu hodnoty dát generovaných naprieč členskými štátmi.

5. Pravidlá pre uľahčovanie opätovného využívania údajov v dispozícii verejného sektora a pre aktivity subjektov zdieľajúcich dáta určuje **nariadenie Európskeho parlamentu a Rady (EÚ) 2022/868 o európskej správe údajov** (Data Governance Act – DGA)[19]. Strategickým cieľom tohto nariadenia je stanovenie podmienok pre rozvoj spoločných

---

[12] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32019L1024, Dátum referencie: 24.04.2023

[13] Zdroj: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=celex:31996L0009, Dátum referencie: 24.04.2023

[14] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32019L0790, Dátum referencie: 24.04.2023

[15] Zdroj: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=celex:32016L0943, Dátum referencie: 24.04.2023

[16] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32009L0024, Dátum referencie: 24.04.2023

[17] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32005L0029, Dátum referencie: 24.04.2023

[18] Zdroj: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_sk, Dátum referencie: 24.04.2023

[19] Zdroj: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32022R0868&from=EN, Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

európskych dátových priestorov a posinenie dôvery v zdieľanie dát a sprostredkovanie dát.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

3 Transformácia údajov v kontexte dôveryhodnosti

Nesprávny a neoveriteľný proces transformácie údajov má zásadný negatívny vplyv na dôveryhodnosť údajov. Preto sa v kontexte štandardizácie dôveryhodných údajov detailnejšie venujeme procesu transformácie, ktorý je ale podrobne štandardizovaný v dokumente 1.1.6 Štandardizácia dátovej transformácie.

3.1 Aktualizácia štandardu pre transformáciu údajov s využitím centrálneho modelu údajov

Koncepcia riešenia integrácie vzájomnej výmeny dát medzi integrovanými systémami je postavená na využívaní služieb poskytovaných IS CSRÚ. IS CSRÚ zabezpečuje prostredie pre elektronickú komunikáciu medzi informačnými systémami v správe rôznych OVM, jednotný prístup k informačným systémom OVM na účely výkonu verejnej moci elektronicky a integráciu údajov, synchronizáciu údajov pri referencovaní a jednotný spôsob poskytovania údajov z informačných systémov v správe OVM.

Jedným z hlavných cieľov transformácie údajov je zvýšenie interoperability medzi systémami verejnej správy, priblíženie sa odporúčaniam a štandardom EÚ pre interoperabilitu verejnej správy a medzi krajinami EÚ a zjednodušenie prístupu k údajom pre prijímateľov. Za týmto účelom napríklad vzniká v rámci projektu CIP transformačný modul IS CSRÚ, ktorý bude zabezpečovať transformáciu dát z aktuálneho XML formátu do RDF formátu v 5★ kvalite prelinkovaných údajov („Linked Data“)[20].

Konzumentami transformovaných údajov budú, rovnako ako v prípade netransformovaných údajov, informačné systémy v správe OVM, ale najmä platforma MOU. V rámci projektu MOU sa počíta s využitím údajov aj na právne záväzné úkony. Preto je fundamentálnou požiadavkou, aby údaje po transformácii mali minimálne rovnakú dôveryhodnosť ako pred transformáciou. Presnejšie, aby procesom transformácie, pri ktorom dochádza k zmene štruktúry, formátu aj objemu pôvodných dát, nedošlo k zníženiu ich dôveryhodnosti.

Špeciálnu úlohu v procese transformácie má Centrálny model údajov (CMÚ). Centrálny model údajov verejnej správy je množina slovníkov (ontológií), ktoré sa používajú pri popise údajov verejnej správy, ako napríklad referenčné registre, centrálne databázy a podobne. Vybudovanie a udržiavanie CMÚ bolo stanovené ako prioritná úloha v rámci stratégie Manažmentu údajov a je súčasťou verejnej politiky digitalizácie verejnej správy na Slovensku od roku 2017. V rámci SR spravuje CMÚ MIRRI. CMÚ je možné chápať ako dátový model kľúčových dátových entít a atribútov v ekosystéme eGovernmentu (dátové entity s vysokým integračným potenciálom pre prijímateľov). Vzniká tým priestor na unifikáciu slovníka a spôsobu popisu jednotlivých údajov. Jednotlivé časti boli preto štandardizované (vo vyhláške Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021[21] Z. z., ktorou sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020

[20] Zdroj: https://5stardata.info/en/, Dátum referencie: 08.03.2023

[21] Zdroj: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/546/vyhlasene_znenie.html , Dátum referencie: 24.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Z. z. o štandardoch pre informačné technológie verejnej správy). Podrobne sa CMÚ tiež venuje dokument 1.1.2 Štandardizácia pre modelovanie údajov.

V procese transformácie sa predpokladá aj obohatenie a doplnenie pôvodných údajov tak, aby spĺňali požiadavku na kvalitu výstupu na úrovni 5★ RDF.

Pre zachovanie dôveryhodnosti údajov v procese transformácie je potrebné zabezpečiť:

1. Do výsledného transformovaného datasetu sa musia dostať všetky údaje z pôvodného datasetu. Nedôjde tak k strate informácií oproti pôvodným údajom.
2. Transformácia zohľadňuje a aplikuje štandardy pre modelovanie údajov, popísaných v dokumente 1.1.2 Štandardizácia pre modelovanie údajov UP, najmä kapitola 2.3 Modelovanie údajov vo verejnej správe na Slovensku, z toho predovšetkým (ale nie len) využívanie CMÚ a dodržiavanie pravidiel pre jednotné referencovateľné identifikátory (URI).
3. Proces transformácie sa ďalej vykonáva pomocou štandardov, metodík a nástrojov definovaných v dokumente 1.1.6 Štandardizácia dátovej transformácie, pričom na výsledný RDF dataset sa aplikujú aj „proofs“ podľa bezpečnostného stacku (Obrázok 5) popísaného v kapitole 4.2.1.
4. Pri obohacovaní sa vychádza výlučne z informácií obsiahnutých v pôvodných údajoch a informácií CMÚ. Je možné aplikovať biznis pravidlá, ktoré zabezpečia zlepšenie kvality údajov, ich výsledok však musí byť jednoznačný. Pri nejednoznačnom výsledku transformácie údaju sa údaj nesmie transformovať. Príkladom jednoznačnej transformácie s obohatením je zmena pôvodného údaju pohlavia fyzickej osoby v podobe „M“ (ako muž) na číselníkovú hodnotu CMÚ základného číselníka Pohlavie aj s definovanou URI https://data.gov.sk/def/sex/1 a prípadne s doplňujúcim údajom preferovaného pomenovania „Muž“ a referenciou na daný číselník https://data.gov.sk/set/codelist/CL003003.

   Príkladom nejednoznačnej transformácie môže byť určenie adresného bodu z Centrálneho registra adries (jednoznačného identifikátora adresného bodu) na základe pôvodného neúplného údaju adresy v neštruktúrovanej forme “Čakanovce 79”, kedy nie je možné rozhodnúť, o ktorú obec sa presne jedná, nakoľko sa ich na Slovensku nachádza viacero. Vtedy sa do transformovaných údajov má dostať iba pôvodný údaj adresy, nie však identifikátor adresného bodu.
5. Dôveryhodnosť samotného prostredia vykonávajúceho transformáciu - z tohoto pohľadu za dôveryhodné považujeme samotné zdrojové IS VS v správe OVM a IS CSRÚ / CIP.

Pre zachovanie dôveryhodnosti údajov vo vzťahu k CMÚ je potrebné navyše zabezpečiť správnosť a aktuálnosť použitých údajov CMÚ v procese samotnej transformácie. Toto je ideálne zabezpečiť priamou aplikačnou integráciou, napríklad s portálom znalosti.gov.sk alebo metais2.vicepremier.gov.sk na úrovni API, prípadne pravidelnou aktualizáciou týchto údajov v lokálnych úložiskách modulov transformácie, a zamedziť tak použitiu neaktuálnych alebo neplatných údajov v procese transformácie. Pri aktualizáciách CMÚ je tiež nevyhnutné myslieť na spätnú kompatibilitu a interoperabilitu transformovaných údajov.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

3.2 Návrh metód dátovej transformácie

V rámci štandardizácií W3C sa určujú odporúčania, ako transformovať údaje z formátu XML (prípadne CSV, JSON a pod.) do RDF. Pre zachovanie dôveryhodnosti transformovaných údajov odporúčame:

1. Vhodným spôsobom využiť práve tieto odporúčania v kombinácii s centrálnym dátovým katalógom a CMÚ.
2. Transformačný modul umiestniť:
   a) Buď priamo na zdrojový systém pod správou OVM – preferovaná no technicky a časovo náročná alternatíva – dôveryhodnosť údajov vtedy garantuje samotný zdrojový systém rovnako, ako v prípade pôvodných údajov.
   b) Alebo ako modul IS CSRÚ / CIP – technicky aj časovo ľahšie realizovateľná alternatíva – dôveryhodnosť údajov garantuje zdrojový systém pôvodných údajov v kombinácii s IS CSRÚ / CIP, kde garantom je prevádzkovateľ systému – MIRRI.

Podrobnejšie sa štandardu transformácie venuje dokument 1.1.6 Štandardizácia dátovej transformácie.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

4 Výber vhodných metód pre jednotlivé prípady použitia

4.1 Metódy pre zabezpečenie dôveryhodných údajov

4.1.1 Elektronické (digitálne) podpisovanie

Pojmy „elektronický podpis“ a „digitálny podpis“ sa často používajú zameniteľne, ale ide o veľmi odlišné pojmy, keďže „elektronický podpis“ je právny pojem, zatiaľ čo „digitálny podpis“ je technický pojem, ktorý sa používa na poskytnutie konkrétnej inštancie elektronického podpisu.

Nariadenie eIDAS definuje elektronické podpisy ako údaje v elektronickej forme, ktoré používa signatár na podpis a sú spojené s inými elektronickými údajmi alebo k nim pripojené. Existujú rôzne kategórie elektronických podpisov, pričom jednoduché elektronické podpisy (*Simple Electronic Signature*, SES) sú základnou formou a Kvalifikované elektronické podpisy (*Qualified Electronic Signature,* QES) sú najbezpečnejšie. SES je napríklad podpis na konci e-mailu, zatiaľ čo zdokonalené elektronické podpisy (*Advanced Electronic Signature,* AdES) majú vlastnosti, že sú jedinečne prepojené, dokážu identifikovať signatára a dokážu zistiť zmeny vykonané v údajoch od podpisu. QES sú založené na zaručených certifikátoch a majú rovnakú právnu hodnotu ako vlastnoručné podpisy. QES je AdES s pridaním kvalifikovaného certifikátu.

Digitálny podpis je technický koncept, ktorý je založený na infraštruktúre verejného kľúča a zahŕňa okrem iného kryptografiu s verejným kľúčom a certifikáty verejného kľúča. Digitálne podpisy možno použiť na zabezpečenie jedinečnej identifikácie podpisovateľa, pravosti podpisu a integrity údajov. Identifikácia podpisovateľa, ako aj pravosť podpisu sú zaručené dešifrovaním hodnoty digitálneho podpisu pomocou verejného kľúča potvrdeného certifikátom verejného kľúča. Komponentom digitálneho podpisu, ktorý umožňuje zistiť, či sa s podpísanými údajmi nemanipulovalo, je kryptografická funkcia nazývaná hašovacia funkcia.

4.1.1.1 PKI infraštruktúra

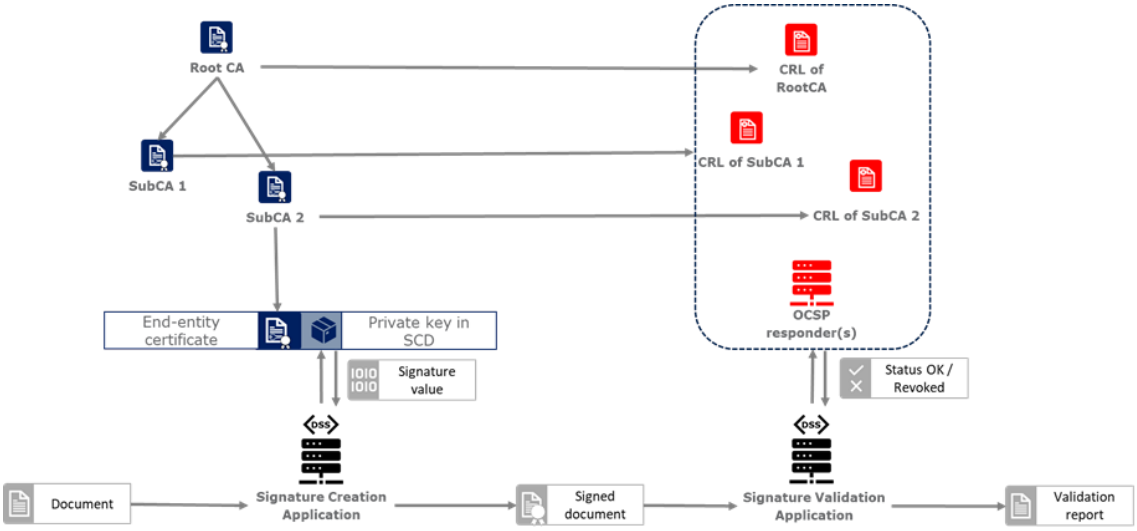
PKI (Public Key Infrastructure) je infraštruktúra kryptografických protokolov, algoritmov a procesov, ktoré sa používajú na vytváranie, správu a distribúciu digitálnych certifikátov a párov verejných a súkromných kľúčov. Je neoddeliteľnou súčasťou každej bezpečnej digitálnej komunikácie, ktorá umožňuje autentifikáciu a šifrovanie informácií vymieňaných cez internet. Využíva asymetrické šifrovanie pre bezpečnosť a ochranu údajov, ktorému sa venujeme v dokumente 1.1.3 Štandardizácia pre bezpečnosť a ochranu údajov a v dokumente 1.1.5 Štandardizácia anonymizácie údajov. Hlavnou výhodou používania šifrovania s verejným kľúčom je robustnejšie zabezpečenie údajov. Keďže používatelia nemusia nikomu zdieľať, prenášať ani prezrádzať svoje súkromné kľúče, znižuje sa riziko, že útočník zachytí súkromný kľúč a zneužije ho na dešifrovanie komunikácie. Pomáha teda riešiť problémy s distribúciou kľúčov, ktoré nastávajú pri symetrickom šifrovaní s využitím súkromných kľúčov.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

PKI infraštruktúra umožňuje organizáciám zachovať dôvernosť a integritu údajov aj vďaka digitálnemu certifikátu - dokumentu, ktorý obsahuje informácie o identite používateľa a je digitálne podpísaný certifikačnou autoritou (CA). CA je dôveryhodná organizácia tretej strany, ktorá je zodpovedná za overenie identity používateľa a vydávanie digitálnych certifikátov. Infraštruktúra PKI je základnou súčasťou zabezpečenej komunikácie a používa sa v aplikáciách, ako sú zabezpečený e-mail, bezpečné prehliadanie webu, bezpečný prenos súborov, elektronický podpis, elektronická pečať a zabezpečené pripojenia VPN. Ďalšie príklady infraštruktúry PKI zahŕňajú digitálne certifikačné autority, ako je VeriSign, a šifrovacie protokoly, ako napríklad Secure Socket Layer a Transport Layer Security.



Obrázok 3: Zjednodušený model PKI[22]

V tomto zjednodušenom modeli sa PKI skladá z:

- Digitálnych certifikátov X.509;
- Certifikačných autorít (CA), ktoré vydávajú certifikáty;
- Zoznamov odvolaných certifikátov (CRL) vydaných CA; a
- Respondentov v protokole online stavu certifikátov („Online Certificate Status Protocol (OCSP)“), ktorý používajú certifikačné autority na kontrolu stavu odvolania digitálneho certifikátu: Keď používateľ žiada o overenie platnosti certifikátu, žiadosť OCSP sa odošle odpovedajúcemu serveru OCSP. Ten overí konkrétny certifikát u dôveryhodnej certifikačnej autority a naspäť sa odošle odpoveď OCSP s odpoveďou "dobrý", "zrušený" alebo "neznámy".

4.1.1.2 *Kvalifikovaný elektronický podpis*

Kvalifikovaný elektronický podpis, alebo QES (*Qualified Electronic Signature*), je typ digitálneho podpisu, ktorý spĺňa štandardy elektronickej identifikácie a dôveryhodných

[22] Zdroj: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html#PKI, Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

služieb. Poskytuje bezpečný proces autentifikácie, ktorý zaisťuje overenie identity podpisovateľa a bezpečnosť dokumentu. Je právne uznaný v Európskej únii a ďalších krajinách, ktoré prijali nariadenie eIDAS. QES sa používa na overovanie dokumentov, transakcií a digitálnych identít. Poskytuje vyššiu úroveň bezpečnosti ako bežné digitálne podpisy, pretože je založený na dvojfaktorovej autentifikácii, čo znamená, že podpisujúci musí vlastniť fyzické zariadenie (napríklad čipovú kartu alebo token), aby mohol dokument podpísať.

Aplikácie pre kvalifikovaný elektronický podpis môžu byť na Slovensku použité na vytváranie a spracovanie elektronického podpisu, ktorý slúži na autorizáciu elektronických podaní a elektronických úradných dokumentov podľa zákona č. 305/2013 Z.z. o e-Governmente a v súlade s nariadením o elektronickej identifikácii a dôveryhodných službách. Aplikácie určené na vytváranie QES sú v zhode a spĺňajú relevantné bezpečnostné, funkčné a obsahové požiadavky na aplikácie pre vytváranie elektronického podpisu, ktoré sa nachádzajú v dokumente CEN CWA 14170, v zákone č. 272/2016 Z. z. o dôveryhodných službách a príslušných vyhláškach NBÚ SR pre oblasť kvalifikovaného elektronického podpisu. V zmysle platnej Slovenskej legislatívy fyzické osoby vytvárajú:

- **elektronický podpis** (SES) – predstavuje najnižšiu a najmenej dôveryhodnú úroveň elektronického podpisu;
- **zdokonalený elektronický podpis** (AdES) – je obdobou staršieho "elektronického podpisu“ a môže sa vytvárať pomocou certifikátu pre elektronický podpis vydaného poskytovateľom dôveryhodných služieb;
- **kvalifikovaný elektronický podpis** (QES) – je obdobou staršieho "zaručeného elektronického podpisu" a je ekvivalentom vlastnoručného podpisu. Vytvára sa pomocou kvalifikovaného certifikátu pre elektronický podpis vydaného kvalifikovaným poskytovateľom dôveryhodných služieb.

4.1.1.3 Elektronická pečať

Právnické osoby vytvárajú v zmysle platnej Slovenskej legislatívy:

- **elektronickú pečať** – predstavuje najnižšiu a najmenej dôveryhodnú úroveň elektronickej pečate;
- **zdokonalenú elektronickú pečať** – je obdobou staršej "elektronickej pečate" a môže sa vytvárať pomocou certifikátu pre elektronickú pečať vydaného poskytovateľom dôveryhodných služieb;
- **kvalifikovanú elektronickú pečať** – je obdobou staršej "zaručenej elektronickej pečate" a zabezpečuje iba integritu a originalitu elektronického dokumentu. Vytvára sa pomocou kvalifikovaného certifikátu pre elektronickú pečať vydaného kvalifikovaným poskytovateľom dôveryhodných služieb a pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate (napr. čipovej karty).

4.1.1.4 Digital Signature Service

Služba digitálneho podpisu (Digital Signature Service, DSS) je projekt financovaný EÚ, ktorého cieľom je vytvoriť rámec elektronického podpisu na používanie elektronických dokumentov v Európe. Cieľom projektu je vytvoriť jednotný, bezpečný a interoperabilný európsky rámec pre digitálny podpis. Tento rámec umožní interoperabilitu rôznych

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

technológií elektronického podpisu a používanie kvalifikovaných elektronických podpisov na bezpečné digitálne transakcie. Projekt DSS je výsledkom spolupráce medzi Európskou komisiou, Európskym inštitútom pre telekomunikačné normy a Európskou agentúrou pre bezpečnosť sietí a informácií.

Projekt Digital Signature Service je projekt navrhnutý tak, aby umožnil bezpečnejšie, efektívnejšie a nákladovo efektívnejšie procesy a služby digitálneho podpisu. Jeho primárnym cieľom je poskytovať bezpečnú a spoľahlivú službu digitálneho podpisu, ktorú možno použiť na overenie pravosti digitálnych dokumentov, ochranu integrity týchto dokumentov a zabezpečenie bezpečnej výmeny informácií. Okrem toho sa projekt zameriava na to, aby sa digitálne podpisy ľahšie používali, boli prístupnejšie a nákladovo efektívnejšie. Cieľom projektu je tiež zlepšiť celkovú bezpečnosť digitálnych dokumentov poskytnutím lepších mechanizmov autentifikácie a šifrovania. Snaží sa tiež znížiť náklady na digitálne podpisy poskytovaním nástrojov, ktoré umožňujú automatizované vytváranie, overovanie a ukladanie digitálnych podpisov.

DSS vytvoril súbor algoritmov a protokolov, ktoré používajú kryptografiu s verejným kľúčom na vytváranie digitálnych podpisov pre digitálne dokumenty, overovanie platnosti a integrity týchto podpisov a bezpečnú výmenu digitálnych certifikátov. DSS sa široko používa v mnohých odvetviach a aplikáciách vrátane finančných služieb, štátnej správy, zdravotníctva a ďalších.

4.2 Metódy pre zabezpečenie overiteľných údajov v online ekosystéme so zapojením tretích strán

4.2.1 Verifiable Credentials

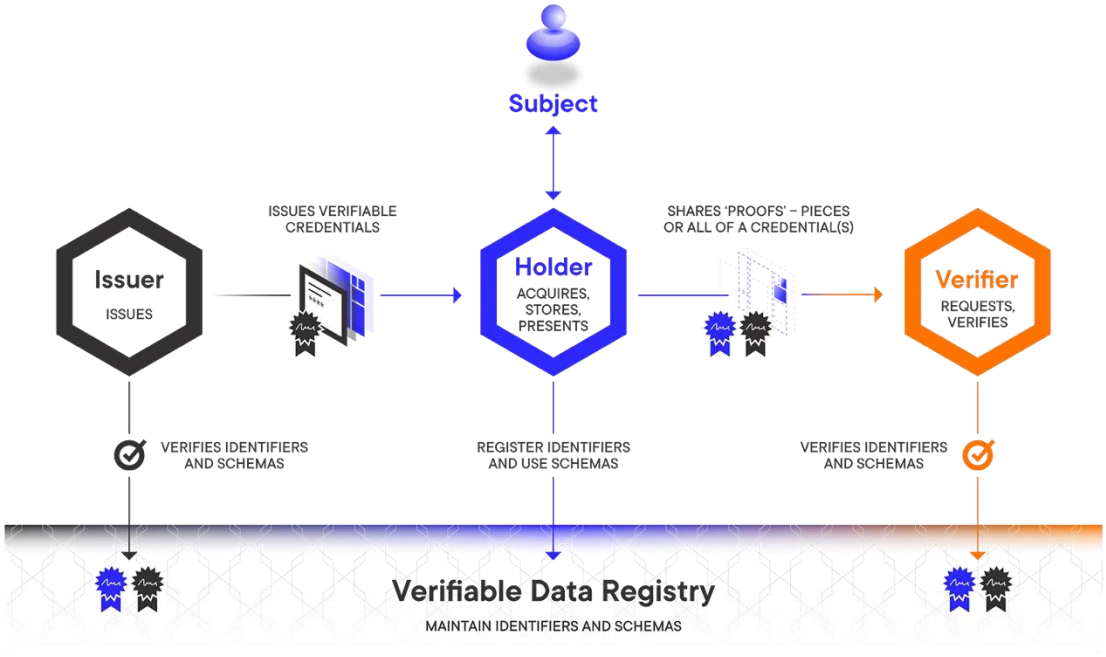
Verifiable Credentials („Overiteľné poverenia“) tvoria základ implementácie overiteľných údajov v online ekosystéme, kedy sa prijímateľ potrebuje dostať k overiteľným údajom o dotknutej osobe alebo subjekte vydaným nejakou autoritou. Možno si ich predstaviť ako kontajner pre mnoho rôznych typov informácií, ako aj pre rôzne typy poverení. Keďže ide o otvorený štandard W3C, Verifiable Credentials môžu implementovať mnohí poskytovatelia softvéru, organizácie, štátne a verejné správy a podniky.

Vydavateľ alebo autorita („Issuer“), ktorá disponuje určitými informáciami o dotknutej osobe alebo inom subjekte, vydáva držiteľovi („Holder“) poverenie obsahujúce tieto informácie vo forme nárokov alebo tvrdení. Držiteľ je zodpovedný za uchovávanie a správu tohto poverenia a vo väčšine prípadov je to softvér, ktorý koná v mene dotknutej osoby alebo subjektu, napríklad digitálna peňaženka alebo úložisko osobných údajov či systém na správu osobných informácií („Personal Information Management Systems (PIMS)“). Keď overovateľ (Verifier), niekedy označovaný ako prijímateľ alebo tretia strana, potrebuje overiť nejaké informácie, môže si od držiteľa vyžiadať určité údaje, aby splnil svoje požiadavky na overenie. V závislosti od možností základnej technológie môže držiteľ voľne prezentovať nároky alebo tvrdenia obsiahnuté vo svojich Verifiable Credentials pomocou ľubovoľného počtu techník slúžiacich na zachovanie svojho súkromia. Tento celý ekosystém znázorňuje Obrázok 4.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.



Obrázok 4: Ilustrácia kľúčových úloh v ekosystéme s Verifiable Credentials[23]

Mechanizmy vo Verifiable Credentials umožňujú aj prepojenie overiteľných údajov s inými druhmi údajov s cieľom ich ľahšieho pochopenia v kontexte vzťahov a procesov. To sa dá dosiahnuť použitím dátových schém alebo dátových slovníkov. Schémy sú súborom typov a vlastností, ktoré sa používajú na opis údajov. V kontexte zdieľania údajov sú schémy neuveriteľne užitočným a potrebným nástrojom na presné reprezentovanie údajov od momentu ich vytvorenia až po zdieľanie a overovanie. Dátové schémy v ekosystéme Verifiable Credentials sú v podstate užitočné len vtedy, ak ich vo veľkej miere opakovane používa mnoho rôznych strán. Ak sa každý implementátor Verifiable Credentials rozhodne opísať a reprezentovať údaje trochu iným spôsobom, vytvára to nesúlad a nekonzistentnosť údajov a hrozí, že sa zníži potenciál všadeprítomného prijatia otvorených štandardov a schém.

Verifiable Credentials využívajú štandard JSON-LD na rozšírenie dátového modelu na podporu dynamických dátových slovníkov a schém. To umožňuje nielen používať existujúce schémy JSON-LD, ale aj využívať mechanizmus definovaný JSON-LD na vytváranie a zdieľanie nových schém. Tento štandard podporuje aj spomínaný CMÚ v ekosystéme slovenského eGovernmentu (viac v dokumente 1.1.2 Štandardizácia pre modelovanie údajov).

Linked Data Proofs, implementované aj v rámci MOU a nedávno premenované na „Linked Data Integrity“ (dátová integrita)[24], definujú možnosť overovania pravosti a integrity datasetov prelinkovaných údajov („Linked Data“) pomocou matematických dôkazov a asymetrickej kryptografie. Poskytujú jednoduchý bezpečnostný protokol, ktorý

[23] Zdroj: https://medium.com/mattr-global/a-solution-for-privacy-preserving-verifiable-credentials-f1650aa16093, Dátum referencie: 31.03.2023

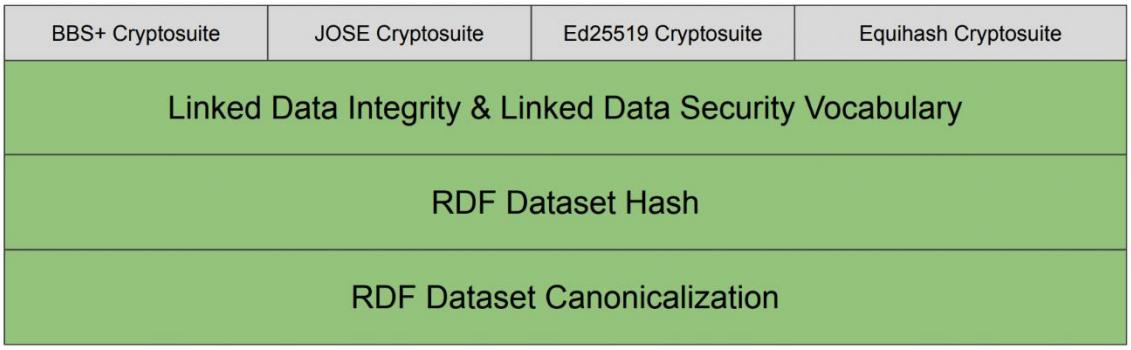
[24] Zdroj: https://w3c.github.io/vc-data-integrity/, Dátum referencie: 28.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

je natívny pre JSON-LD. Vzhľadom na povahu prepojených údajov sú tieto „proofs“ vytvorené tak, aby kompaktne reprezentovali reťazce dôkazov a umožňovali jednoduchú ochranu overiteľného poverenia na podrobnejšom základe - skôr na základe jednotlivých atribútov ako na základe jednotlivých poverení.

Tento mechanizmus sa stáva obzvlášť užitočným pri vyhodnocovaní reťazca dôveryhodných poverení patriacich organizáciám a jednotlivcom. Reťaz dôkazov („proof chain“) sa používa vtedy, keď tie isté údaje musia byť podpísané viacerými subjektmi a záleží na poradí, v akom boli dôkazy vygenerované. Ak je potrebné zachovať poradie, reťaz dôkazov sa reprezentuje zahrnutím usporiadaného zoznamu dôkazov s kľúčom pre reťaz dôkazov do Verifiable Credentials.

Verifiable Credentials vo formáte JSON-LD sú vybudované nad celým bezpečnostným stackom pre prepojené údaje (Obrázok 5).



Obrázok 5: Bezpečnostný stack pre prepojené údaje (Linked Data Security Stack)[25]

RDF Dataset Canonicalization (Kanonizácia RDF datasetu) transformuje dátový vstup v štandarde RDF na deterministický výstup, ktorý je užitočný napríklad pre digitálne podpisy. Táto kanonická podoba v N-Quads[26] serializácii sa zoradí pre správnu aplikáciu kryptografickej hašovacej funkcie. Linked Data Integrity predstavuje rámec pre definovanie dôkazov („proofs“) na zabezpečenie integrity pre RDF datasety v podobe RDF grafov. Používa sa na vyjadrenie rôznych typov digitálnych dôkazov, ako napríklad:

- “Proof of Work”,
- Dôkaz existencie,
- Dôkaz uplynutého času,
- Digitálne podpisy (“Linked Data Signatures”).

Linked Data Security Vocabulary definuje pojmy používané v štandarde Linked Data Integrity. Definuje aj JSON-LD kontext, ktorý sa používa pri serializácii RDF do JSON-LD. “Cryptosuites” prepojených údajov poskytujú schválené / vopred pripravené

[25] Zdroj: https://lists.w3.org/Archives/Public/public-credentials/2021May/att-0082/2021-Linked-Data-Security-WG-Charter.pdf, Dátum referencie: 31.03.2023

[26] Zdroj: https://www.w3.org/TR/n-quads/, Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

kryptografické knižnice, ktoré zvyčajne zlučujú algoritmus kanonizácie, hašovací algoritmus a podpisový algoritmus. Definujú formát verejného kľúča a formát podpisu.

4.2.2 Verifiable Presentation

Overiteľná prezentácia („Verifiable Presentation“)[27] vyjadruje údaje z jedného alebo viacerých Verifiable Credentials a je zabalená takým spôsobom, aby bolo možné overiť autorstvo údajov. Ak sa Verifiable Credentials prezentujú priamo, stávajú sa overiteľnými prezentáciami. Formáty údajov odvodené z Verifiable Credentials, ktoré sú kryptograficky overiteľné, ale samy o sebe neobsahujú overiteľné poverenia, môžu byť tiež overiteľnými prezentáciami.

Údaje vo Verifiable Presentation sa často týkajú tej istej dotknutej osoby alebo subjektu, ale mohli ich vydať viacerí vydavatelia. Súhrn týchto informácií zvyčajne vyjadruje nejaký aspekt dotknutej osoby, organizácie alebo iného subjektu.

Proces zdieľania overiteľných údajov pomocou Verifiable Credentials pozostáva z nasledovných krokov:

1 Vydanie jedného alebo viacerých Verifiable Credentials.
2 Uloženie Verifiable Credentials v úložisku poverení (napríklad v digitálnej peňaženke alebo v osobnom úložisku či v PIMS).
3 Zloženie viacerých Verifiable Credentials do overiteľnej prezentácie (Verifiable Presentation) pre overovateľov.
4 Overenie overiteľnej prezentácie (Verifiable Presentation) overovateľom.

4.2.3 Selektívne zverejňovanie („Selective disclosure“)

Jednou z dôležitých zásad v súlade s GDPR, ktorú chceme dosiahnuť pri navrhovaní akéhokoľvek systému, ktorý zahŕňa spracovanie osobných údajov, je minimalizovať množstvo údajov zverejnených pri danej interakcii zúčastnených strán. Keď používatelia zdieľajú informácie, mali by mať možnosť vybrať si, v akom rozsahu ich zdieľajú v jednotlivých prípadoch použitia – táto možnosť sa často označuje ako selektívne zverejňovanie („selective disclosure“). Aj pri selektívnom zverejňovaní majú mať prijímatelia istotu o pôvode a integrite predložených informácií. Pokiaľ ide o riešenia, existuje mnoho rôznych spôsobov, ako tento problém adresovať, pričom pre tento štandard odporúčame aplikovať nasledujúce:

1 Vydávanie informácií v okamihu potreby („**just in time issuance**“) – vtedy sa kontaktuje vydavateľ v čase žiadosti buď priamo, alebo nepriamo, aby poskytol so súhlasom držiteľa overovateľovi – prijímateľovi - na mieru šité tvrdenie obsahujúce len informácie, ktoré požaduje tento prijímateľ.
2 Vydavateľ (autorita) vytvorí takzvané „**atomické“ tvrdenia („atomické datasety“)**, ktoré uloží u držiteľa a z ktorých možno vyskladať výsledný dataset s informáciami, ktoré požaduje prijímateľ (tento prístup v súčasnosti implementuje platforma MOU pre Manažment osobných údajov).

[27] Zdroj: https://www.w3.org/TR/vc-data-model/#presentations, Dátum referencie: 28.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

3. **Kryptografické riešenia** - Použitie kryptografickej techniky na zverejnenie podmnožiny informácií z väčšieho tvrdenia (datasetu).

Hoci je každé riešenie vhodné v rôznych prípadoch použitia, tieto prístupy majú niektoré zásadné kompromisy. Model pre „just in time issuance“ spopularizoval OpenID Connect[28] (MOU tiež využíva štandard OpenID Connect ako implementáciu Oauth 2.0[29] na autorizáciu používateľov). Tento model predpokladá, že vydavateľ je vysoko dostupný, čo pre vydavateľa znamená záťaž infraštruktúry, ktorá je úmerná počtu dotknutých osôb a ďalších subjektov, pre ktoré má informácie, a tomu, kde tieto dotknuté osoby a ďalšie subjekty používajú svoje informácie. Okrem toho sa vo väčšine prípadov tohto modelu vydavateľ dozvie, kde dotknutá osoba alebo iný subjekt používa svoje osobné údaje a citlivé informácie, čo môže predstavovať vážny problém v oblasti ochrany súkromia.

Model atomických datasetov rieši problém s vysokou dostupnosťou vydavateľa tým, že tieto atomické, ďalej nedeliteľné tvrdenia sú vystavené držiteľovi vopred. Rieši aj problém s narušením súkromia modelu „just in time issuance“. Avšak nevýhodou tohto modelu je duplikovanie informácií a veľký počet možných atomických datasetov pre rozsiahle datasety. Alternatívou tohto prístupu je „Selective Disclosure“ pre JWTs (SD-JWT)[30]. Pre každé tvrdenie, ktoré sa má selektívne zverejniť, vydavateľ vytvorí poverenie („disclosure“), zahašuje ho a zahrnie haš namiesto pôvodného tvrdenia do SD-JWT, ako je detailne popísané tu. Poverenia sa potom zašlú držiteľovi.

Kryptografické riešenia ponúkajú alternatívu k týmto dvom modelom tým, že riešia problém selektívneho zverejňovania priamo na základnej vrstve dátového modelu Verifiable Credentials, čím poskytujú jednoduchšiu a flexibilnejšiu metódu zachovania súkromia používateľa. Na dosiahnutie selektívneho zverejnenia alebo minimalizácie údajov možno kryptografiu použiť rôznymi spôsobmi, ale asi najpopulárnejším prístupom je použitie odvetvia kryptografie známeho ako Zero-Knowledge Proofs alebo ZKP. Výnimočnou vlastnosťou tejto technológie je, že držiteľ môže dokázať niektoré tvrdenia v údajoch bez toho, aby odhalil akékoľvek ďalšie údaje. ZKP umožňujú používateľovi dynamicky generovať ľubovoľný počet tvrdení - dôkazov, ktoré minimálne odhaľujú informácie s cieľom uspokojiť požiadavky na prezentáciu poverenia. Na rozdiel od jednoduchších prístupov VC, pri používaní VC s podporou ZKP pôvodné poverenie takmer nikdy neopustí peňaženku alebo osobné úložisko držiteľa. Časť informácií, ktorá sa zverejňuje externým stranám, je prezentácia poverenia, ktorá sa dynamicky generuje podľa potreby, a nie samotné poverenie. Problémom tohto modelu je však to, že štandardy ešte nie sú ustálené a rôzne riešenia vytvárajú nové závislosti od infraštruktúry, ako aj zvýšenie nárokov na výpočtové kapacity potrebné na ich implementáciu. ZKP, ktoré sa používajú v kontexte Verifiable Credentials, môžu a mali by byť implementované v jednom z dvoch existujúcich formátov tvrdení, ktoré sú dnes definované na použitie v rámci štandardu, a to JSON-LD[31] a JWT[32].

---

[28] Zdroj: https://openid.net/connect/, Dátum referencie: 28.03.2023

[29] Zdroj: https://oauth.net/2/, Dátum referencie: 28.03.2023

[30] Zdroj: https://github.com/oauth-wg/oauth-selective-disclosure-jwt, Dátum referencie: 31.03.2023

[31] Zdroj: https://json-ld.org/, Dátum referencie: 28.03.2023

[32] Zdroj: https://jwt.io/introduction/, Dátum referencie: 28.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Je síce pravda, že JWT možno použiť s JSON-LD na dosiahnutie niektorých funkcií modelovania otvoreného sveta údajov, vďaka ktorým je JSON-LD taký užitočný, ale tento prístup trpí tým, že nepodporuje bezpečnostné funkcie, ktoré ponúkajú Linked Data Proofs (Obrázok 5). Na pridanie ochrany do JWT je potrebné vykonať ďalšie predbežné a následné spracovanie údajov. Naproti tomu ochrana VC založeného na JSON-LD je taká jednoduchá ako odovzdanie platného VC implementácii Linked Data Signatures a vygenerovanie digitálneho podpisu. Podrobné zhodnotenie týchto prístupov možno nájsť v tejto tabuľke. Jedným zo sľubne sa vyvíjajúcich štandardov pre ZKP vo VC je BBS Signature Scheme[33]. Alternatívne možno implementovať algoritmus na vytvorenie merkle stromu[34] z kanonizovaného súboru N-Quads[35] a potom podpísať root hash.

4.3 Dôveryhodnosť údajov v platforme MOU[36]

Manažment osobných údajov (MOU) je možné považovať za dôležitý nástroj pre dôveryhodné zdieľanie údajov, ktoré o používateľovi (dotknutej osobe či subjekte) evidujú inštitúcie verejnej správy. V tejto časti je vysvetlené, akým spôsobom sú v rámci MOU implementované požiadavky na ochranu údajov, požiadavky na kybernetickú bezpečnosť a ako sa zabezpečuje dôveryhodnosť a overiteľnosť údajov. Základnými otázkami, ktoré bolo potrebné rozhodnúť, sú:

- Bezpečná autentifikácia používateľa.
- Ukladanie a ochrana osobných údajov v MOU.
- PKI a uloženie privátneho kľúča.
- Autorizácia osobných údajov.
- Zdieľanie overiteľných údajov.

V nasledujúcej časti sú popísané základné scenáre zdieľania dôveryhodných údajov v MOU. Na obrázkoch (Obrázok 6, Obrázok 7 a Obrázok 8) sú vždy výrazne viditeľné tie moduly MOU, ktoré sa v danom scenári zapájajú.

Súvisiace zdroje

- Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správy osobných údajov – fáza 1
- Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správy osobných údajov - fáza 2
- Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1
- Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 2

---

[33] Zdroj: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html, Dátum referencie: 31.03.2023

[34] Zdroj: https://iden3-docs.readthedocs.io/en/latest/iden3_repos/research/publications/zkproof-standards-workshop-2/merkle-tree/merkle-tree.html, Dátum referencie: 31.03.2023

[35] Zdroj: https://www.w3.org/TR/n-quads/, Dátum referencie: 31.03.2023

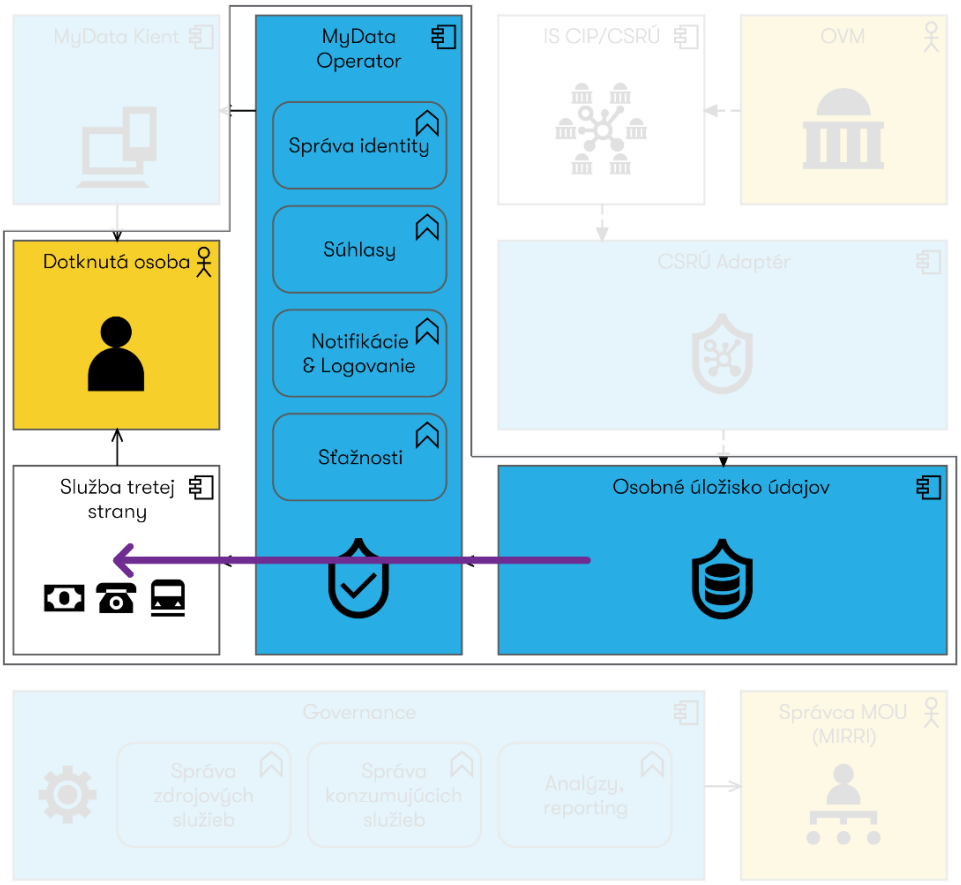
[36] Zdroj: https://datalab.digital/cip-a-mou/manazment-osobnych-udajov/, Dátum referencie: 24.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Poskytnutie dát Službe tretej strany z Osobného úložiska



Obrázok 6: Poskytnutie dát Službe tretej strany z Osobného úložiska v MOU[37]

Predpoklady:

- Zaregistrovaná služba MOU na prenos konkrétneho datasetu z Osobného úložiska Službe tretej strany.
- Vlastník účtu si pripojil túto službu.
- Vlastník účtu zadal súhlas pre túto službu na prenos a spracovanie dát z osobného úložiska Službou tretej strany.
- Implementácia súhlasu zabezpečí, že do procesu zadávania súhlasu (vlastník je prihlásený v MOU) sú zaradené aj kroky:
    - výber požadovaného datasetu z osobného úložiska a jeho rozšifrovanie krypto materiálom vlastníka,
    - zašifrovanie požadovaného datasetu krypto materiálom Tretej strany a uloženie do osobného úložiska.

[37] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

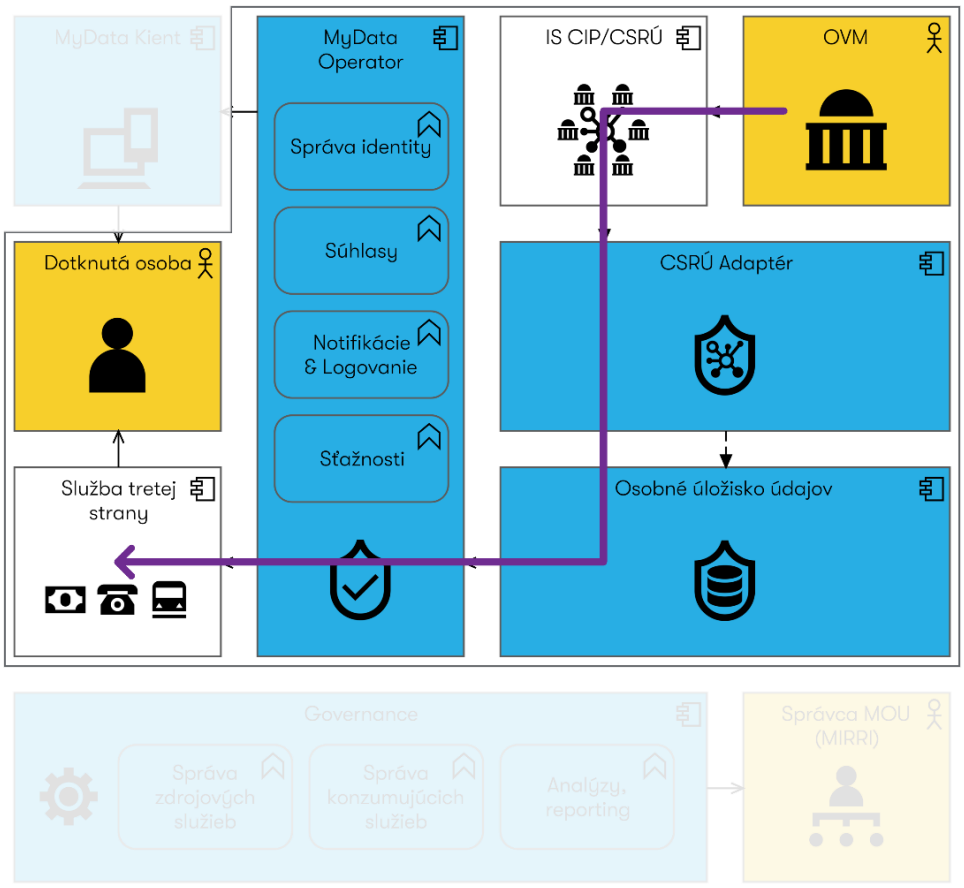
Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Kroky prenosu:

1. Komponent MyData Operátor prečíta požadované dáta, ktoré sú zašifrované pre prijímateľa - tretiu stranu.
2. Dáta sú poskytnuté Službe tretej strany cez príslušné API MOU.
3. Služba tretej strany overí kvalifikovanú elektronickú pečať MIRRI a dešifruje dáta použitím svojho krypto materiálu, spracuje dáta a prípadne poskytne vhodný výstup občanovi alebo podnikateľovi.

Poskytnutie dát Službe tretej strany cez Osobné úložisko



Obrázok 7: Poskytnutie dát Službe tretej strany cez Osobné úložisko v MOU[38]

Predpoklady:

- Zaregistrovaná služba MOU na prenos konkrétneho datasetu do Osobného úložiska a z Osobného úložiska Službe tretej strany.
- Vlastník účtu si pripojil túto službu.

[38] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

- Vlastník účtu zadal súhlas pre túto službu na prenos dát do osobného úložiska a súhlas na prenos a spracovanie dát z osobného úložiska Službou tretej strany.

Kroky prenosu:

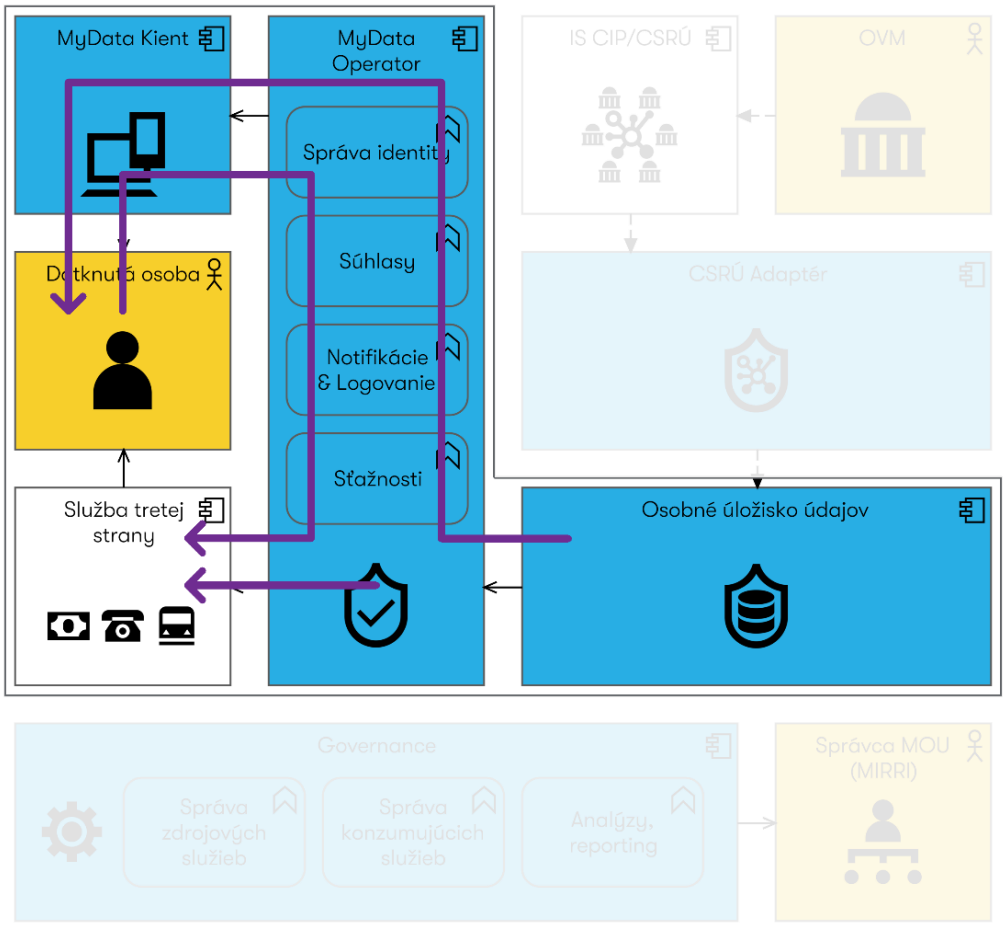
1. IS CIP/CSRÚ prenesie požadované dáta z OVM. Dáta sú prenášané pod identitou MOU/MIRRI (záujmová osoba je MIRRI).
2. CSRÚ Adaptér transformuje údaje do požadovanej formy.
3. Dáta sú podpísané kvalifikovanou elektronickou pečaťou MIRRI, zašifrované s použitím krypto materiálu Služby tretej strany a uložené do Osobného úložiska.
4. Dáta sú zašifrované aj krypto materiálom Vlastníka účtu a uložené do Osobného úložiska.
5. Komponent MyData Operátor prečíta požadované dáta (tie, ktoré sú zašifrované pre prijímateľa - tretiu stranu) z osobného úložiska.
6. Dáta sú poskytnuté Službe tretej strany cez príslušné API MOU.
7. Služba tretej strany overí kvalifikovanú elektronickú pečať MIRRI a dešifruje dáta použitím svojho krypto materiálu, spracuje dáta a prípadne poskytne vhodný výstup občanovi alebo podnikateľovi.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Ad-hoc poskytnutie dát z Osobného úložiska Službe tretej strany



Obrázok 8: Ad-hoc poskytnutie dát z Osobného úložiska Službe tretej strany v MOU[39]

Predpoklady:

- Zaregistrovaná služba MOU na prenos konkrétneho datasetu z Osobného úložiska Službe tretej strany (služba overovateľa),
- Služba tretej strany propaguje/informuje o svojej službe vo svojom front-ende (napríklad portál tretej strany) a poskytuje možnosť ad-hoc pripojenia pre MOU (napríklad formou QR kódu),
- Vlastník účtu má už vo svojom úložisku dáta, ktoré služba požaduje.

Kroky prenosu:

1. Vlastník účtu (Občan) zistí, že existuje Služba tretej strany, ktorá je pripravená na integráciu s MOU a umožňuje ad-hoc pripojenie služby. Napríklad je o tom

[39] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

informovaný na portáli poskytovateľa tejto služby a pripojenie služby je možné cez QR kód zobrazený na portáli.

2. Vlastník účtu prilinkuje danú službu napríklad zosnímaním QR kódu cez MyData Klient mobilnú aplikáciu.
3. Na základe informácii získaných pri pripojení (z QR kódu) naviaže MyData Operátor komunikáciu so Službou tretej strany a zistí aj, aký dataset služba požaduje.
4. MyData operátor vyhľadá v Osobnom úložisku Vlastníka účtu vhodné datasety, rozšifruje ich s použitím krypto materiálu Vlastníka účtu a zobrazí ich cez MyData Klient Vlastníkovi účtu.
5. Vlastník účtu vyberie dataset z ponuky a potvrdí alebo zamietne poskytnutie tohto datasetu Službe tretej strany.
6. MyData Operátor zašifruje dáta krypto materiálom Služby tretej strany a poskytne ich Službe tretej strany.
7. Služba tretej strany overí kvalifikovanú elektronickú pečať MIRRI, dešifruje dáta použitím svojho krypto materiálu, spracuje dáta a prípadne poskytne vhodný výstup občanovi alebo podnikateľovi.

4.3.1 Bezpečná autentifikácia používateľa

Používateľ MOU pristupuje k funkcionalite MOU cez mobilnú alebo webovú aplikáciu. Pre prácu v MOU musí byť používateľ autentifikovaný. Predpokladáme nasledujúce alternatívy autentifikácie popísané nižšie. Autentifikácia cez eID kartu je eIDAS registrovaná schéma autentifikácie s vysokou úrovňou bezpečnosti. Rovnako to bude platiť aj pri pripravovanej eID2.0 karte.

Pri autentifikácii cez mID sa predpokladá úroveň eIDAS „pokročilá“.

A1: Autentifikácia cez mID

Autentifikácia používateľa bude primárne riešená použitím pripravovaného riešenia mobilnej identity (mID). mID bude použité pri autentifikácii používateľa, ktorý bude pracovať s mobilnou aplikáciou „MyData Client“. Ak používateľ bude pracovať s Web verziou „MyData Client“, taktiež predpokladáme primárne použitie autentifikácie cez mID, s integráciou cez QR kód.

A2: Autentifikácia cez eID kartu

V prípade, že bude používateľ pracovať s Web verziou „MyData Client“, môže použiť na autentifikáciu eID kartu s kontaktnou čítačkou kariet.

A3: Autentifikácia cez eID2.0 kartu

Pripravovaná eID2.0 karta bude vybavená aj bezkontaktným čipom. Ako o prípadnej alternatíve prihlasovania k mobilnej aj Web verzii „MyData Client“ je možné uvažovať aj o použití eID2.0 karty.

Preferovanou alternatívou je A1: Autentifikácia cez mID. mID umožňuje autentifikáciu pre mobilnú a webovú verziu „MyData Client“. Cieľovo bude aplikácia MOU súčasťou

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

komplexnejšej aplikácie SvM (Slovensko v mobile), ktorej súčasťou bude aj mID. Podporovaná bude aj Autentifikácia cez eID kartu.

4.3.2 Ukladanie a ochrana osobných údajov v MOU

Osobné údaje sú v MOU perzistentne ukladané iba do komponentu „Osobné úložisko“. Osobné úložisko predstavuje privátny priestor každého Vlastníka účtu. Dáta budú ukladané do Osobného úložiska v šifrovanej forme. Použitý krypto materiál bude zabezpečený tak, že bude pod výhradnou kontrolou Vlastníka účtu. Dáta budú zdieľané v zašifrovanej forme a rozšifrovanie sa udeje až v aplikácii prijímateľa - tretej strany.

Možnosti šifrovania dát v Osobnom úložisku sú:

- S1. Asymetrické šifrovanie,
- S2. Symetrické šifrovanie.

S1. Asymetrické šifrovanie

Pred perzistentným uložením dát do osobného úložiska budú dáta zašifrované verejným kľúčom Vlastníka účtu. Ak dal Vlastník účtu súhlas na poskytnutie dát prijímateľovi - tretej strane, bude do osobného úložiska uložená kópia dát zašifrovaná verejným kľúčom prijímateľa - tretej strany.

S2. Symetrické šifrovanie

Pred perzistentným uložením dát do osobného úložiska bude vygenerovaný náhodný tajný kľuč a dáta budú zašifrované týmto kľúčom (symetrickou šifrou – tajný kľuč). Tento symetrický kľúč je následne zašifrovaný verejným kľúčom Vlastníka účtu a uložený. Ak dal Vlastník účtu súhlas na poskytnutie dát prijímateľovi - tretej strane, bude tajný kľúč zašifrovaný aj verejným kľúčom prijímateľa - tretej strany a v takto zašifrovanej forme poskytnutý prijímateľovi - tretej strane. V tomto prípade sa teda nevytvára v osobnom úložisku ďalšia zašifrovaná kópia dát pre prijímateľa - tretiu stranu.

V rámci MOU je implementovaná alternatíva S2. Symetrické šifrovanie. V osobnom úložisku sa vytvára iba jedna kopia dát zašifrovaná pre držiteľa aj pre všetkých prijímateľov - tretie strany, ktoré získali súhlas na prístup k daným dátam. Pri asymetrickom šifrovaní by sa vytváralo niekoľko kópii.

Dáta sú pred uložením do osobného úložiska zašifrované s použitím formátu JWE[40]. Dáta sú zašifrované tak, aby k nim mal prístup iba vlastník účtu a prijímatelia - tretia/tretie strany, ktorým dal vlastník účtu súhlas na prístup k dátam. Na vstupe sú dáta, verejný kľúč vlastníka účtu ako aj verejný kľúč prijímateľa - služby tretej strany dostupné. Systém zašifruje dáta do formátu JWE náhodne vygenerovaným tajným kľúčom a odošle ich do osobného úložiska. Tento tajný kľúč bude následne zašifrovaný do formátu JWE verejným kľúčom vlastníka účtu a uložený. Takisto bude tajný kľúč

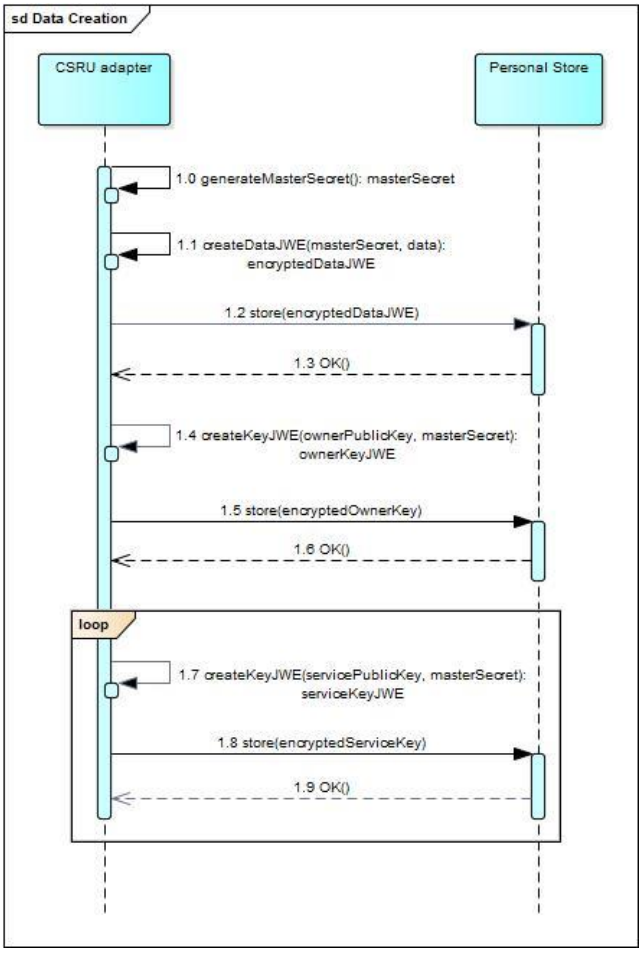
[40] Zdroj: https://www.rfc-editor.org/rfc/rfc7516 , Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

zašifrovaný do formátu JWE aj verejným kľúčom prijímateľa - služby tretej strany a bude uložený.



Obrázok 9: Sekvenčný diagram – zašifrovanie dát pred uložením do osobného úložiska v MOU[41]

Tabuľka 4: Opis krokov – zašifrovanie dát pred uložením do osobného úložiska v MOU

Krok	Názov operácie	Vstupné parametre	Popis
1.0	generateMasterSecret		Vygeneruje sa symetrický master secret, ktorého veľkosť je 256 bitov.
1.1	createDataJWE	masterSecret, data	Dáta sú zašifrované prostredníctvom master secret algoritmom AES CBC do formátu JWE. Šifrovanie dát sa vykoná prostredníctvom knižnice Nimbus JOSE + JWT. Jedná sa o open source knižnicu pre prácu s JWT, ktorá podporuje algoritmy JWE a JWS.

[41] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Krok	Názov operácie	Vstupné parametre	Popis
1.2	store	encryptedDataJWE	Následne sa JWE dáta uložia do osobného úložiska a nastaví sa prístup k dátam pre vlastníka účtu.
1.3	ok()		data boli úspešne uložené
1.4	createKeyJWE	OwnerPublicKey, masterSecret	Prostredníctvom verejného kľúča vlastníka účtu sa zašifruje master secret do formátu JWE. Používa sa algoritmus EC (Elliptic Curve).
1.5	store	encryptedOwnerKey	Vlastníkov kľúč sa následne uloží do osobného úložiska a nastaví sa prístup len pre neho.
1.6	ok()		Kľúč bol úspešne uložený
1.7	createKeyJWE	servicePublicKey, masterSecret	Pre každú službu sa pomocou jej verejného kľúča zašifruje master key vo formáte JWE. Používa sa algoritmus EC (Elliptic Curve).
1.8	store	encryptedServiceKey	Kľúč sa uloží do úložiska a nastaví sa prístup len pre túto službu.
1.9	ok()		Kľúč bol úspešne uložený

4.3.3 PKI a uloženie privátneho kľúča

Alternatívy pre získanie PKI a uloženia privátneho kľúča v MOU sú:

- P1. Kľúčový pár generovaný v MOU pre vlastníka účtu a u prijímateľa - v tretej strane pre službu tretej strany.
- P2. Použitie šifrovacieho certifikátu v eID karte.
- P3. Použitie šifrovacieho certifikátu v mID.
- P4. Šifrovací certifikát vydaný ACA – žiadosť a nahratie offline.
- P5. Šifrovací certifikát vydaný ACA – online integrácia MOU a RA.

MOU bude implementovať alternatívu P1. Kľúčový pár generovaný v MOU pre vlastníka účtu a u prijímateľa - v tretej strane pre službu tretej strany. Z hľadiska bezpečnosti je to postačujúce a z hľadiska nárokov na implementáciu vyhovujúce riešenie.

P1. Kľúčový par generovaný v MOU

Kľúčový pár bude generovaný v MOU pre držiteľa. Privátny kľúč bude bezpečne uložený v MOU a chránený heslom (wallet password). Na ukladanie kľúčového páru bude použité KMS[42] s úrovňou bezpečnostnej certifikácie minimálne úrovne FIPS 140-2. Kľúčový pár

[42] Zdroj: https://www.thesslstore.com/blog/what-is-a-key-management-service-key-management-services-explained/, Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

pre prijímateľa - tretiu stranu bude generovaný prijímateľom - treťou stranou a verejný kľúč bude zaslaný do MOU v rámci procesu registrácie služby tretej strany. Privátny kľúč bude uložený a zabezpečený v bezpečnom úložisku prijímateľa - tretej strany. Spôsob generovania a ukladania krypto materiálu bude pre prijímateľa - tretiu stranu predpísaný MOU v integračnom zámere.

P2. Použitie šifrovacieho certifikátu v eID karte

Predpoklad takejto alternatívy je, že držiteľ má alebo si zaobstará šifrovací certifikát na eID karte. Certifikáty je možné nahrať aj online. Platí to ale iba pre karty vydané od 26.6.21. Táto alternatíva je ale použiteľná iba pre MOU klienta typu webová, desktopová aplikácia. Navyše by eID karta musela byť dostupná v kontaktnej čítačke vždy, keď bude držiteľ robiť operácie vyžadujúce dešifrovanie dát, napríklad prezeranie dát v osobnom úložisku.

P3. Použitie šifrovacieho certifikátu v mID

Predpoklad je, že šifrovací certifikát bude k dispozícii aj v mID.

P4. Šifrovací certifikát vydaný ACA – žiadosť a nahratie off line

Šifrovací certifikát vydaný ACA, napríklad cez registračnú autoritu (RA) MV SR. Nahratie do príslušného úložiska bude manuálny krok, ktorým by bol zaťažený držiteľ. Certifikát môže byť nahratý do bezpečného úložiska kľúčov v danom operačnom systéme.

P5. Šifrovací certifikát vydaný ACA – online integrácia MOU a RA

Šifrovací certifikát vydaný ACA, napríklad cez registračnú autoritu (RA) MVSR, ktorá bude integrovaná s MOU. Privátny kľúč bude uložený v MOU (napríklad zaheslovaná peňaženka).

4.3.4 Autorizácia osobných údajov

Autorizácia údajov zabezpečuje autentickosť (pravosť) a integritu údajov. Pred uložením dát do osobného úložiska MOU sú dáta podpísané kvalifikovanou elektronickou pečaťou MIRRI a zašifrované. Predpokladá sa, že privátny kľúč je uložený a dostupný na zariadení Hardware Security Module (HSM)[43]. Komunikácia s klientmi HSM prebieha prostredníctvom štandardu PKCS-11. Uvedené alternatívy podpisu môžu byť použité podľa typu podpisovaných dát:

- P1. Kvalifikovaná elektronická pečať zdrojového systému.
- P2. Kvalifikovaná elektronická pečať MOU / MIRRI.
- P3. Self signed (Podpísanie dotknutou osobou).

[43] Zdroj: https://www.techtarget.com/searchsecurity/definition/hardware-security-module-HSM, Dátum referencie: 08.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

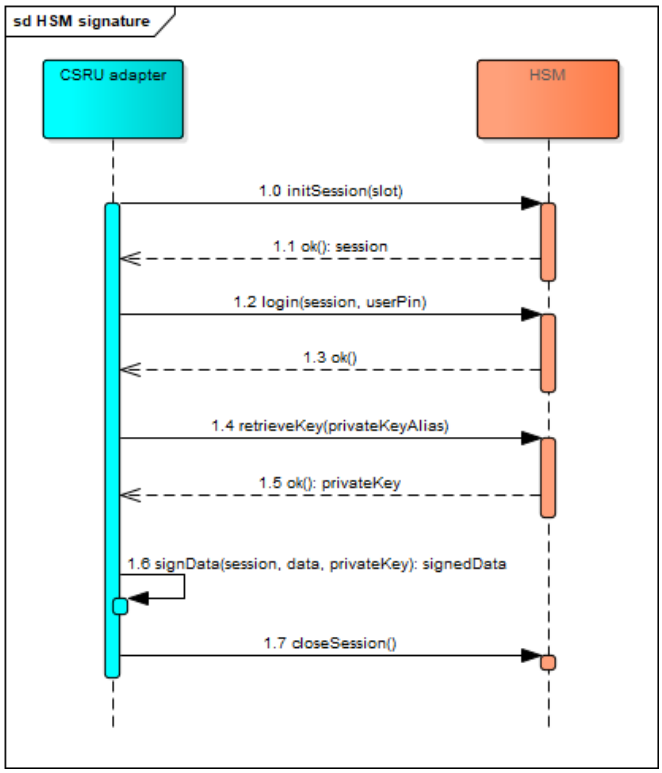
Tento projekt je podporený z Európskeho sociálneho fondu.

P1. Kvalifikovaná elektronická pečať zdrojového systému

V prípade, že finálny dataset typu elektronický doklad je vytvorený priamo v zdrojovom systéme, je preferovaný jeho podpis priamo v tomto zdrojovom systéme. V takom prípade by bol daný elektronický doklad opatrený kvalifikovanou elektronickou pečaťou zdrojového systému v jeho podateľni a v takejto nezmenenej forme prenesený (okrem šifrovania) do osobného úložiska a prípadne aj prijímateľovi - tretej strane, ktorá by použila kvalifikovanú elektronickú pečať na overenie pravosti poskytovaných dát.

P2. Kvalifikovaná elektronická pečať MOU / MIRRI SR

V prípade, že dáta prenesené zo zdrojového systému budú v MOU upravované do finálnej formy (výber dát, transformácia do štandardu RDF a následná serializácia do JSON-LD), bude finálny dataset podpísaný kvalifikovanou elektronickou pečaťou pečaťou MOU/MIRRI SR v MOU.



Obrázok 10: Sekvenčný diagram pre podpísanie dát kvalifikovanou elektronickou pečaťou MIRRI v MOU[44]

[44] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 1

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Tabuľka 5: Popis krokov – podpísanie dát kvalifikovanou elektronickou pečaťou MIRRI v MOU

Krok	Názov operácie	Vstupné parametre	Popis
1.0	initSession	slot	Vytvorí sa session na danom slote zariadenia HSM. Slot je logický prístupový bod pre prístup do zariadenia. Prostredníctvom daného slotu sa získa prístup k tokenu, na ktorom sa vytvára session.
1.1	ok()		Session vytvorená
1.2	login	session, userPin	Prostredníctvom daného userPin sa prihlási do už vytvorenej session. UserPin je používateľský pin nastavený pre daný slot pri konfigurácii zariadenia.
1.3	ok()		Prihlásenie úspešné.
1.4	retrieveKey	session, privateKeyAlias	Zo session sa získa objekt Key podľa daného aliasu. Poznámka: Privátny kľúč zostáva iba v HSM.
1.5	ok()		
1.6	signData	session, data, privateKey	Vstupné dáta sa použitím objektu Key z predchádzajúceho bodu podpíšu. Poznámka: Daná metóda komunikuje s HSM (PKCS#11, alebo iné API) tak, že vytvorí haš vstupných dát a zašle na podpis do HSM. Haš je podpísaný privátnym kľúčom v HSM.
1.7	closeSession		Session sa uzavrie.

P3. Self signed

Osobné údaje môže držiteľ podpísať aj svojím kvalifikovaným elektronickým podpisom a uložiť ich do osobného úložiska a poskytnúť prijímateľovi - tretej strane. Na podpis môže držiteľ použiť napríklad certifikát z eID karty a vhodný nástroj na vytvorenie podpisu. Pri rozširovaní MOU a podľa záujmu o tento typ kvalifikovaného elektronického podpisu do úvahy prichádza aj nástroj na podpisovanie integrovaný priamo v MOU.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

4.3.5 Zdieľanie overiteľných údajov

V MOU je zdieľanie overiteľných údajov zabezpečené cez štandardy a metódy popísané v kapitolách 4.2.1, 4.2.2 a 4.2.3.

Dátový objekt súhlasu v MOU[45]

Dátový objekt súhlasu je definovaný ako:

- Štruktúra záznamu súhlasu - VerifiableCredential (VC),
- Štruktúra záznamu stavu súhlasu – CredentialStatus,
- Štruktúra pre overenie súhlasu - JSON-LD Linked Data proof.

Tabuľka 6: Štruktúra záznamu súhlasu - VerifiableCredential (VC)

Kľúč	Type	Popis
@context	array[String]	JSON-LD kontext pre Verifiable Credential (VC)
id	String	ID pre Verifiable Credential (VC)
type	array[String]	JSON-LD typ pre Verifiable Credential (VC)
issuer	Issuer	Vydavateľ Verifiable Credential (VC)
issuanceDate	String	Pole, ktoré obsahuje počiatočný dátum a čas, kedy má požadovaný prístup nadobudnúť účinnosť; t.j. nadobúda platnosť. Ak sa vynechá, vydavateľ uvedie dátum a čas vydania VC.
expirationDate	String	Pole, ktoré obsahuje dátum a čas, kedy vyprší požadovaný prístup; t.j. sa stáva neplatným.
credentialSubject	array[String]	Koho sa údaje vo VC týkajú.
proof	LinkedDataProof	Tabuľka 8
credentialStatus	CredentialStatus	Tabuľka 7

[45] Zdroj: Detailný návrh riešenia (DNR) pre Manažment osobných údajov: Modul správa súhlasov - fáza 2

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Tabuľka 7: Štruktúra záznamu stavu súhlasu - CredentialStatus

Kľúč	Type	Popis
id	String	ID pre Verifiable Credential (VC), ktoré musí byť vo formáte URI: https://vc.mou.dev.cloud/status/<credential>#<idx>
revocationListCredential	String	Obsahuje linku na zoznam poverení, ktoré boli v MOU odvolané: https://vc.mou.dev.cloud/status/<credential>
revocationListIndex	String	Obsahuje index (poradie) v zozname poverení (riadok vyššie), ktoré boli v MOU odvolané: <idx>
type	Issuer	Vyjadruje typ stavu poverenia. Očakáva sa, že hodnota bude poskytovať dostatok informácií na určenie aktuálneho stavu poverenia (ako napríklad platné či odvolané poverenie) a že strojovo čitateľné informácie musia byť vyhľadateľné: „RevocationList2020Status“

Tabuľka 8: Štruktúra pre overenie súhlasu - JSON-LD Linked Data proof

Kľúč	Type	Popis
type	String	„Linked Data Signature Suite“ používaný na vytvorenie dôkazu.
created	String	Dátum vytvorenia dôkazu.
challenge	String	Hodnota zvolená overovateľom na zmiernenie útokov na overenie totožnosti.
domain	String	Doména dôkazu na obmedzenie jeho použitia na konkrétny cieľ.
nonce	String	Hodnota zvolená tvorcom dôkazu na náhodné usporiadanie hodnôt dôkazu na účely ochrany osobných údajov.
verificationMethod	String	Overovacia metóda použitá na overenie dôkazu.
proofPurpose	String	Účel dôkazu, ktorý sa má použiť s metódou overovania (verificationMethod).
jws	String	JSON Web Signature.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Kľúč	Type	Popis
proofValue	String	Obsah „Linked Data proof“.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Tabuľka 9: Príklad konkrétnej implementácie súhlasu ako Verifiable credential


```
{
 "verifiableCredential": {
  "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "https://vc.mou.dev.cloud/credential/a79e2b46-c7d4-4613-b7e3-d93f637fbb29",
  "type": [
   "VerifiableCredential",
   "SolidCredential",
   "SolidConsentRequest"
  ],
  "expirationDate": "2022-10-25T03:21:58.708Z",
  "credentialStatus": {
   "id": "https://vc.mou.dev.cloud/status/xCZZ#0",
   "revocationListCredential": "https://vc.mou.dev.cloud/status/xCZZ",
   "revocationListIndex": "0",
   "type": "RevocationList2020Status"
  },
  "credentialSubject": {
   "id": "https://solid.mou.dev.cloud/requestingParty/profile/card#me",
   "inbox": "https://solid.mou.dev.cloud/requestingParty/inbox/",
   "hasConsent": {
    "mode": [
     "http://www.w3.org/ns/auth/acl#Read",
     "http://www.w3.org/ns/auth/acl#Write"
    ],
    "hasStatus": "https://w3id.org/GConsent#ConsentStatusRequested",
```


© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

```
  "forPersonalData": [
   "https://solid.mou.dev.cloud/john-doe/dataset/mydata"
  ],
  "forPurpose": "https://example.com/SomeSpecificPurpose"
 }
},
"issuer": {
 "id": "https://vc.mou.dev.cloud"
},
"issuanceDate": "2022-02-07T16:05:14.666Z",
"proof": {
 "created": "2022-02-07T16:05:14.666Z",
 "type": "JsonWebSignature2020",
 "proofPurpose": "assertionMethod",
 "verificationMethod": "https://vc.mou.dev.cloud/key/ovsDKYBjFemIy8DVhc-w2LSi8CvXMw2AYDzHj04yxkc",
 "jws": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..Fpr1thmowrDeXhLFLkdJVdAlXcqTCn6aQ_T6vhXeJHejM8zK1eWBVaOcnXHhgQ-BbhzfQL5n-oWd2bd-lxxdBw"
 }
}
}
```


© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

5 Príklady dobrej praxe aplikácie štandardu v zahraničí

Údaje sú pre podniky a organizácie neuveriteľne cenným zdrojom, ktoré im pomáhajú zlepšovať služby a procesy. Existuje však stále viac dôkazov, ktoré naznačujú, že plná hodnota údajov sa nerealizuje, pretože dôležité informácie sa nedostávajú tam, kde by mali byť. Veľká časť potenciálu údajov spočíva v ich schopnosti byť prepojené a opätovne použité v rôznych organizáciách, doménach a sektoroch. Aby sa zabezpečilo, že sa tento potenciál naplní, je dôležité vytvoriť správne podmienky a stimuly pre organizácie na spoluprácu s prístupom ku kvalitným údajom. Je tiež potrebné nájsť rovnováhu medzi prístupom a stimulmi pre zber a spracovanie údajov.

V nasledujúcej časti predstavíme prípadové štúdie z jednotlivých štátov, ktoré možno považovať za dobrú prax:

- Iniciatíva: Úloha sprostredkovateľov údajov pri podpore zodpovedného zdieľania údajov (UK),
- Projekt: TRUSTS – Trusted Secure Data Sharing Space (EÚ),
- Národná stratégia: Mon Espace Santé (FR),
- Projekt: GAIA-X (DE).

5.1 Úloha sprostredkovateľov údajov pri podpore zodpovedného zdieľania údajov (UK)

Zodpovedné zdieľanie údajov je vo Veľkej Británii definované ako synonymum dôveryhodného zdieľania údajov v rámci EÚ.

Tabuľka 10: Iniciatíva Úloha sprostredkovateľov údajov pri podpore zodpovedného zdieľania údajov (UK) – Sumár

Iniciatíva: Úloha sprostredkovateľov údajov pri podpore zodpovedného zdieľania údajov (UK)	
Zapojené subjekty	CDEI - Centrum pre dátovú etiku a inováciu pomohlo formovať vládny prístup k uprednostňovaniu iniciatív na podporu dostupnosti údajov, podporu inovácií a rastu. V spolupráci s vládou preskúmalo mechanizmy, ktoré umožňujú dôveryhodné používanie a zdieľanie údajov, vrátane mechanizmov riadenia, ako sú sprostredkovatelia údajov, vrátane technológií na zvýšenie súkromia (PET). DCMS – Ministerstvo pre digitálnu transformáciu, kultúru, médiá a šport pôsobí v srdci vlády Spojeného kráľovstva pri niektorých z najväčších ekonomických a sociálnych problémov. Ich poslaním je podporovať rast a propagovať Spojené kráľovstvo vo svete inovácií, vrátane umelej inteligencie. ICO – Úrad komisára pre informácie je nezávislým dozorným orgánom Spojeného kráľovstva na ochranu údajov. Úlohou ICO je monitorovať, zabezpečovať a presadzovať dodržiavanie ustanovení o ochrane údajov a súkromia vrátane vybavovania

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

	sťažností dotknutých osôb. ICO má širokú škálu právomocí, ktoré mu umožňujú byť účinným orgánom na ochranu údajov.
Harmonogram implementácie	2021 - súčasnosť

Súkromie je základné právo, pričom organizácie majú povinnosť chrániť súkromie a pri práci s osobnými alebo citlivými údajmi musia brať do úvahy dôležité právne, etické problémy a obavy týkajúce sa súkromia. Britská Národná dátová stratégia bola zverejnená 9. septembra 2020 a spojila ambície Spojeného kráľovstva v oblasti údajov do jedného koherentného dokumentu.

Táto stratégia identifikuje päť potenciálnych príležitostí pre údaje na transformáciu Spojeného kráľovstva vrátane: zvyšovania produktivity a obchodu, podpory nových podnikov a pracovných miest, zvyšovania rýchlosti, efektívnosti a rozsahu vedeckého výskumu, podpory lepšieho poskytovania verejných služieb a vytvorenie spravodlivejšej spoločnosti pre všetkých. Obrovský potenciál verejných a súkromných údajov v Spojenom kráľovstve sa však ešte musí využiť. Na podporu prvej misie zo stratégie: „Uvoľnenie hodnoty údajov v celej ekonomike“ sa uskutočnili rôzne iniciatívy, ktoré skúmali úlohu sprostredkovateľov údajov (*Data intermediary*) a technológií na zvýšenie súkromia (*Privacy-enhancing Technologies*, ďalej len PET) pri podpore zodpovedného zdieľania údajov.

5.1.1 Témy

Sprostredkovateľ údajov

Existujú rôzne činnosti, ktoré sa uskutočňujú, keď sú údaje zdieľané, sprístupňované alebo používané. Sprostredkovatelia údajov, ktorí môžu byť vo verejnom alebo súkromnom sektore, môžu pomôcť absorbovať náklady a riziká spojené s vykonávaním činností spracovania údajov. Existuje široká škála inovatívnych dátových sprostredkovateľov, ktorí vytvárajú nové, technologické riešenia umožňujúce bezpečné a bezproblémové zdieľanie dát. Príkladom je platforma pre zdieľanie dát v priemysle „MK Data Hub“[46], platforma na zdieľanie genomických údajov medzi výskumníkmi so zapojením pacientov „Genomics England“[47] či platforma na férové zdieľané osobných údajov za odmeny „Bits about Me“[48].

Sprostredkovatelia údajov poskytujú technickú infraštruktúru, odborné znalosti a konzultačné služby na uľahčenie zdieľania, prístupu a združovania údajov medzi stranami. V závislosti od okolností môžu pôsobiť aj ako správcovia údajov alebo sprostredkovatelia. Umožňujú mať väčšiu kontrolu a možnosť voľby nad tým, kto má prístup k ich údajom a na vopred definované účely. Sprostredkovatelia údajov tiež uľahčujú prístup k údajom a ich zdieľanie pre výskum a inovácie, ako aj pre nezávislý audit technológií založený na údajoch.

[46] Zdroj: https://www.mksmart.org/data/, Dátum referencie: 27.03.2023

[47] Zdroj: https://www.genomicsengland.co.uk, Dátum referencie: 27.03.2023

[48] Zdroj: https://bitsabout.me, Dátum referencie: 27.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Štúdia CDEI[49] skúma sedem typov dátových sprostredkovateľov vrátane: dátových fondov, dátových búrz, systémov správy osobných informácií, priemyselných dátových platforiem, správcov dát, dátových družstiev a dôveryhodných tretích strán.

Tabuľka 11: Sedem typov dátových sprostredkovateľov

TYP	DEFINÍCIA
Dátové fondy (Data Trusts)	Poskytujú správcovstvo údajov v mene dotknutých osôb.
Dátové burzy (Data Exchanges)	Fungujú ako online dátové platformy, kde je možné inzerovať súbory údajov a pristupovať k nim – komerčne alebo na neziskovom základe.
Systémy na správu osobných informácií (Personal information management systems, PIMS)	Snažia sa poskytnúť dotknutým osobám väčšiu kontrolu nad ich osobnými údajmi.
Priemyselné dátové platformy (Industrial data platforms)	Poskytujú zdieľanú infraštruktúru na uľahčenie bezpečného zdieľania údajov a analýzy medzi spoločnosťami.
Správcovia údajov (Data custodians)	Umožňujú analýzu ochrany súkromia alebo kontrolu atribútov dôverných údajov, napríklad prostredníctvom aplikácie PET.
Dátové družstvá (Data cooperatives)	Poskytujú zdieľané dátové priestory kontrolované dotknutými osobami.
Dôveryhodné tretie strany (Trusted third parties)	Poskytujú uistenie tým, ktorí chcú získať prístup k dôverným súborom údajov, že údaje sú vhodné na daný účel (napríklad z hľadiska kvality alebo etických noriem).

Technológie na zvýšenie súkromia (PET)

Národná dátová stratégia vlády Spojeného kráľovstva si okrem iného stanovila za cieľ preskúmať úlohu technológií na zvýšenie súkromia pri zabezpečovaní dôveryhodného používania údajov.

Technológia na zvýšenie súkromia je akákoľvek technická metóda, ktorá chráni súkromie osobných alebo citlivých informácií. Táto definícia zahŕňa relatívne jednoduché technológie, ako aj infraštruktúru šifrovania. Pre iniciatívu CDEI je obzvlášť zaujímavý užší súbor vznikajúcich PET. Ide o skupinu relatívne nových technológií, ktoré sa implementujú v čoraz väčšom počte projektov v reálnom svete, aby pomohli prekonať problémy v oblasti súkromia a bezpečnosti.

PETs majú potenciál odomknúť inovácie tým, že umožňujú zdieľanie a analýzu údajov a zároveň chránia súkromie a dôvernosť používateľov. Bolo identifikovaných a preskúmaných päť nových PETs:

- homomorfné šifrovanie (*Homomorphic encryption*),
- dôveryhodné spúšťacie prostredia (*Trusted execution environments*),
- bezpečné výpočty viacerých strán (*Secure multi-party computation*),

[49] Odkaz: link, Dátum referencie: 14.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

- diferenciálne súkromie (*Differential privacy*), a
- federovaná analytika (*Federated analytics*).

Tieto technológie podporujú celý rad prípadov použitia zahŕňajúcich bezpečné spracovanie údajov, dôveryhodné zdieľanie údajov a strojové učenie s ohľadom na ochranu súkromia. Môžu byť užitočné najmä v sektoroch, kde sú vysoko citlivé údaje normou, ako je zdravotníctvo a financie.

5.1.2 Ciele

CDEI spolupracuje s DCMS a ICO, aby preskúmali, ako možno PETs použiť na zlepšenie zdieľania a dôveryhodnosti údajov. PETs získavajú na popularite v politike aj v kruhoch odborníkov, ale prijatie zostáva nízke kvôli nedostatku povedomia, odborných znalostí a technických obmedzení. CDEI sa snaží riešiť tieto problémy tým, že organizáciám poskytuje technické zručnosti a praktický súbor nástrojov na rozhodovanie a na uľahčenie prijatia PETs. CDEI verí, že pri použití v správnom prostredí môžu PETs priniesť značné výhody a umožniť použitie údajov v rámci organizácií, domén a sektorov.

Plánované iniciatívy v rámci PETs budú zahŕňať aj napríklad použitie systémov na správu osobných informácií (PIMS), v ktorých jednotlivec importuje osobné údaje od vydavateľov - poskytovateľov a môže spravovať, kto má prístup k jeho úložisku osobných údajov, udeľovaním alebo odvolaním prístupu. SOLID[50] je jedným z takýchto príkladov technológie pre PIMS, ktorú využíva aj MOU.

5.1.3 Výsledky

Táto iniciatíva sa uskutočnila s cieľom identifikovať oblasti, v ktorých by používanie technológií na zvýšenie súkromia (PETs) mohlo priniesť významné výhody. Na tento účel tím zhromaždil príklady a vykonal hĺbkové prípadové štúdie s cieľom získať spoločné poznatky.

Vo februári 2021 spustili otvorenú výzvu, v ktorej požiadali jednotlivcov a organizácie vyvíjajúce alebo využívajúce PETs, aby sa podelili o príklady, kde boli PETs testované alebo úspešne používané v produkčnom prostredí. Na otvorenú výzvu dostali pozitívnu odpoveď, pričom viac ako 50 zainteresovaných strán z celého priemyslu, akademickej obce a verejného sektora predložilo svoje príklady používaných PETs. Dozvedeli sa o množstve rôznych prípadov použitia PETs v mnohých odvetviach vrátane financií, zdravotníctva a digitálnych platforiem.

Bolo identifikovaných niekoľko prekážok rozšíreného prijatia PETs, vrátane nedostatku povedomia a odborných znalostí, slabých dátových základov, finančného rizika, regulačnej neistoty a technologickej nezrelosti. Na riešenie týchto problémov tím navrhol vláde celý rad intervencií. Tím zverejnil archív prípadov použitia, ktoré zhromaždil, čo je užitočný zdroj pre organizácie, ktoré chcú využiť PETs. Zverejnili tiež príručku o implementácii PETs.

5.1.4 Súvisiaca literatúra

HM CDEI. 2021. *Unlocking the value of data: Exploring the role of data intermediaries*. Odkaz.

[50] Zdroj: https://solidproject.org/, Dátum referencie: 14.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

HM CDEI. 2021. *Privacy Enhancing Technologies Adoption Guide*. Odkaz.

HM DCMS. 2020. *National Data Strategy*. Odkaz.

ICO. 2022. *Guidance in privacy-enhancing Technologies*. Odkaz.

ODI. 2022. *What are data intermediaries*. Odkaz.

TechUK. 2021. *The future of ethical data sharing: the role of data intermediaries*. Odkaz.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

5.2 TRUSTS

Tabuľka 12: Projekt TRUSTS – Sumár

Projekt: TRUSTS – Trusted Secure Data Sharing Space (EU)	
Zapojené subjekty	Konzorcium pozostáva zo sedemnástich partnerov so sídlom v deviatich krajinách v Rakúsku, Belgicku, na Cypre, v Nemecku, Grécku, Izraeli, Holandsku, Rumunsku a Španielsku.
Harmonogram implementácie	Január 2020 až December 2022

Trusted Secure Data Sharing Space (TRUSTS) je inovačný projekt financovaný z programu Európskej únie pre výskum a inovácie Horizont 2020. Cieľom projektu je vytvoriť bezpečný a dôveryhodný európsky dátový trh pre osobné a priemyselné využitie dát, prepojením rôznych skupín používateľov a poskytnutím všeobecných funkcionalít pre inovatívne aplikácie a služby. TRUSTS spája poskytovateľov technológií, poskytovateľov údajov a výskumné inštitúcie.

5.2.1 Témy

Dátové platformy, spoločné dátové priestory alebo trhoviská sú čoraz populárnejšie, keďže aj tvorcovia politík veria, že údaje by mali byť obchodovateľnou komoditou. Praktickej uskutočniteľnosti takýchto prístupov však bránia rôzne výzvy, ako napríklad nedostatok zručností a znalostí, potreba chrániť súkromie, bezpečnosť, regulácia a konkurencieschopnosť. Existujú už dátové trhy, ktoré sa špecializujú na určité odvetvia alebo dátové typy, ale aby boli úspešné na európskej úrovni, je potrebné vytvárať systémy dátových trhovísk, ktoré môžu navzájom spolupracovať a vytvoriť tak veľký ekosystém.

TRUSTS bol výskumný projekt, ktorý sa zameriaval na riešenie hlavných výziev v oblasti ochrany osobných údajov s cieľom poskytnúť právne a technické pohľady na ochranu súkromia a analýzy zlúčenia šifrovania s inými prístupmi strojového učenia. Na to, aby zdieľanie údajov fungovalo, je tiež potrebný solídny právny a etický rámec, preto TRUSTS vyvinul etické princípy výskumu na riešenie právnych a etických problémov vyplývajúcich z výskumných aktivít projektu.

5.2.2 Ciele

TRUSTS bol projekt zameraný najmä na vývoj platformy na podporu dôvery v dátové trhy ako celok. Platforma bola navrhnutá tak, aby fungovala nezávisle a ako federátor platforiem, berúc do úvahy právne a etické aspekty, ktoré sa vzťahujú na celý reťazec, od poskytovateľov údajov až po konzumentov. Cieľom projektu bolo vytvoriť európsky dátový trh v súlade s GDPR pre osobné aj neosobné údaje so zameraním na osobné aj komerčné využitie. Platforma mala byť obohatená o nové funkcie a služby a demonštrovať a realizovať svoj potenciál v troch prípadoch použitia zameraných na finančný sektor a telekomunikačných operátorov.

Aby bolo možné spolupracovať s inými trhmi s údajmi, TRUSTS musí byť interoperabilný s externými trhmi a iniciatívami European Open Science Cloud. Okrem toho musí mať

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

komponent na kontrolu, či existuje platná zmluva medzi poskytovateľom a konzumentom, čo zaisťuje, že prístup a používanie údajov je bezpečné a chránené.

5.2.3 Výsledky

Konečným výsledkom TRUSTS bola úspešná implementácia federatívneho dátového trhu, ktorý bol hodnotený tromi špecificky navrhnutými prípadmi použitia:

1. UC1: inteligentný systém na zdieľanie veľkých dát (Big data) a analytický systém pre dodržiavanie pravidiel boja proti praniu špinavých peňazí;
2. UC2: agilná marketingová kampaň prostredníctvom korelácie anonymizovaných bankových údajov a údajov operátorov;
3. a UC3: nákup údajov z dátového trhu na zlepšenie prirodzenej interakcie.

Pre úspešnú implementáciu platformy TRUSTS sa vykonala podrobná analýza požiadaviek na komerčnú finančnú platformu a platformu vertikálnych trhov s údajmi operátorov a prípady použitia. Táto správa obsahuje aj definíciu scenárov vysokej úrovne a cieľových kľúčových indikátorov výkonnosti, ktoré sa použijú na meranie úspešnosti projektu.

Prípady použitia celkovo splnili svoje kľúčové indikátory výkonnosti s pozoruhodným úspechom. Najviac sa páčilo používateľské rozhranie a výkon aplikácií UC1. Tok údajov a proces boli v tomto prípade použitia dobre štruktúrované a vykonávané. UC2 demonštroval schopnosti platformy TRUSTS ako „Trusted Secure Data Sharing Space“ pre pokročilé marketingové aktivity prostredníctvom korelácie anonymizovaných bankových a telekomunikačných údajov. Spätná väzba bola vo všeobecnosti pozitívna, pokiaľ ide o uskutočnené kroky a tok, aj keď sú stále potrebné zlepšenia. UC3 bol schopný otestovať a demonštrovať schopnosti platformy TRUSTS a poskytnúť informácie a spätnú väzbu na základe vykonaných testov. UC3 testoval „Zber údajov na zlepšenie služieb zákazníckej podpory“ so všeobecným výsledkom, že dosiahnutý výsledok spĺňa očakávania projektu. Napriek všetkým problémom, platforma nakoniec dokázala poskytnúť služby potrebné na úspešné dokončenie UC3.

5.2.4 Súvisiaca literatúra

TRUSTS-data. 2022. Deliverables. https://www.trusts-data.eu/deliverables/

IDS. 2021. The Trusts Project. https://internationaldataspaces.org/the-trusts-project-enables-european-data-markets-based-on-the-ids-architecture/

L3S. 2021. TRUSTS. https://www.l3s.de/en/projects/trusts

DIO. 2021. The core of TRUSTS. https://www.dataintelligence.at/en/webinar-the-core-of-trusts/

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

5.3 Mon Espace Santé

Tabuľka 13: Národná stratégia: Mon Espace Santé (FR)

Národná stratégia: Mon Espace Santé (FR)	
Zapojené subjekty	MoSH - Ministerstvo sociálnych vecí a zdravotníctva CNAM - Národný fond zdravotného poistenia ANS - Úrad pre digitálne zdravie (Agence du Numérique en Santé) Atos – Globálny líder v oblasti digitálnej transformácie, kybernetickej bezpečnosti, cloudu a vysokovýkonnej výpočtovej technik.
Harmonogram implementácie	2019 - súčasnosť

V roku 2019 bolo zriadené francúzske národné centrum údajov o zdraví (Health Data Hub) spolu s digitálnym priestorom pre osobné zdravotné informácie občanov s názvom Mon Espace Santé (*My Health Space*). Stratégia digitálneho zdravia Ministerstva sociálnych vecí a zdravotníctva (MoSH), ktorá zastrešuje tieto intervencie, zdôrazňuje dôležitosť holistického prístupu kombinujúceho etické, technické a bezpečnostné štandardy, spoluprácu so súkromným sektorom, zapojenie zainteresovaných strán a digitálne zručnosti.

Platforma Mon Espace Santé (Ďalej len MES), vyvinutá konzorciom vedeným spoločnosťou Atos v spolupráci s francúzskym Národným fondom zdravotného poistenia (CNAM), je prístupná všetkým francúzskym občanom od januára 2022. MES, kľúčový pilier francúzskeho plánu Ma santé 2022, zjednodušuje cestu k zdravotnej starostlivosti pre 65 miliónov používateľov tým, že funguje ako personalizovaná digitálna služba, ktorá umožňuje bezpečne ukladať a zdieľať zdravotné údaje. Údaje pre MES platformu sú ukladané vo Francúzsku s využitím medzinárodných štandardov (štandard HL7® FHIR®) pre výmenu zdravotných informácií.

5.3.1 Témy

Vďaka MES má používateľ prístup k 4 hlavným funkciám:

- Zdravotný spis – umožňuje nahliadnutie a doplnenie dokumentov užívateľom alebo zdravotníkmi (recept, prepúšťacia správa, laboratórne výsledky, atď.). Modul je založený na aktuálnom francúzskom zdieľanom lekárskom zázname (DMP).

- Služba zasielania správ – umožňuje bezpečný príjem osobných informácií prostredníctvom služby zasielania správ. Používateľ nemôže kontaktovať zdravotníckeho pracovníka, ak ho ešte tento odborník nekontaktoval.

- Katalóg eHealth služieb – umožňuje prístup k zdravotníckym aplikáciám (môžu to byť webové stránky a aplikácie, bezplatné alebo platené služby, od súkromných alebo verejných subjektov). Katalóg služieb bol spustený 3.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

novembra 2022 a v súčasnosti je referencovaných 12 služieb pre 65,4 milióna používateľov.

- Kalendár – kalendár na sledovanie a pripomienkovanie vyšetrení.

5.3.2 Ciele

Kľúčové ciele MES platformy zahŕňajú:

- Pomôcť občanom zorientovať sa v zdravotnej starostlivosti a ponúknuť im bezpečný systém na manažment zdravotníckych dát, vrátane zasielania a prijímania dôverných dokumentov o zdraví,
- zlepšiť a regulovať ponuku digitálnych zdravotníckych služieb prostredníctvom katalógu služieb,
- vylepšiť spôsob zdieľania lekárskych záznamov (DMP).

5.3.3 Výsledky

Zavedením MES umožnila francúzska vláda 69 miliónom ľudí prístup k zabezpečenému online priestoru pre manažment zdravotníckych údajov a personalizované služby. Väčšina príjemcov bola informovaná e-mailom (77 %) a zvyšok (23 %) bol informovaný poštou. Zaujímavé je, že menej ako 2 % ľudí namietalo proti vytvoreniu svojho online priestoru a doteraz si tento systém osvojilo už 65,4 milióna francúzskych poistencov. Ide o vysokú mieru prijatia – viac ako 98 % Francúzov teraz môže dostať zdravotnú správu elektronicky.

5.3.4 Súvisiaca literatúra

Report for the National Co-ordinating Centre for NHS Service Delivery and Organisation R & D (NCCSDO) Programme of Research on E-health. https://njl-admin.nihr.ac.uk/document/download/2026824

Zablit I. Accelerating e-health implementation with MyHealthSpace and the renewed role of the state as a platform. ECDC consultation on digital technologies in public health; 2021 June 15.

Digital Health Summit. https://echalliance.com/wp-content/uploads/2021/11/Isabelle-Presentation-v1.pdf

Accelerating the Development of the eHealth Market in Europe. https://www.digitalhealthnews.eu/images/stories/pdf/lmi-report-final-2007dec.pdf

Shared Medical Record (DMP). https://gnius.esante.gouv.fr/en/regulations/regulation-profiles/shared-medical-record-dmp

Accelerating Virtual Health Implementation Following the COVID-19 Pandemic: Questionnaire Study. https://pubmed.ncbi.nlm.nih.gov/35323115/

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

5.4 GAIA-X

Tabuľka 14: Projekt: GAIA-X (Nemecko, Francúzsko) - sumár

Projekt: GAIA-X (Nemecko, Francúzsko**)**	
Zapojené subjekty	Ministerstvo hospodárstva v Nemecku Ministerstvo hospodárstva vo Francúzsku Európska komisia (medzi členov patrí aj MIRRI SR, MO SR, MH SR, MZV SR)
Harmonogram implementácie	2019 - súčasnosť

V októbri 2019 Peter Altmaier, bývalý nemecký minister hospodárstva, a Bruno Le Maire, jeho francúzsky náprotivok, predstavili verejnosti svoju spoluprácu, Gaia-X, na digitálnom summite. Cieľom tohto francúzsko-nemeckého projektu bolo vytvoriť bezpečnú dátovú infraštruktúru pre Európu s pomocou vedeckých inštitúcií a predstaviteľov spolkovej vlády a francúzskej vlády.

Projekt GAIA-X získal podporu od nemeckej a francúzskej vlády spolu s 300 organizáciami z rôznych krajín a je prepojená s Európskou komisiou. Vyvinuli technickú architektúru, ktorá poskytuje bezpečnú a združenú dátovú infraštruktúru, reprezentujúcu európske hodnoty, ako je digitálna suverenita vlastníkov dát, interoperabilita rôznych platforiem a Open-sourcing. Vytvoril sa tak ekosystém, v ktorom môžu byť údaje zdieľané, používané a poskytované v dôveryhodnom prostredí, čím sa podnecuje inovácia a vytvára sa hodnota pre dátovú ekonomiku.

GAIA-X používa štandard IDS na základe iniciatívy IDS (*Intenational Data Spaces*)[51]. Štandard IDS definuje, ako je možné nastaviť dôveryhodné dátové priestory a ako musia byť navrhnuté prístupové body k takémuto dátovému priestoru. Štandard zabezpečuje rovnaké podmienky a presadzuje suverenitu údajov pomocou technických opatrení.

5.4.1 Témy

GAIA-X je postavená na troch pilieroch:

- GAIA-X Association for Cloud and Infrastructure (AISBL) – Asociácia GAIA-X pôsobí aj ako ambasádor pre GAIA-X, zastupuje členov a podporuje medzinárodnú spoluprácu v oblastiach digitálnej suverenity, Cloudu, high performance computingu, Edge výpočtovej techniky, kybernetickej bezpečnosti a štandardizácie. Za týmto účelom organizácia úzko spolupracuje s existujúcimi

[51] https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-GAIA-X-and-IDS.pdf

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

štandardizačnými iniciatívami a inými súvisiacimi organizáciami, aby sa zabezpečila synergia s existujúcimi znalosťami a predchádzajúcimi investíciami.

- Národné Huby GAIA-X – Nemecký GAIA-X Hub je prvým kontaktným bodom pre všetky spoločnosti, organizácie a zainteresované strany v Nemecku, ktoré sa chcú dozvedieť viac o open-source projekte alebo sa chcú zapojiť do komunity. V súčasnej dobe existuje aj slovenský Hub[52].

- Komunita Gaia-X

5.4.2 Ciele

Platforma GAIA-X nie je navrhnutá tak, aby konkurovala existujúcim službám, ale namiesto toho spája existujúce služby a komponenty prostredníctvom otvorených rozhraní a štandardov s cieľom zhromažďovať údaje a vytvárať platformu pre inovácie. Platforma je k dispozícii všetkým zainteresovaným stranám, od veľkých korporácií až po malé podniky a startupy, s hlavným zameraním na používateľov. Technická implementácia služieb GAIA-X sa zameriava na:

- implementáciu bezpečných federovaných mechanizmov identity a dôvery (bezpečnosť a súkromie už od návrhu – „privacy by design“),
- suverénne dátové služby, ktoré zaisťujú bezpečnosť a transparentnosť,
- jednoduchý prístup k dostupným poskytovateľom, uzlom a službám. Údaje sú poskytované prostredníctvom združených katalógov, a
- integráciu existujúcich noriem a štandardov na zabezpečenie interoperability a prenosnosti v rámci infraštruktúry, aplikácií a údajov.

5.4.3 Výsledky

Do platformy GAIA-X je už zapojených viac ako 300 organizácií z mnohých krajín (ako napríklad BDI, Bitkom, eco, VOICE, VDMA, Cigref a MEDEF a existujúce iniciatívy ako International Data Spaces Association a Trusted Cloud sú tiež intenzívne zapojené). Predstavenstvo GAIA-X sa skladá z vedúcich zamestnancov európskych spoločností vrátane OVHCloud, Airbus, Orange a Deutsche Telekom.

Článok Euractiv[53] z roku 2021 upozorňuje na potenciálne problémy, ktorým môže projekt v budúcnosti čeliť, napríklad ako vytvoriť škálovateľnú a bezpečnú dátovú infraštruktúru a ako si získať dôveru vlastníkov údajov. Podľa spomínaného článku od Euractiv zaznamenala GAIA-X od svojho vzniku výrazný nárast členov, pričom pôvodných 22 zakladajúcich členov sa rozrástlo na viac ako 350. Patria sem niektoré z najväčších technologických spoločností na svete, ako sú Microsoft, Google, Amazon a IBM. Toto rozšírenie vyvolalo znepokojenie medzi niektorými zúčastnenými stranami, ktorí sa obávajú, že GAIA-X by mohol byť použitý ako „trójsky kôň“.

[52] https://gaia-x.sk/home/

[53] https://www.euractiv.com/section/digital/news/cracks-appear-as-gaia-x-celebrates-its-progress/

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Na Slovensku bol v júni 2021 zriadený GAIA-X Hub Slovakia. Koordinačný výbor je zložený zo zástupcov MIRRI SR, PIK, ITAS/SCDI, ministerstiev zahraničia, hospodárstva a obrany a Fakulty riadenia a informatiky Žilinskej univerzity.

Rámec Gaia-X[54] definuje tri kľúčové piliere súladu, federácie a výmeny údajov a ich vzájomné prepojenie s cieľom vytvoriť novú generáciu hospodárstva založeného na zdieľaní údajov. Viaceré mechanizmy a štandardy, predovšetkým v rámci rámca dôveryhodnosti, sú v súlade s týmto dokumentom (kapitola 4.2).

Združenie Gaia-X vyvíja prostredníctvom svojho laboratória Gaia-X Lab[55] implementáciu rámca dôveryhodnosti a ponúka jeho inštanciu prostredníctvom služieb „Gaia-X Compliance“ a „Gaia-X Registry“. Laboratórium Gaia-X vytvára aj ukážky a overené koncepty, ktoré pomáhajú technicky overiť špecifikácie Gaia-X. V rámci iniciatív GXFS[56] sa vyvíja súbor softvérových komponentov na základe špecifikácií federatívnych služieb. Vytvorený kód je otvorený a do týchto projektov môže prispievať ktokoľvek.

Gaia-X tiež definuje takzvaný „dátový priestor“ („data space“), ktorý sa vzťahuje na typ dátového vzťahu medzi dôveryhodnými partnermi, ktorí dodržiavajú rovnaké štandardy a usmernenia v súvislosti s ukladaním a zdieľaním údajov v rámci jedného alebo viacerých vertikálnych ekosystémov, napríklad pre financie, zdravotníctvo, mobilitu, energetiku, verejnú správu a inteligentné mestá.

5.4.4 Súvisiaca literatúra

German Federal Ministry for Economic Affairs & Energy, and French Ministry of Economy & Finance (2020): Franco-German Position on GAIA-X, https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10,

German Federal Ministry for Economic Affairs & Energy and Ministry of Economy & Finance (2020): Germany and France take the lead as Europe makes first step towards building a European data infrastructure, https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2020/20200604-germany-and-france-take-the-lead-as-europe-makes-first-step-towards-building-a-european-data-infrastructure.html

Achim Streit und Jos van Weze (2021): Deutschland in der European Open Science Cloud, in: M. Putnings, H. Neuroth, & J. Neumann (ed.), Praxishandbuch Forschungsdatenmanagement, p. 40, https://doi.org/10.1515/9783110657807-003.

German Federal Ministry for Economic Affairs and Energy (ed.): GAIA-X: Driver of digital innovation in Europe.

Achim Streit und Jos van Weze (2021): Deutschland in der European Open Science Cloud, in: M. Putnings, H. Neuroth, & J. Neumann (ed.), Praxishandbuch Forschungsdatenmanagement, p. 40, https://doi.org/10.1515/9783110657807-003.

[54] Zdroj: https://docs.gaia-x.eu/framework/, Dátum referencie: 27.04.2023

[55] Zdroj: https://gitlab.com/gaia-x/lab, Dátum referencie: 27.04.2023

[56] Zdroj: https://gitlab.com/gaia-x, Dátum referencie: 27.04.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Is Gaia-X on course to challenge the big tech platforms? https://www.raconteur.net/technology/will-gaia-x-challenge-the-big-tech-platforms/

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

6 Záver: Návrh odporúčaní na aplikáciu štandardu

Návrh odporúčaní na aplikáciu štandardu dôveryhodných údajov pre informačné prostredie verejnej správy a projekty z programu Manažment údajov si kladie nasledovné ciele:

1. Zabezpečiť dôveryhodnosť údajov, predovšetkým v zmysle dátovej integrity (kapitola 2.1.1 a 2.1.2).
2. Zdieľať overiteľné údaje (kapitola 2.1.3).
3. Dať používateľom možnosť vybrať si, v akom rozsahu budú informácie, ktoré majú pod kontrolou, zdieľať (často označované ako selektívne zverejňovanie podľa kapitoly 4.2.3).
4. Umožniť tretím stranám prijímajúcim informácie zachovať si istotu o pôvode, pravosti a integrite predložených informácií (kapitoly 4.1.1, 4.2.1 a 4.2.2).

Dosiahnutie týchto 4 cieľov v praxi bude predstavovať solídny základ pre aplikovanie Nariadenia európskeho parlamentu a rady (EÚ) 2022/868 o európskej správe údajov („European Data Governance Act“)[57] do praxe. Toto nariadenie sa snaží zvýšiť dôveru v zdieľanie údajov, posilniť mechanizmy na zvýšenie dostupnosti údajov a prekonať technické prekážky opakovaného použitia údajov. Navyše podporí aj zriadenie a rozvoj spoločných európskych dátových priestorov v strategických oblastiach, do ktorých budú zapojený súkromný aj verejný sektor, a to v odvetviach, ako sú zdravie, životné prostredie, energetika, poľnohospodárstvo, mobilita, financie, výroba, verejná správa a zručnosti. Platforma MOU implementuje tieto ciele do praxe (kapitola 4.3).

6.1 Cieľ 1: Zabezpečiť dôveryhodnosť údajov

Dôveryhodný údajov je údaj, u ktorého je vysoká miera istoty, že nebol nejakým spôsobom narušený, poškodený alebo pokazený, že k nemu nemá prístup niekto na to neoprávnený, a že nedošlo k jeho neoprávnenej alebo neodôvodnenej zmene.

PKI infraštruktúra slúži pre dátovú integritu pri vybavovaní životných situácií občanov a podnikateľov (kapitola 4.1.1.1). Podpisujú sa pomocou nej aj datasety, ktoré štátna správa poskytuje občanom a podnikateľom cez osobné úložisko v MOU (kapitola 4.1.1).

Autentifikácia a autorizácia pri vytváraní, zdieľaní a ďalších formách spracovania údajov sa riešia v dokumente 1.1.3 Štandardizácia pre bezpečnosť a ochranu osobných údajov, pseudonymizácii sa venuje dokument 1.1.5 Štandardizácia anonymizácie údajov.

V prípade zdieľania prelinkovaných údajov cez platformu MOU treba neustále aktualizovať implementáciu štandardov a knižníc podľa Linked Data Security Stack (Obrázok 5).

[57] Zdroj: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act, Dátum referencie: 31.03.2023

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

6.2 Cieľ 2: Zdieľať overiteľné údaje

Jednou z ciest, ako dosiahnuť tento cieľ, je implementovať štandardy Verifiable Credentials (kapitola 4.2.1) a Verifiable Presentation (kapitola 4.2.2) podľa implementácie v MOU (kapitola 4.3.5).

6.3 Cieľ 3: Poskytovať selektívne zdieľanie

Vďaka riešeniam, ktoré ľahko umožňujú selektívne zverejňovanie informácií („selective disclosure“), je nutné podporovať kultúru založenú na minimálnej výmene informácií potrebnej na posilnenie súkromia používateľov.

Na dosiahnutie tohto cieľa treba rozvíjať implementáciu VC aj so selective disclosure podľa Linked Data Security Stacku s cryptosuites podporujúcimi ZKP cez kryptografiu (Obrázok 5 a kapitola 4.2.3).

6.4 Cieľ 4: Umožniť tretím stranám zachovať si istotu o pôvode, pravosti a integrite predložených informácií

Treba rozlišovať prípady použitia, kedy je postačujúci self-signed dataset – tvrdenia podpísané od dotknutej osoby alebo iného subjektu (kapitola P3. Self signed), a kedy je potrebné transparentne zdieľať aj celý životný cyklus údajov od ich vzniku cez ich transformáciu, aktualizáciu až po zneplatnenie – odvolanie. Druhý prípad súvisí s implementáciou overiteľných procesov (kapitola 2.1.3) a dátovou integritou (kapitola 2.1.2). Základom implementácie je kvalifikovaná elektronická pečať či podpis (kapitola 4.1.1) a Verifiable Credentials a Presentation (kapitoly 4.2.1 a 4.2.2). Okrem toho treba priebežnú aktualizáciu implementácie štandardu Linked Data Integrity (kapitola 4.2.1).

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.

Contact us

Rudalf Sedmina

Partner

E rsedmina@kpmg.sk

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

www.kpmg.com

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© yyyy Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Document classification: KPMG Confidential

Tento projekt je podporený z Európskeho sociálneho fondu.