Príručka pre uplatňovanie GDPR vo vzťahu k Informačnému systému Manažment osobných údajov

Čo je to GDPR?

GDPR alebo po anglicky General Data Protection Regulation je európske nariadenie o ochrane osobných údajov, ktoré je platné pre všetky štáty Európskej únie a je priamo uplatniteľné pre každý štát Európskej únie.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Toto nariadenie vzniklo, aby sa stanovili spoločné požiadavky európskych štátov na správne a legitímne spracúvanie osobných údajov fyzických osôb tak, aby platilo v každom štáte rovnako. Nariadenie stanovuje všeobecné povinnosti, práva a požiadavky všetkých aktérov, ktorí sú zapojení do spracúvania osobných údajov v celom európskom priestore. Nariadenie reguluje voľný tok osobných údajov v Európskej únii a zároveň stanovuje, čo všetko spadá pod ochranu osobných údajov a čo už je vyňaté spod ochrany osobných údajov. Toto nariadenie bolo aj priamo transponované do slovenského právneho poriadku v podobe zákona *č. 18/ 2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov*. Od dátumu účinnosti tohto zákona od 25. mája 2018 bol dvakrát zákon novelizovaný, naposledy v roku 2021, keď novelou zákona boli osobné údaje zosnulých osôb na Slovensku vyňaté spod ochrany osobných údajov.

Predmety a ciele

Cieľom GDPR je stanoviť jednotné zásady a pravidlá ochrany osobných údajov pre jednotlivé členské štáty Európskej únie. Zároveň nariadenie zabezpečuje voľný tok osobných údajov a vymedzuje hranice spracúvania osobných údajov. Poskytuje legislatívne útočisko pre všetky fyzické osoby v oblasti ochrany ich osobných údajov a uplatňovania svojich základných práv a slobôd v medziach ochrany osobných údajov. Vznikom GDPR sa zabránilo rozdielom, ktoré by mohli vznikať pri ochrane osobných údajov fyzických osôb.

Obsah GDPR

- KAPITOLA I – Všeobecné ustanovenia
    - (Článok 1 – Predmet úpravy a ciele, 2 – Vecná pôsobnosť, 3 – Územná pôsobnosť, 4 – Vymedzenie pojmov)

- KAPITOLA II – Zásady
- KAPITOLA III – Práva dotknutej osoby
    - Oddiel 1 – Transparentnosť a postupy
    - Oddiel 2 – Informácie a prístup k osobným údajom
    - Oddiel 3 – Oprava a vymazanie
    - Oddiel 4 – Právo namietať a automatizované individuálne rozhodovanie
    - Oddiel 5 – Obmedzenia
- KAPITOLA IV – Prevádzkovateľ a sprostredkovateľ
    - Oddiel 1 – Všeobecné povinnosti
    - Oddiel 2 – Bezpečnosť osobných údajov
    - Oddiel 3 – Posúdenie vplyvu na ochranu údajov a predchádzajúca konzultácia
    - Oddiel 4 – Zodpovedná osoba
    - Oddiel 5 – Kódexy správania a certifikácia
- KAPITOLA V – Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám
- KAPITOLA VI – Nezávislé dozorné orgány
    - Oddiel 1 – Nezávislé postavenie
    - Oddiel 2 – Príslušnosť, úlohy a právomoci
- KAPITOLA VII – Spolupráca a konzistentnosť
    - Oddiel 1 – Spolupráca
    - Oddiel 2 – Konzistentnosť
    - Oddiel 3 – Európsky výbor pre ochranu údajov
- KAPITOLA VIII – Prostriedky nápravy, zodpovednosť a sankcie
- KAPITOLA IX – Ustanovenia o osobitných situáciách spracúvania
- KAPITOLA X – Delegované akty a vykonávacie akty
- KAPITOLA XI – Záverečné ustanovenia

[Zdroj: *https://sk.wikipedia.org/wiki/V%C5%A1eobecn%C3%A9_nariadenie_o_ochrane_%C3%BAdajov*]

Osobné údaje podľa GDPR

Čo sa rozumie pod pojmom osobný údaj

Osobné údaje sú všetky informácie, ktoré sa týkajú **identifikovanej alebo identifikovateľnej osoby**. Rôzne útržky informácií, ktoré po spojení môžu viesť k identifikácii konkrétnej osoby, takisto predstavujú osobné údaje.

Osobné údaje, ktoré boli **odidentifikované**, zašifrované alebo **pseudonymizované**, ale možno ich použiť na opätovnú identifikáciu osoby, zostávajú osobnými údajmi a patria do rozsahu pôsobnosti GDPR.

Osobné údaje, ktoré boli **anonymizované** takým spôsobom, že jednotlivca viac nemožno identifikovať, sa viac nepovažujú za osobné údaje. Na to, aby údaje boli skutočne anonymizované, musí byť anonymizácia nezvratná.

GDPR chráni osobné údaje **bez ohľadu na technológiu použitú na spracovanie týchto údajov**. Sú teda technologicky neutrálne a pokiaľ sú údaje organizované podľa vopred vymedzených kritérií (napr. v abecednom poradí), tak sa uplatňujú na automatizované aj manuálne spracovanie. Nezáleží ani na tom, ako sa údaje ukladajú – či už v systéme IT, v bezpečnostnom kamerovom systéme alebo na papieri. Vo všetkých prípadoch osobné údaje podliehajú požiadavkám na ochranu definovaným v GDPR.

[Zdroj: *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_sk*]

Príklady osobných údajov

- meno a priezvisko
- domáca adresa
- e-mailová adresa, napr. *priezvisko@podnik.com*
- číslo preukazu totožnosti
- lokalizačné údaje (napr. funkcia lokalizačných údajov na mobilnom telefóne)*
- adresa internetového protokolu (IP)
- ID súboru cookie*
- reklamný identifikátor na vašom telefóne
- údaje, ktoré uchováva nemocnica alebo lekár, napr. to môže byť symbol, ktorý jedinečne identifikuje osobu

**Upozorňujeme, že v niektorých prípadoch existujú osobitné odvetvové právne predpisy, ktorými sa napr. riadi používanie lokalizačných údajov alebo používanie súborov cookies – smernica o súkromí a elektronických komunikáciách [smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 (Ú. v. ES L 201, 31.7.2002, s. 37) a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 z 27. októbra 2004 (Ú. v. ES L 364, 9.12.2004, s. 1)]*

[Zdroj: *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_sk*]

Príklady údajov, ktoré sa nepovažujú za osobné

- registračné číslo spoločnosti
- e-mailová adresa, napr. *info@podnik.com*
- anonymizované údaje

[Zdroj: *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_sk*]

Osobitné kategórie osobných údajov

Osobné údaje osobitej povahy sú typy osobných údajov, s ktorými sa musí narábať citlivo a smú sa spracúvať iba podľa osobitných výnimiek, ktoré GDPR stanovuje v článku 9 ods. 2. Napr. ak bol udelený výslovný súhlas alebo je spracúvanie potrebné z dôvodov významného verejného záujmu na základe práva EÚ alebo vnútroštátneho práva.

Sú to údaje o:

- rasovom alebo etnickom pôvode
- sexuálnej orientácii
- politických názoroch
- náboženských alebo filozofických presvedčeniach
- členstve v odborových organizáciách
- genetických, biometrických alebo zdravotných informáciách

Ďalej sú samostatnou kategóriou osobné údaje citlivej povahy podľa čl. 10 GDPR, ktoré sa môžu spracúvať len pod kontrolou orgánov verejnej moci alebo ak je to povolené právom EÚ alebo vnútroštátnym právom.

Sú to údaje o:

- uznaní viny za trestné činy a priestupky

[Zdroj: *https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_sk.htm*]

Vysvetlenie a kontext GDPR v oblasti verejnej správy

Analýza súčasného stavu reálnej implementácie právnych noriem týkajúcich sa bezpečnosti a oprávnenosti manipulácie s údajmi v informačných systémoch verejnej správy

a. Právna norma
   - Pripravovaný zákon o údajoch a o zmene a doplnení niektorých zákonov; zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
   - Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
   - Zákon č. 18/2018 Z. z. o ochrane osobných údajoch a o zmene a doplnení niektorých zákonov
   - Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
   - Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
   - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
   - Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
   - Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
   - Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/ 2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
   - Vyhláška Národného bezpečnostného úradu č 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení:
     - organizácia informačnej bezpečnosti
     - riadenie aktív, hrozieb a rizík
     - personálna bezpečnosť
     - riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov
     - technické zraniteľnosti systémov a zariadení
     - riadenie bezpečnosti sietí a informačných systémov

        - riadenie prevádzky
        - riadenie prístupov
        - kryptografické opatrenia
        - riešenie kybernetických bezpečnostných incidentov
        - monitorovanie, testovanie bezpečnosti a bezpečnostné audity
        - fyzická bezpečnosť a bezpečnosť prostredia
        - riadenie kontinuity procesov
b. Technická norma
    - Norma ISO 27000 – Systém manažérstva informačnej bezpečnosti pre splnenie právnych, regulačných a zmluvných úloh
    - Norma ISO 29100 – Bezpečnostné techniky
c. Organizačná norma

Povinnosti a zodpovednosti prevádzkovateľa a sprostredkovateľa

a. Analýzy rozdielov (audit)
b. Návrh implementácie (implementačný plán)
    - Definovať, čo prevádzkovateľ už má a vyhodnocovať, čo prevádzkovateľ plní
        - aké požiadavky prevádzkovateľ plní (súlad)
        - akým spôsobom dané požiadavky plní
        - aké požiadavky prevádzkovateľ neplní / nesprávne plní (nesúlad)
        - aké požiadavky prevádzkovateľ plní nedostatočne (čiastočný súlad)
c. Povinnosti a zodpovednosti prevádzkovateľa
    - Základné zásady spracúvania osobných údajov
    - Právne základy spracúvania osobných údajov
    - Test proporcionality
    - Informačné povinnosti
    - Práva dotknutých osôb
    - Záujmy, základné práva a slobody fyzických osôb
    - Bezpečnosť a ochrana osobných údajov (privacy by default / design)
    - Zmluvné vzťahy (spoloční prevádzkovatelia, sprostredkovateľ)
    - Záznamy o spracovateľských činnostiach
    - Oznámenie porušenia ochrany osobných údajov
    - Posúdenie vplyvu na ochranu údajov (DPIA)
    - Vymenovanie zodpovednej osoby (DPO)
    - Prenosy do tretích krajín a medzinárodným organizáciám
d. Povinnosti a zodpovednosti sprostredkovateľa
    - Povinnosti pre sprostredkovateľa vyplývajú zo zmluvy (čl. 28 ods. 3 GDPR)
    - Viesť záznamy o spracovateľských činnostiach
    - Prijať primerané bezpečnostné opatrenia (organizačné a technické opatrenia)
    - Oznámenie porušenia ochrany osobných údajov
    - Vymenovanie zodpovednej osoby (DPO)
    - Prenosy osobných údajov do tretích krajín a medzinárodným organizáciám

Povinnosť posúdenia vplyvu na ochranu údajov (DPIA)

Prevádzkovateľ má povinnosť vypracovať DPIA, ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania, pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, a to najmä, ak ide o:

a. Systematické a rozsiahle hodnotenie FO (aut. sprac. a profilovanie)
b. Spracúvanie osobitných kategórii osobných údajov vo veľkom rozsahu
c. Systematické monitorovanie verejných miest (veľký rozsah)
d. Zoznam spracovateľských operácií podliehajúcich požiadavke na posúdenie vplyvu na ochranu údajov čl. 35 ods. 4 GDPR (13 spracovateľských operácií)
    - Spracúvanie biometrických údajov FO na účely individuálnej identifikácie FO v spojení aspoň s jedným kritériom uvedeným v usmerneniach
    - Spracúvanie genetických údajov FO v spojení aspoň s jedným kritériom uvedeným v usmerneniach
    - Spracúvanie lokalizačných údajov v spojení aspoň s jedným kritériom uvedeným v usmerneniach
    - Spracovateľské operácie vykonávané podľa čl. 14 GDPR (ak je daná výnimka podľa čl. 14 ods. 5 písm. b) až d) GDPR, v spojení aspoň s jedným kritériom uvedeným v usmerneniach)
    - Hodnotenie alebo prideľovanie bodov (vplyv výsledku na poskytnutie alebo kvalitu služby)
    - Posúdenie dôveryhodnosti (systematické hodnotenie osobných údajov alebo hodnotenie osobných údajov vo veľkom rozsahu)
    - Posúdenie platobnej schopnosti (systematické hodnotenie osobných údajov alebo hodnotenie osobných údajov vo veľkom rozsahu)
    - Profilovanie (systematické hodnotenie osobných údajov)
    - Monitoring práce zamestnanca na základe vážnych dôvodov vyplývajúcich z osobitnej povahy činnosti zamestnávateľa (systematické monitorovanie + zraniteľných osôb)
    - Spracúvanie osobných údajov na účely vedeckého alebo historického výskumu bez súhlasu dotknutej osoby v spojení aspoň s jedným kritériom uvedeným v usmerneniach
    - Spracovateľské operácie využívajúce nové alebo inovatívne technológie v spojení aspoň s jedným kritériom uvedeným v usmerneniach
    - Systematické kamerové monitorovanie verejných priestorov (v jednotlivých mestách, obciach a dopravcami mestskej a prímestskej verejnej dopravy)
    - Sledovanie osôb súkromnými detektívnymi, resp. bezpečnostnými službami

Prevádzkovateľ má ďalšie povinnosti v súvislosti so spracúvaním osobných údajov:

a. Testy proporcionality v prípade, že koná na základe oprávneného záujmu
b. Informačné povinnosti (aj spôsob plnenia zásady transparentnosti)
c. Súhlasy so spracúvaním osobných údajov (aj spôsob získavania)

d. Zoznam sprostredkovateľov (aj spôsob ich identifikácie, vyhodnocovania primeraných záruk, kontrola a audit)
e. Zmluvné dojednania (náležitosti, realizácia v praxi)
f. Politika ochrany osobných údajov (napr. internou smernicou o ochrane osobných údajov)
g. Záznamy o spracovateľských činnostiach (aj porovnanie so zoznamom procesov)
h. Plán vzdelávania
i. Bezpečnostné role
j. Rozdelenie práv, povinností a zodpovedností, určenie sprostredkovateľov
k. Nástup a výstup zamestnanca, disciplinárne konanie
l. Spôsob oboznamovania sa s bezpečnostnými politikami, pokynmi

Plány kontinuity činností (RPO, RTO, krízové scenáre)

Rola Zodpovednej osoby (DPO alebo „Data Protection Officer“) a vymedzenie jej kompetencií v organizácii

Aké povinnosti má zodpovedná osoba pre oblasť ochrany osobných údajov?

Zodpovedná osoba pre oblasť ochrany osobných údajov je zodpovedná za monitoring súladu spracúvania s GDPR a ostatnými právnymi predpismi v oblasti ochrany údajov a za zvyšovanie povedomia o ochrane osobných údajov v organizácii.

Zodpovedná osoba pomáha prevádzkovateľovi so všetkými otázkami, ktoré sa týkajú ochrany osobných údajov a radí prevádzkovateľovi ohľadom všetkých situácií súvisiacich s ochranou osobných údajov.

Zodpovedná osoba:

- poskytuje informácie a poradenstvo prevádzkovateľovi aj zamestnancom
- poučuje zamestnancov o ich právach a povinnostiach pri spracúvaní podľa právnych predpisov o ochrane osobných údajov
- monitoruje, či organizácia pri spracúvaní dodržiava súlad so všetkými právnymi predpismi týkajúcimi sa ochrany osobných údajov
- vykonáva činnosti na zvyšovanie povedomia či odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií, napr. formou vzdelávacích aktivít
- poskytuje poradenstvo pri vykonávaní posúdenia vplyvu na ochranu údajov a monitoruje jeho vykonávanie
- funguje ako kontaktné miesto pre žiadosti dotknutých osôb týkajúcich sa spracúvania ich osobných údajov a výkonu ich práv
- spolupracuje s Úradom na ochranu osobných údajov Slovenskej republiky a pôsobí ako kontaktné miesto pre tento úrad v otázkach týkajúcich sa spracúvania

Zodpovednú osobu musí organizácia zapojiť dostatočne včas a poskytnúť jej podporu, zdroje a prístup k osobným údajom, aby mohla riadne vykonávať svoju činnosť. Zodpovedná osoba nesmie k výkonu svojich úloh dostávať žiadne pokyny. Zodpovedná osoba sa zodpovedá priamo najvyššej úrovni riadenia organizácie a v mnohých ohľadoch má nezávislé postavenie.

Kedy musí mať organizácia zodpovednú osobu (DPO)?

Na Slovensku nie je automaticky všeobecná povinnosť vymenovať zodpovednú osobu v každej organizácii. Organizácia musí vymenovať zodpovednú osobu vždy, ak spracúvanie vykonáva **orgán verejnej moci,** či verejný subjekt (z povinnosti sú vyňaté súdy). Ďalej musí mať organizácia zodpovednú osobu, ak spracúva **osobné údaje osobitnej kategórie vo veľkom rozsahu** (osobné údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby) alebo ak medzi hlavné činnosti organizácie patrí **rozsiahle, pravidelné a systematické monitorovanie** dotknutých osôb.

Zodpovedná osoba musí byť vymenovaná na základe jej odborných kvalít, pričom nie je nutné, aby bola špecialistom na bezpečnosť alebo aby mala vzdelanie dosiahnuté v tejto oblasti. Kontaktné údaje zodpovednej osoby musia byť vždy poskytnuté Úradu na ochranu osobných údajov Slovenskej republiky.

Aj keď organizácii nevyplýva povinnosť vymenovať zodpovednú osobu, môže sa organizácia rozhodnúť vymenovať ju dobrovoľne.

Zodpovedná osoba môže byť zamestnanec danej organizácie alebo sa môže s jednotlivcom uzavrieť externá dohoda na základe zmluvy o poskytovaní služieb. Organizácia môže mať jednu aj viac zodpovedných osôb.

PRÍKLADY:

Zodpovedná osoba **je** povinná, napríklad keď spoločnosť/organizácia:

- je zdravotnícke stredisko, ktorá spracúva rozsiahle súbory osobných údajov o zdraví
- je bezpečnostnou spoločnosťou zodpovednou za monitorovanie nákupných stredísk a verejných priestorov
- je malou personálnou agentúrou, ktorá profiluje jednotlivcov (monitoruje správanie dotknutých osôb na internete napr. na účely reklamy, ktorá je potom odvodená od výsledkov správania jednotlivcov)

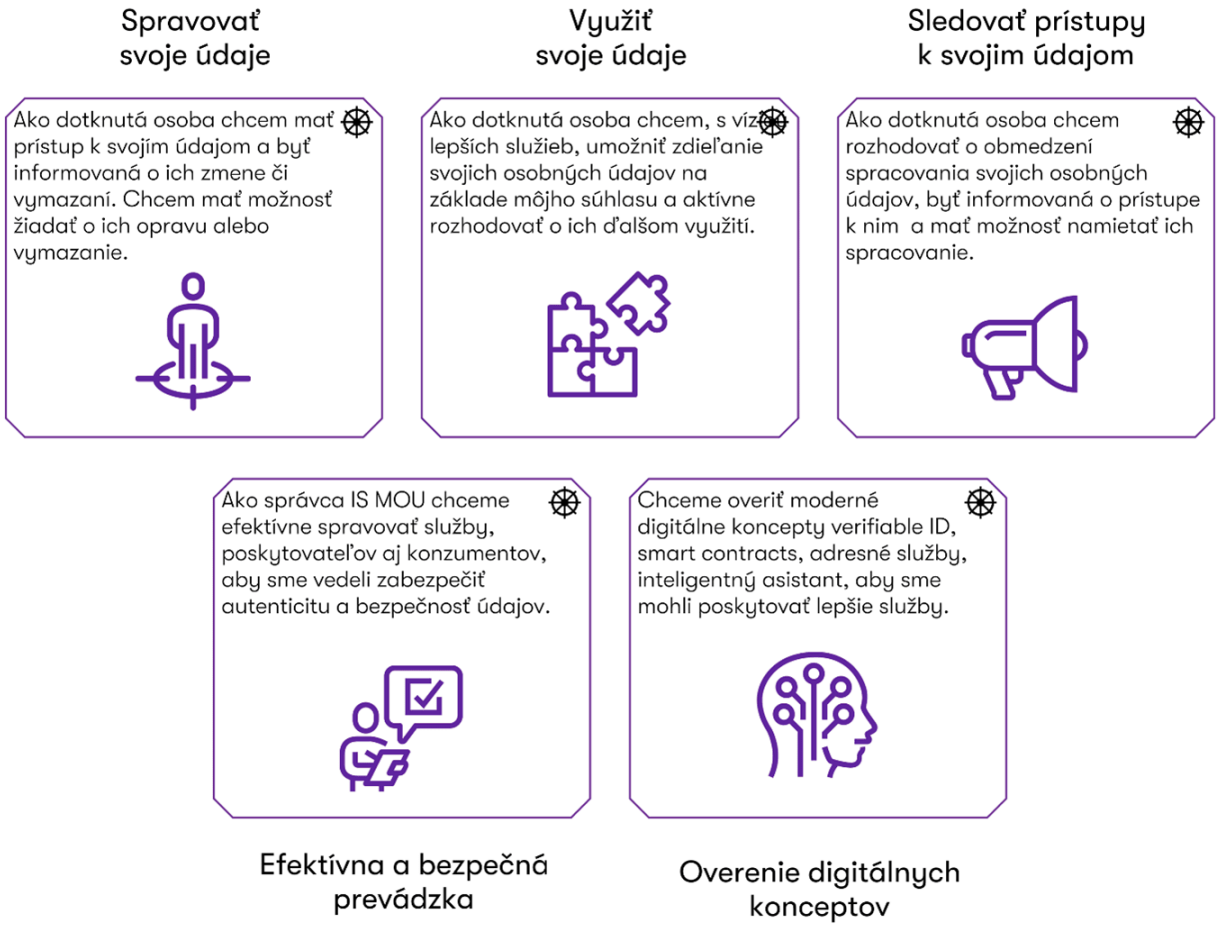
Zodpovedná osoba **nie je** povinná, ak ide o:

- miestneho obvodného lekára, ktorý spracúva osobné údaje svojich pacientov v malom rozsahu
- malú právnickú firmu, ktorá spracúva osobné údaje svojich klientov v malom rozsahu

Koncept MOÚ a jeho uplatňovanie pri ochrane osobných údajov

Ciele MOÚ

Ciele MOÚ môžeme rozdeliť do nasledovných oblastí:



Spravovať svoje údaje znamená, že dotknutá osoba priamo v aplikácii vidí, aké údaje sú o nej evidované v jednotlivých informačných systémoch VS. Ako príklad môžeme uviesť, že občan uvidí presný záznam, ktorý je o ňom evidovaný v Registri fyzických osôb.

Využiť svoje údaje je oblasť, ktorá do budúcna ponúka veľké možnosti. Vďaka službám z tejto oblasti môže dotknutá osoba svoje údaje využiť nie len v rámci verejnej správy, ale na základe jej súhlasu môžu byť údaje poskytnuté tretím stranám, ktoré môžu na nich budovať kvalitnejšie a komfortnejšie služby. Napríklad pri schvaľovaní úveru občan nemusí nosiť rôzne potvrdenia.

Banka, na základe občanovho súhlasu, dostane údaje ktoré potrebuje, napríklad daňové priznanie.

Oblasti Spravovať a využiť svoje údaje sú zamerané na získanie, poskytovanie a správu údajov. Tretia oblasť **Sledovanie prístupov** slúži na informovanie dotknutej osoby o prístupoch k osobným údajom.

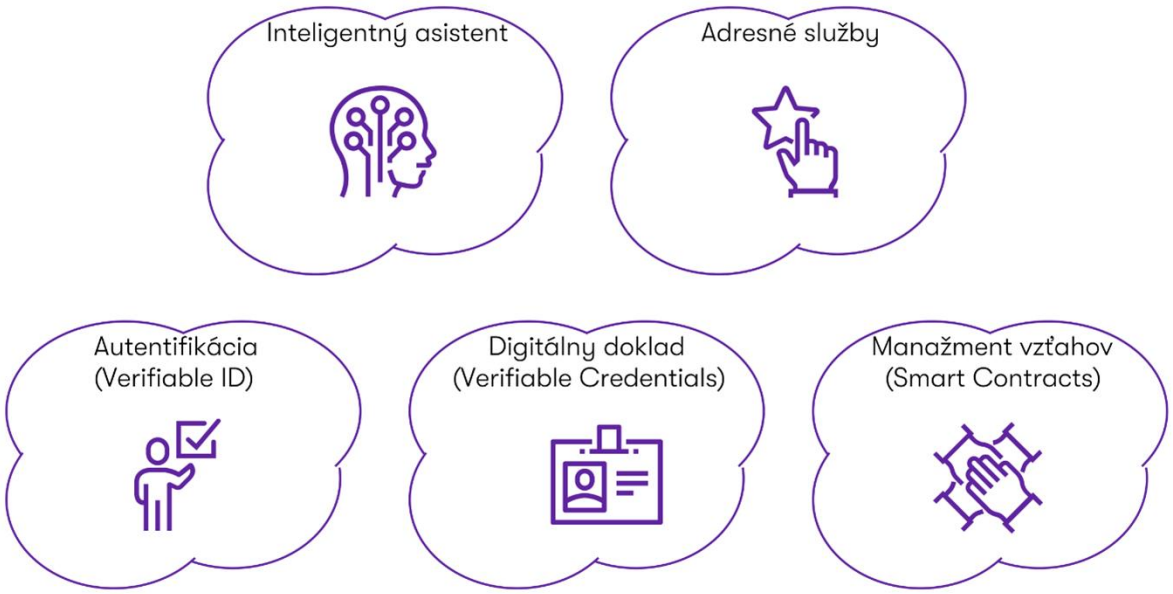
Hovoríme o týchto základných scenároch:

- *Spracovanie osobných údajov* – napríklad, úradník si pozrie osobné údaje na karte dotknutej osoby. Ďalším príkladom môže byť spracovanie osobných údajov dotknutej osoby pri vybavovaní žiadosti. Cieľom nie je obmedzovať spracovávanie osobných údajov, naopak IS MOÚ podporuje budovanie služieb založených na efektívnom využívaní osobných údajov, ale chceme zabezpečiť, aby dotknutá osoba bola o spracovaní osobných údajov informovaná.
- *Zmena osobných údajov* – typickým príkladom je zmena adresy. Pod zmeny osobných údajov zahrnieme aj vznik a vymazanie osobných údajov. Zdôraznime, že úlohou modulu Logovanie prístupov nie je prenos samotných zmenených údajov (ten zabezpečuje modul Správa osobných údajov), ale iba získanie informácie o tejto zmene. To znamená, že aj informačný systém, ktorý nepodporuje zasielanie zmien údajov, môže podporiť zasielanie informácie o zmene údajov.
- *Prenos osobných údajov* – prenos medzi OVM, prenos zo zdrojového OVM do osobného úložiska dotknutej osoby a poskytnutie osobných údajov z osobného úložiska tretej strane na základe súhlasu.

Všetky tieto scenáre sú pre občana užitočné a MOÚ nemá "strážiť", ani brániť využívaniu osobných údajov, len má dotknuté osoby informovať, vždy keď to nastane.

Oblasť **Efektívna a bezpečná prevádzka** pokrýva správu služieb MOÚ, poskytovateľov, konzumentov údajov a používateľov MOÚ.

Posledná oblasť **Overenie digitálnych konceptov** si kladie za cieľ overiť moderné digitálne koncepty, či integráciu s projektami na európskom meradle. Ak sa ukážu užitočné, môžu na ich základe vzniknúť samostatné projekty.



V rámci projektu dôjde k overeniu nasledujúcich konceptov:

- *Inteligentný asistent*: je možné navrhnúť asistenta, ktorý pomáha používateľovi vybavovať jeho interakciu zo štátom?
- *Adresné služby*: dokáže verejná správa personalizovať svoju ponuku tak, aby sa používateľskou skúsenosťou priblížila k súkromnému sektoru?
- *Autentifikácia*: odskúšanie konceptu a demonštrovanie možností použitia nových, nastupujúcich technológii , konkrétne tzv. "European Self Sovereign Identity", ktorý je postavený na Blockchain technológii pre autentifikáciu a občanov k službám komerčných subjektov alebo štátu.
- *Digitálne doklady*: využiť osobné úložisko na uchovávanie digitálnych dokladov (ako sú občiansky preukaz, pas, vodičský preukaz) ako digitálny, overiteľný dokument ("Verifiable Credentials").
- *Manažment vzťahov*: overiť riešenie udeľovania splnomocnení a zastupovania prostredníctvom služby Moje dáta, vrátane možností, ktoré prinášajú takzvané "smart contracts".

Vízia projektu MOÚ

Štát prostredníctvom projektu MOÚ dáva dotknutej osobe nástroj na praktickú **realizáciu jej práv, ktoré vychádzajú z nariadenia GDPR, vo vzťahu k jej údajom, ktoré sú o nej spravované verejnou správou**. Formálne práva občanov v oblasti ochrany osobných údajov, ktorých vymáhanie je často náročné a zdĺhavé, budú jednoducho realizovateľné elektronicky „na jedno kliknutie“ nástrojmi pre:

- **získanie prístupu k svojim osobným údajom spravovaných verejnou správou** (právo na prístup k údajom)
- **monitorovanie prístupu k týmto údajom** (právo na informáciu, kto k mojim osobným dátam pristupoval)
- **monitorovanie zmien osobných údajov** (oznamovacia povinnosť pri oprave či výmaze dát)
- **namietanie ich spracovania** (právo na obmedzenie spracovania, právo namietať)
- **zabezpečenie práva na opravu či výmaz údajov** (právo na opravu a vymazanie)

MOÚ umožní dotknutej osobe svoje údaje zdieľať a rozhodovať o ich ďalšom využití za jasne definovaných podmienok. Dotknutá osoba bude môcť svoje osobné údaje spravované verejnou správou poskytnúť tretím stranám prostredníctvom otvoreného aplikačného rozhrania v podobe vhodnej na strojové spracovanie (právo na prenosnosť údajov).

Dotknuté osoby tak budú môcť, pomocou zrozumiteľných elektronických nástrojov, kontrolovať čo sa s ich údajmi spravovanými štátom deje a zároveň rozhodovať o ďalšom využití svojich údajov.

Očakávame, že to prinesie **vznik nových kvalitných služieb**, ktoré dotknutým osobám zjednodušia život a odbremenia ich od nepotrebnej byrokracie. Zároveň sa zaväzujeme, že systém bude napojený na dátové zdroje, a že v rámci projektu vybrané služby zrealizujeme. Zameriame sa na scenáre, kde je poskytovateľom údajov verejná správa. Ak sa ukážu konkrétne atraktívne scenáre, kde je poskytovateľom tretia strana, technicky bude pre nich cesta vytvorená a do budúcna ich treba rozpracovať a zvážiť ako nasledujúce iniciatívy.

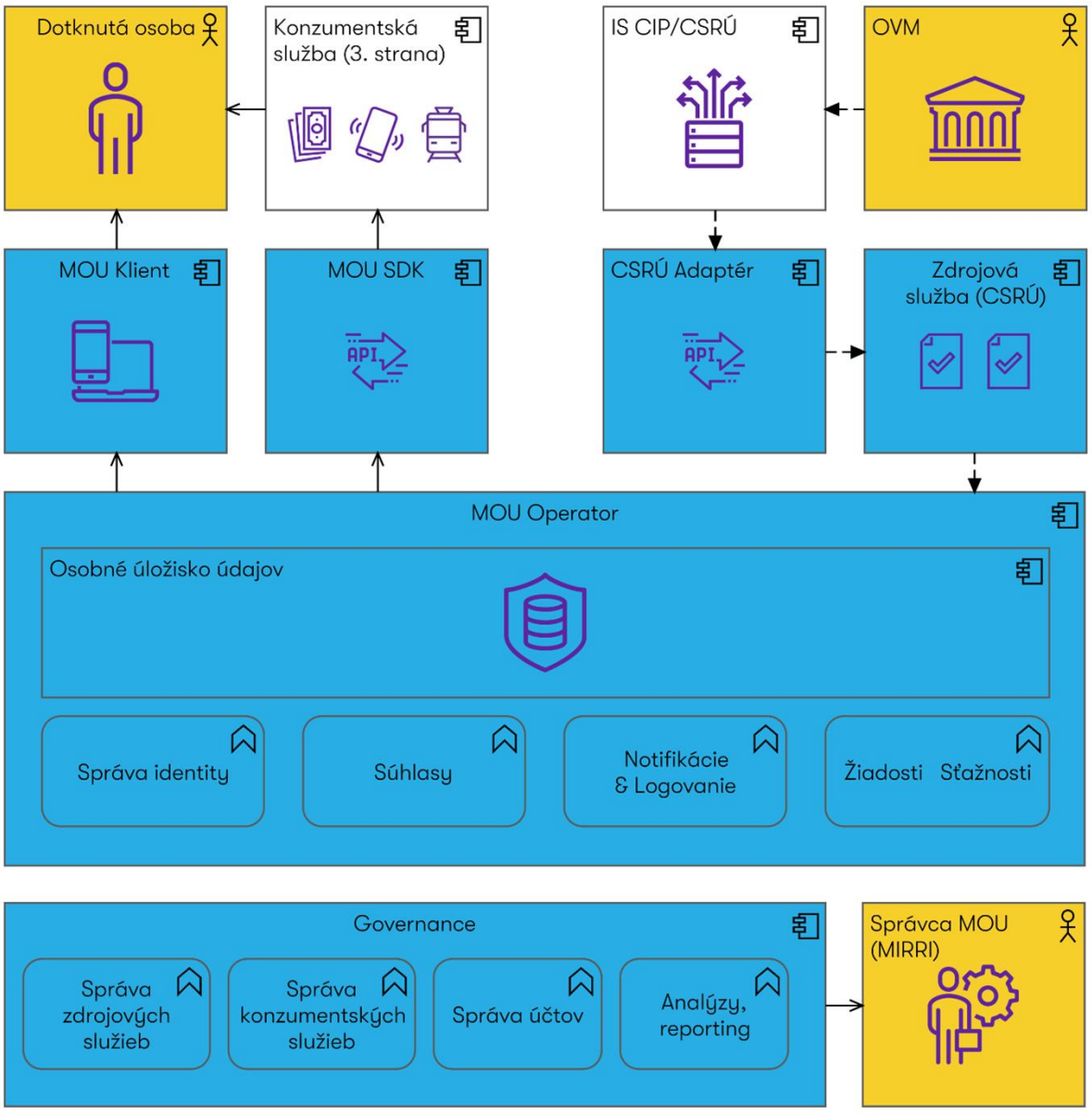
MIRRI, ako správca IS MOÚ, čiže špecifickej informačnej technológie, ktorá je súčasťou centrálnej informačnej technológie verejnej správy, bude **zodpovedať za autenticitu** zdrojov týchto údajov, za poskytnutie iba údajov, na ktoré dala dotknutá osoba súhlas, za konzistentnosť a integritu údajov a za bezpečnosť prenosu údajov. Systém je navrhnutý tak, aby celý proces bol pre používateľa zrozumiteľný, jednoduchý a nevyžadoval zbytočné kroky.

Projekt sa primárne zameriava na služby v rámci Slovenska. Snahou je, aby občania Slovenska mali plnohodnotné možnosti v rámci Európskej únie. Navrhnuté riešenie je v maximálnej miere interoperabilné a založené na medzinárodných štandardoch a skúsenostiach. Projekt implementuje princípy MyData.org a má ambíciu predstaviť vhodné riešenie pre implementáciu budúcich dátových politík na úrovni EÚ. Slovensko sa tak stane vzorovou krajinou pre správu mojich údajov vo verejnej správe.

Služby poskytované MOÚ

	(A) Spravovať svoje údaje	(B) Sledovať prístupy k svojim údajom	(C) Využiť svoje údaje	(E) Efektívna a bezpečná prevádzka
Občan	Získanie údajov do osobného úložiska Prezeranie údajov Žiadosti o opravy a výmaz údajov	Sledovanie používania údajov Prezeranie histórie prístupov k údajom Žiadosti o vysvetlenia prístupu k údajom	Poskytovanie údajov tretím stranám Správa súhlasov	Občan spravuje svoj účet v MOÚ
MIRRI	Registrácia a správa služieb poskytovateľov údajov		Registrácia a správa služieb tretích strán	Správa účtov Správa kanonického modelu Kompozitné a „zero knowledge proof“ služby Správa šablón Reporty
Tretie strany		Logovanie o prístupe k osobným údajom	Registrácia a správa služieb treťou stranou	Tretia strana spravuje svoj účet v MOÚ Podpora prevádzky služieb tretích strán

Koncept architektúry



Na obrázku sú žltou farbou znázornení základní aktéri, modrou farbou komponenty dodávané v rámci projektu MOÚ a bielou farbou sú znázornené externé komponenty (z pohľadu IS MOÚ), s ktorými sa MOÚ integruje.

Dotknutá osoba – autentifikovaný používateľ MOU, vlastník účtu MOU – využíva mobilnú alebo webovú aplikáciu **MOU Klienta,** pomocou ktorej pristupuje k službám MOU. V aplikácii vidí svoje údaje, spravuje súhlasy, sleduje využívanie svojich údajov.

Dotknutá osoba využíva **Služby tretích strán** – aplikácie tretích strán, mimo verejnej správy SR, ktoré po zaregistrovaní služby v MOU, na základe súhlasu dotknutej osoby, spracovávajú jej údaje a vďaka tomu poskytujú lepšie služby.

Orgán verejnej moci (**OVM**) spravuje a poskytuje osobné údaje. Vystupuje v roli poskytovateľa údajov, je napojený na **IS CIP/CSRÚ**, ktorý centrálne zabezpečuje komunikáciu medzi MOU a OVM. MOU pomocou **CSRÚ Adaptéru** kkomunikuje s IS CIP/CSRÚ. Zdrojová služba získava osobné údaje, ukladá ich do úložiska, rozdeľuje na atomické datasety a podobne.

Služby tretích strán sú aplikácie tretích strán registrovaných v MOU, ktoré na základe jej súhlasu spracovávajú jej údaje. Napríklad sú to služby banky, ktorá pomocou MOU získava údaje z daňového priznania pri poskytovaní hypotéky. Služby tretích strán komunikujú s MOU pomocou API, pre jednoduchosť je možnosť použiť aj MOU SDK.

Osobné údaje sú ukladané do **Osobného úložiska**, ktoré tvorí jadro **MOU Operátora**. Osobné úložisko je súčasťou vládneho cloudu. Každá dotknutá osoba prihlásená do MOÚ má v ňom vytvorený svoj vlastný priestor, kde sa ukladajú jej dáta v zašifrovanej podobe tak, že má k nim prístup iba vlastník účtu (dotknutá osoba), ani administrátor MOU ich nemôže vidieť. Tieto údaje sú, so súhlasom dotknutej osoby, potom poskytované tretím stranám so zaregistrovanými službami. Služba je postavená na Solid Community Server s rozšíreniami pre MOU. Osobné úložisko sa vytvára aj pre jednotlivé služby a operátora. Služby majú v úložisku uložené napríklad consenty – technický záznam o súhlase spracovania údajov službou

MOU Operator zabezpečuje správu identít/účtov, registráciu služieb tretích strán a pripojenie služieb tretích strán k používateľovi, správu súhlasov, notifikácie a logovanie, podávanie a sledovanie stavu sťažností a návrhov na opravu osobných údajov zastrešuje správu účtov, identít, súhlasy občana, manažment notifikácií a sťažností.

Governance pre správu celého MOÚ s funkciami ako odsúhlasenie dátových setov zdrojov dát a služieb tretích strán. Zároveň poskytuje analýzy a reporty využívania MOU. Ako správca MOU vystupuje MIRRI.

Využitie MOÚ v súlade s nariadením GDPR

Prínosy MOÚ pre OVM v oblasti plnenia GDPR

Orgány verejnej moci (OVM), spravujúce informačné systémy s osobnými údajmi občanov, musia plniť požiadavky GDRP.

Implementácia riešenia pre splnenie technických podmienok GDPR, je úloha náročná na zdroje. Pre OVM je výhodné využiť integráciu s Manažmentom osobných údajov (MOÚ), ktorá umožní preukázateľne splniť požiadavky GDPR, z hľadiska zásad spracúvania osobných údajov, ale aj bezpečnosti, integrity, hodnovernosti, či aktuálnosti dát.

Minimalizácia

Prevádzkovateľ IS VS spracúva iba osobné údaje dotknutých osôb v rozsahu nevyhnutnom na dosiahnutie stanoveného účelu. Inými slovami, rozsah osobných údajov je zminimalizovaný iba na tie osobné údaje, ktoré OVM potrebuje na splnenie zákonom daných úloh.

MOÚ umožňuje využiť minimalizáciu pri prenose údajov tretím stranám

Dostupnosť

- Získanie prístupu k evidovaným osobným údajom
- Získanie prístupu k informáciám o spracúvaní osobných údajov

Dostupnosťou sa rozumie povinnosť prevádzkovateľa IS VS zabezpečiť informačné systémy takými organizačno-technickými prostriedkami, aby sa v prípade potreby dalo vždy k osobným údajom bez problémov dostať vo chvíli, keď daný údaj dotknutá osoba požaduje.

Každý občan má právo na prístup k evidovaným osobným údajom a tiež informáciám o spracúvaní osobných údajov. OVM musí občanovi na požiadanie poskytnúť kópiu jeho osobných údajov.

MOÚ umožňuje získať prístup k osobným údajom dotknutej osoby touto dotknutou osobou, a tiež umožňuje získať informácie o ich spracúvaní

Integrita

- Zaručenie integrity osobných údajov

Integrita zaručuje, že osobné údaje dotknutých osôb sú v danom čase bezchybné, úplné, správne a aktualizované. Integritou sa tiež zabezpečuje, že nikto a nič zvonka nenaruší celistvosť osobných údajov.

MOÚ zaručuje integritu osobných údajov pri prenose tretím stranám

Dôvernosť

- Zaručenie dôvernosti pri spracúvaní osobných údajov

Dôvernosť v oblasti bezpečnosti spracúvania osobných údajov znamená, že prevádzkovateľ IS VS zabezpečí, aby sa k osobným údajom občanov dostali iba vybrané osoby na základe *„need to know basis“* – princípu, pri ktorom osobné údaje spracúva iba úzky okruh osôb, ktoré prístup k osobným údajom nevyhnutne potrebujú pre prácu a pre splnenie stanovených úloh a osoby, ktoré na splnenie úloh majú potrebnú odbornú úroveň znalostí.

MOÚ zabezpečí dotknutej osobe dôvernosť pri spracovaní jej osobných údajov

Nespojiteľnosť

- Šifrovanie dát kľúčom vlastníka
- Pseudonymizácia

Prevádzkovateľ IS VS aktívne nehodnotí dotknutú osobu na základe evidovaných osobných údajov.

Nespojiteľnosť sa v praxi často zabezpečí používaním pseudonymizácie.

MOÚ zabezpečí dotknutej osobe informovanie o spracovaní jej osobných údajov, umožní pseudonymizáciu pre praktické zabezpečenie nespojiteľnosti pri zdieľaní údajov s tretími stranami a osobné údaje zabezpečí šifrovaním vlastníka účtu

Transparentnosť

- Informovanie o spracúvaní osobných údajov
- Informovanie o zmenách v osobných údajoch

Prevádzkovateľ IS VS voči dotknutej osobe nič neskrýva; naopak odhaľuje všetky informácie o spracúvaní tak, aby boli ľahko dostupné. Prevádzkovateľ zabezpečuje, že informácie sú komplexné, prehľadné a neskreslené.

MOÚ zabezpečí informovanie dotknutej osoby o zmenách v jej údajoch, spracúvaní *jej údajov medzi OVM, poskytnutí údajov tretím stranám*

Intervencia

- Intervenovanie do spracovania osobných údajov
- Požiadanie o opravu alebo výmaz osobných údajov

Intervencia predstavuje akcie, ktoré činnosť spracúvania osobných údajov obmedzujú, korigujú alebo priamo zabránia v ďalšom spracúvaní.

Občan ako dotknutá osoba môže zakročiť: namietať, požiadať o vymazanie nesprávnych osobných údajov alebo vymazanie nepotrebných osobných údajov, ktoré sa už na daný účel nesmú spracúvať.

MOÚ umožní dotknutej osobe namietať spracovanie osobných údajov, alebo žiadať o ich opravu alebo vymazanie

Súčinnosť, spolupráca

- Spracúvanie údajov delegované na sprostredkovateľa
- Poskytnutie údajov tretej strane na základe aktívneho rozhodnutia dotknutej osoby

Súčinnosť znamená, že prevádzkovateľ IS VS pri spracúvaní osobných údajov nemusí konať bezvýhradne sám. Môže delegovať svoje právomoci na sprostredkovateľa alebo ich môže poskytnúť iným ďalším príjemcom. Každá takáto spolupráca musí byť s druhou stranou zmluvne viazaná alebo zakotvená právne záväzným aktom.

Dotknutá osoba sa môže rozhodnúť umožniť tretej strane prístupiť k jej údajom.

MOÚ zabezpečí informovanie dotknutej osoby o poskytnutí jej údajov medzi OVM. Dotknutá osoba má možnosť zdieľať svoje údaje s tretími stranami na základe vlastného rozhodnutia.

Checklist využitia MOÚ v súlade s pravidlami a odporúčaniami GDPR

	Minimalizácia	**Dostupnosť**	**Integrita**	**Dôvernosť**	**Nespojiteľnosť**	**Transparentnosť**	**Intervencia**	**Súčinnosť, spolupráca**
Články GDPR	5 (1) (c), 5 (1) (e),	5 (1) (e),	5 (1) (f),	5 (1) (f),	5 (1) (c), 5 (1) (e),	5 (1) (a),	5 (1) (d), 5 (1) (f),	
		13, 15,			17, 18,	13, 14, 15, 19,	13 (2) (c), 14 (2) (d), 15 (1) (e), 16, 17, 18,	
	25, 28, 29,	20, 25,	25,	25, 28 (3) (b), 29,	22, 25,	25,	20, 21, 22 (3), 25,	
	30, 32, 39	32,	32, 33, 34, 39,	32, 39,	32, 33,	30, 32, 33, 39,	32, 39,	31, 39,
		49,	49,	49,	40 (2) (d),	40, 42,		
					52	53, 58,	59,	50, 53,
						60, 61, 63,	65, 66, 68, 69,	60, 61, 62, 67, 68,
		78, 79,	78	78,		74, 78,	70, 78,	70, 78,
		86		83		84, 85, 86, 87,	83	
						90, 91		
MOÚ umožní	Spracovanie iba nevyhnutných osobných údajov	Získanie prístupu k evidovaným osobným údajom	Zaručenie integrity osobných údajov	Zaručenie dôvernosti pri spracúvaní osobných údajov	Šifrovanie dát kľúčom vlastníka	Informovanie o spracúvaní osobných údajov	Intervenovanie do spracovania osobných údajov	Poskytnutie údajov tretej strane na základe pokynu od dotknutej osoby
	Pseudonymizovanie osobných údajov	Získanie prístupu k informáciám o spracúvaní osobných údajov				Informovanie o zmenách v osobných údajoch	Požiadanie o opravu alebo výmaz osobných údajov	

Návrh odporúčaní pre inštitúcie vo verejnej správe, akým optimálnym spôsobom využiť službu Moje dáta pre plnenie požiadaviek GDPR

Orgány verejnej moci (OVM), spravujúce informačné systémy s osobnými údajmi občanov, musia plniť požiadavky GDRP.

Implementácia riešenia pre splnenie technických podmienok GDPR, je úloha náročná na zdroje. Pre OVM je výhodné využiť integráciu s Manažmentom osobných údajov (MOÚ), ktorá umožní preukázateľne splniť požiadavky GDPR, z hľadiska zásad spracúvania osobných údajov, ale aj bezpečnosti, integrity, hodnovernosti, či aktuálnosti dát.

1. Integrácia s Manažmentom osobných údajov (MOÚ)
    - MOÚ umožní preukázateľne splniť požiadavky GDPR
        - Minimalizácia
            - Spracovanie iba nevyhnutných osobných údajový
            - Pseudonymizovanie osobných údajov
        - Dostupnosť
            - Získanie prístupu k evidovaným osobným údajom
            - Získanie prístupu k informáciám o spracúvaní osobných údajov
        - Integrita
            - Zaručenie integrity osobných údajov
        - Dôvernosť
            - Zaručenie dôvernosti pri spracúvaní osobných údajov
        - Nespojiteľnosť
            - Šifrovanie dát kľúčom vlastníka
        - Transparentnosť
            - Informovanie o spracúvaní osobných údajov
            - Informovanie o zmenách v osobných údajoch
        - Intervencia
            - Intervenovanie do spracovania osobných údajov
            - Požiadanie o opravu alebo výmaz osobných údajov
        - Súčinnosť, spolupráca
            - Poskytnutie údajov tretej strane na základe pokynu od dotknutej osoby
        - Viac info na:
            - Prínosy MOÚ pre OVM v oblasti plnenia GDPR
            - Checklist využitia MOÚ v súlade s pravidlami a odporúčaniami GDPR
    - Pri registrácii uviesť kontakt na zodpovednú osobu za ochranu osobných údajov (DPO)
        - Venovať sa námietkam dotknutých osôb k spracúvaniu osobných údajov, žiadostiam o opravu v údajoch a ich vymazanie
2. Zdieľanie dát s inými OVM realizovať cez systém CSRÚ, aby dotknutá osoba mohla byť cez MOÚ informovaná, čo sa s jej dátami deje

Metodika zavádzania Mojich údajov vo verejnej správe

a. Vzorové riešenie pravidiel na ochranu osobných údajov
b. Zabezpečenie prístupu k evidovaným údajom subjektu cez službu „Moje údaje“
c. Implementácia práva na zabudnutie v prostredí verejnej správy
d. Metodika pre anonymizáciu a šifrovanie
e. Manažment zdieľania osobných údajov s tretími stranami
f. Checklist vhodnej implementácie GDPR vo VS
g. Politika ochrany údajov
h. Trvalá CIA a odolnosť systémov spracúvania a služieb
    - Zaistenie primeranej bezpečnosti osobných údajov a zariadení vrátane predchádzania neoprávnenému prístupu (neoprávnenému využitiu týchto osobných údajov a zariadení)
    - Dôvernosť – (miera obmedzenia prístupu k osobným údajom); vlastnosť, že osobné údaje nie sú prístupné neautorizovaným jednotlivcom, entitám alebo procesom (need-to-know)
    - Dostupnosť – (miera dostupnosti osobných údajov); vlastnosť zaisťujúca autorizovaným používateľom prístup k osobným údajom vtedy, keď to potrebujú
    - Integrita – (mera úplnosti a správnosti osobných údajov); vlastnosť, že osobné údaje nebudú pozmenené, poškodené alebo narušené neautorizovaným spôsobom
    - ODPORÚČANIE: zavedenie primeraných technických a organizačných opatrení
    - Obnova pre prípad incidentu
    - Rizikový prístup (riziká pre práva a slobody fyzických osôb a technické riziká)
    - Pravidelné testovanie, hodnotenie účinnosti opatrení
    - Minimalizácia uchovávania
        - Osobné údaje sa nemajú uchovávať dlhšie, než je to nevyhnutné na dosiahnutie účelu
        - ODPORÚČANIE: stanovenie lehôt na vymazanie alebo pravidelné preskúmanie
        - VÝNIMKA: archivácia vo verejnom záujme, vedecký alebo historický výskum, štatistické účely
i. Metodika pre tvorbu analýzy rizík
    - Identifikácia zraniteľností
    - Identifikácia hrozieb
    - Identifikácia a analýza rizík s ohľadom na aktívum
    - Určenie vlastníka rizika
    - Implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením
    - Analýza funkčného dopadu na činnosť prevádzkovateľa
    - Pravidelné preskúmavanie identifikovaných rizík a v závislosti od toho aktualizácia prijatých bezpečnostných opatrení

MANAŽMENT OSOBNÝCH ÚDAJOV

Definícia služby Moje údaje

Všeobecná charakteristika Mojich údajov v európskom priestore

Projekt implementuje princípy MyData.org a má ambíciu predstaviť vhodné riešenie pre implementáciu budúcich dátových politík na úrovni EÚ. Ambíciou je, aby sa Slovensko stalo vzorovou krajinou pre správu osobných údajov vo verejnej správe.

Všeobecná charakteristika Mojich údajov v národnom priestore

Národný projekt Manažment osobných údajov (ďalej len MOÚ) zhmotňuje po praktickej stránke tému „moje dáta“, v podobe nového IS modulu procesnej integrácie a integrácie údajov/národného systému zdieľania dát. Jednou z kľúčových priorít MIRRI v gescii dátovej kancelárie, je zabezpečiť modernú a efektívnu komunikáciu občana a podnikateľa so štátom, ale aj v rámci súkromnej sféry. Projekt MOÚ zabezpečí dostupnosť relevantných údajov fyzickej alebo právnickej osobe.

Očakávania a prínos pre SR v oblasti Mojich údajov

Hlavným cieľom projektu je vytvorenie prostredia, kde sa občan stane aktívnym správcom svojich dát, bude môcť o nich rozhodovať a využívať ich pre svoj prospech, v súlade s definovanými pravidlami. Realizáciou projektu sa zvýši dátová kvalita v informačných systémoch štátu a napomôže sa aplikácii princípu „jedenkrát a dosť“, čo zároveň povedie ku zníženiu byrokracie.

Popis služieb MOÚ

- Služby pre občana
  - Využiť svoje údaje
    - Nahrávanie a prezeranie údajov v osobnom úložisku
    - Udeľovanie súhlasov pre tretie strany
  - Spravovať svoje údaje
    - Žiadosti o opravu, vymazanie údajov
    - Žiadosť o vysvetlenie použitia údajov
    - Sťažnosť na použitie údajov
  - Sledovať prístupy k svojim údajom
    - Notifikácie a logy o použití osobných údajov
    - Notifikácie a logy o zmenách v osobných údajoch
- Služby pre MIRRI
  - Správa zdrojových služieb (poskytovatelia údajov)
  - Správa služieb tretích strán (konzumenti údajov)
- Služby pre tretie strany
  - Registrácia služby tretej strany
  - Vytvorenie a správa účtu tretej strany

Bezpečnosť prevádzky systému MOÚ

Prístup oprávnených osôb a zápis logovaného prístupu

- Služby vystavené navonok budú popísané OPEN API (Swagger).
- Prístup oprávnených osôb
- Zápis logovaného prístupu

Zaznamenávanie oprávneného/neoprávneného prístupu

- Notifikácie o prístupe k dátam

Opatrenia pre prípad neoprávneného prístupu k Mojim údajom

- Prenos dát prebieha pomocou REST volaní cez protokol HTTPS (šifrovaná komunikácia – certifikát bude vydaný dôveryhodnou certifikačnou autoritou)
- Dáta sú chránené pri uložení, ale aj pri prenose symetrickým šifrovaním
- Na prístup k službám je potrebná autentifikácia s použitím protokolu OAUTH 2.0.

Bezpečnosť spracúvaných dát

Povinnosťou prevádzkovateľa je zabezpečiť náležitú ochranu dát prijatím technických a organizačných opatrení.

Technické opatrenia

Fyzická bezpečnosť	**Neoprávnený prístup**	**Riadenie prístupov**	**Riadenie zraniteľností**	**Sieťová bezpečnosť**	**Zálohovanie**	**Likvidácia osobných údajov**
Mechanické zábranné prostriedky (napr. uzamykateľné dvere, okná, mreže) a aj technické zabezpečovacie prostriedky (napr. EZS, EPS)	Šifrová ochrana uložených a prenášaných údajov	Riadenie prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme)	Opatrenia na detekciu a odstránenie škodlivého kódu	Kontrola, obmedzenie alebo zamedzenie prepojenia IS, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou	Test funkčnosti záložných dátových nosičov	Bezpečné vymazanie osobných údajov z dátových nosičov
Oddelenie chráneného priestoru od ostatných častí objektu	Prístup tretích strán k informačnému systému	Riadenie privilegovaných prístupov	Ochrana pred nevyžiadanou elektronickou poštou	Firewall, segmentácia siete	Vytváranie záloh s vopred zvolenou periodicitou	Zariadenie na mechanické zničenie dátových nosičov osobných údajov
Umiestnenie dôležitých IT v chránenom priestore, ochrana infraštruktúry pred neoprávneným prístupom a vplyvmi okolia		Zaznamenávanie prístupu a aktivít poverených osôb	Používanie legálneho a schváleného softvéru	Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia na zamedzenie pripojenia k určitým adresám, pravidlá používania sieťových protokolov	Určenie doby uchovávania záloh a kontrola jej dodržiavania	
Bezpečné uloženie nosičov informácií s osobnými údajmi			Pravidelná aktualizácia OS a programového	Ochrana proti iným hrozbám pochádzajúcim z	Test obnovy informačného systému zo zálohy	

			aplikačného vybavenia	verejne prístupnej počítačovej siete (napr. hackerský útok)		
Zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek			Filtrovanie sieťovej komunikácie (sťahovania súborov z verejne prístupnej počítačovej siete)	Aktualizácia OS a programového aplikačného vybavenia	Bezpečné ukladanie záloh	
			Zhromažďovanie informácií o technických zraniteľnostiach IS, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík			

Organizačné opatrenia

Personálna bezpečnosť	**Riadenie aktív**	**Riadenie prístupov**	**Organizácia spracúvania osobných údajov**	**Likvidácia osobných údajov**	**Porušenie ochrany osobných údajov**	**Kontrolná činnosť**	**Dodávateľské vzťahy**
Poverenie osôb s prístupom k osobným údajom	Vedenie zoznamu aktív a jeho aktualizácia	Pravidlá fyzického vstupu do objektu a chránených priestorov	Pravidlá spracúvania osobných údajov v chránenom priestore	Určenie postupov likvidácie osobných údajov	Postup pri oznamovaní porušenia ochrany osobných údajov	Kontrolná činnosť zameraná na dodržiavanie opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov).	Postup overenia dostatočných záruk
Pokyny (postupy, oprávnenia, povinnosti) pri spracúvaní osobných údajov	Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.	Správa prístupových prostriedkov a zariadení do objektov	Nepretržitá prítomnosť poverenej osoby v chránenom priestore		Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách	Informovanie osôb o kontrolnom mechanizme (napr. Zákonník práce)	Požiadavky na ochranu údajov v rámci požiadaviek nových systémov a do pravidiel vývoja a nákupu systémov
Poučenia poverených osôb	Určenie vlastníctva aktív a zodpovednosti za riziká	Pravidlá prideľovania prístupových práv	Režim údržby a upratovania chránených priestorov		Evidencia porušení ochrany osobných údajov a použitých riešení	Postupy monitorovania súladu spracúvania osobných údajov (súlad s DPIA)	Požiadavky na ochranu údajov v zmluvných vzťahoch s dodávateľmi a tretími stranami
Určenie zodpovednej osoby	Pravidlá a postupy klasifikácie informácií	Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov	Pravidlá spracúvania osobných údajov mimo chráneného priestoru		Postup identifikácie a riešenia jednotlivých typov porušení ochrany osobných údajov		Testovanie bezpečnostných funkcií počas vývoja systémov

			(manipulácia s fyzickými nosičmi osobných údajov; používanie automatizovaných prostriedkov spracúvania; používanie prenosných dátových nosičov)				
Vzdelávanie poverených osôb	Pravidlá a postupy na označovanie informácií a nakladanie s nimi podľa klasifikačnej schémy	Pravidlá vzájomného zastupovania poverených osôb			Postup odstraňovania následkov porušení ochrany osobných údajov		Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi
Postup pri ukončení pracovného alebo obdobného pracovného vzťahu alebo obdobného pomeru poverenej osoby	Pravidlá na prijateľné používanie informácií a aktív	Pravidlá odstránenia alebo zmeny prístupových práv poverených osôb			Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti		
Práca na diaľku a pravidlá mobilného spracovania dát	Opatrenia na vrátenie aktív				Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania		