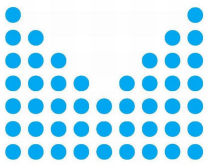
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Pseudonymizace subjektů v datovém fondu úřadu

Pseudonymizace znamená uložení dat technikou oddělení agendových a identifikačních údajů a jejich propojení pomocí AIFO dle uvedeného schématu:

Pseudonymizace **není** anonymizací údajů, a i pseudonymizované údaje jsou nadále osobní údaje.

Účelem pseudonymizace je tedy:

1. Snížení rizika neoprávněného nakládání s osobními údaji
2. Snížení rizika neoprávněného spojování osobních údajů (dále také „Profilování“)

Oproti dnes běžně používanému postupu, kdy veškeré údaje o osobách jsou uloženy v jedné tabulce (tj. včetně údajů osobních), jde o systematické rozdělení uložených údajů tak, aby od sebe byly odděleny minimálně údaje:

- **Agendové vlastní –** údaje vytvářené v rámci agendy, ve které se úřaduje
- **Referenční –** údaje získané z registru obyvatel či jiných ZR
- **Agendové –** údaje získané z jiných agend, relevantní k dané agendě

Právní aspekty pro pseudonymizaci

Zákonem 111/2009 Sb. o základních registrech byl zaveden základní princip pseudonymizace ve veřejné správě formou **Agendového identifikátoru fyzické osoby (AIFO)**(§9 až §11 zákona 111/209 Sb. o základních registrech), který zajišťuje pseudonymizaci v rámci výkonu veřejné správy. Důsledné využívání AIFO v rámci ISVS zajišťuje snížení rizika Profilování ve smyslu neoprávněného spojování údajů o konkrétní osobě z různých agend.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen GDPR) ve článku 4. definuje pseudonymizaci následovně:

„pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě

S odkazem na výše uvedené je nutné poznamenat, že v současnosti stále ještě využívané **rodné číslo je v přímém konfliktu s požadavkem na pseudonymizaci**, protože RČ, kromě toho že jde o významový identifikátor (obsahuje údaj o datu narození a pohlaví osoby), zejména umožňuje spojování jakýchkoli údajů, které jsou ve spojení s ním vedeny.

Odbor Hlavního architekta eGovernmentu Ministerstva vnitra

Ministerstvo vnitra je podle § 12 zákona č. 2/1969 Sb., kompetenčního zákona ústředním orgánem státní správy mj. pro oblast ISVS a plní též koordinační úlohu pro informační a komunikační technologie, jakož i obecně pro organizaci a výkon veřejné správy. Tyto kompetence jsou dále

rozvedeny v ZoISVS, podle něhož se ministerstvo vnitra vyjadřuje k návrhům, projektům a investičním záměrům OVS v oblasti informačních a komunikačních technologií.

Na základě příslušných předpisů plní popsanou koordinační úlohu v oblasti informačních a komunikačních technologií Odbor Hlavního architekta eGovernmentu Ministerstva vnitra (OHA). OHA má nadresortní působnost, to znamená, že je pověřen a zodpovědný za koordinaci a vedení rozvoje eGovernmentu v celé veřejné správě. Samotný eGovernment zahrnuje nejen samotné informační technologie, ale také optimalizaci a zjednodušování služeb veřejné správy vázané na legislativní prostředí. Kromě zmíněných právních předpisů je OHA ke zmíněné koordinační úloze výslovně povolán též usnesením vlády ze dne 27. ledna 2020, č. 86.

Požadavky na pseudonymizaci

Požadavky na pseudonymizaci osobních údajů jsou **architektonické, implementační a procesní.** Jejich zavedení musí být provedeno tak, aby v žádném případě neomezilo výkon veřejné správy. V ideálním případě by uživatelé ISVS neměli zaznamenat, že pro ukládání a práci s osobními údaji jsou použity procesy pseudonymizace.

Konkrétní realizace tohoto požadavku závisí na komplexitě daného informačního systému a agend, které podporuje

Architektonické postupy pseudonymizace

Pseudonymizace není výslovnou podmínkou zpracování osobních údajů, je však doporučeným postupem snižování rizika neoprávněného nakládání s osobními údaji, spolu s jinými technikami např. šifrováním.

- **Celostátní úroveň** – důsledné využívání identifikátoru AIFO, prostřednictvím komunikace s Informačním systémem základních registrů a eGON Service Bus / Informačního systému sdílené služby, při výměně údajů mezi jednotlivými ISVS, a současně zamezení/ukončení jakékoliv výměny agendových dat bez použití AIFO.
- **Lokální úroveň** – oddělení primárních identifikačních údajů osoby (referenční údaje vedené v Registru obyvatel) od údajů vytvářených v rámci vlastní agendy, a také oddělení od údajů případně získaných z jiných agend na základě oprávnění při výkonu konkrétní agendy
- **Agendová úroveň**: Zajištění využívání pseudonymizovaných agendových identifikátorů v AISech a možnosti výměny údajů z propojeného datového fondu prostřednictvím překladu identifikátorů přes ISZR
- **Doprovodná opatření** – šifrování uložených dat, které zvyšuje ochranu osobních údajů v případě odcizení datových souborů (i ve formě záloh) a důsledné logování přístupu k osobním údajům

Na celostátní úrovni

Na celostátní úrovni je zavedením Základních registrů založen bezpečný způsob výměny a správy osobních údajů. Každá agenda má přiděleno AIFO osoby a pouze převodník AIFO (ORG) je schopen převádět AIFO dané osoby mezi jednotlivými agendami. Každý takovýto převod je důsledně zalogován

a výměna údajů je zaznamenána v logu Registru obyvatel.

Při výměně údajů mezi agendami je vždy nutné zvážit rozsah údajů, které jsou přenášeny. Současný právní řád v mnoha případech zakládá oprávnění pro získání velkého rozsahu údajů mezi agendami z důvodu zajištění jednoznačné identifikace osoby, o které jsou údaje předávány. Zde je nutné si ale uvědomit, že ačkoli může existovat široké legislativní zmocnění k získávání údajů ze zdrojové agendy, s ohledem na ochranu osobních údajů je doporučeno využívat pouze údaje nezbytně nutné.

Pro identifikaci fyzické osoby při jejím kontaktu s veřejnou správou je ideální použití platného identifikačního dokladu, neboť každý orgán veřejné moci, který při své činnosti využívá některé referenční údaje vedené v registru obyvatel, je oprávněn využívat údaj o čísle a druhu elektronicky čitelných identifikačních dokladů(§18 odst. 5 zákona 111/2009 Sb. o základních registrech). Pokud tedy fyzická osoba předloží nebo ve formuláři uvede druh a číslo svého elektronicky čitelného dokladu, pak může být jednoznačně ztotožněna v Registru obyvatel. V případě vzdálené identifikace a autentizace prostřednictvím Národního bodu(Zákona 250/2017 Sb. o elektronické identifikaci) je fyzická osoba jednoznačně identifikována bezvýznamovým směrovým identifikátorem (BSI), který je možné převést prostřednictvím informačního systému základních registrů na AIFO (službou E226).

Na lokální úrovni

V rámci informačních systémů jednotlivého orgánu veřejné moci je doporučeno využívání stejných principů, které jsou používány na celostátní úrovni s respektem k faktu, že jde o úřadování v konkrétní agendě, kde se velmi pravděpodobně vyskytují agendově specifické údaje, výjimečně i údaje z agend jiných.

Doprovodná opatření

- **Logování –** každý přístup k osobním údajům a jejich aktuální propojení musí být uložen do provozního logu po dobu minimálně dvou let v souladu s pravidly dle zákona 111/2009 Sb. Musí být tedy dohledatelné, kdo a v rámci jaké činnosti přistupoval k údajům a provedl jejich propojení.
- **Aktualizace údajů –** referenční údaje o fyzické osobě musí být udržovány v aktuálním stavu prostřednictvím notifikačního systému základních registrů. Agendové údaje z jiných agend pak musí být udržovány aktuální podle pravidel platných v agendách, které údaje poskytují. Dle GDPR musí zpracovatel osobních údajů zajistit, že pracuje s aktuálními údaji tak, aby bylo minimalizováno nebezpečí chybného rozhodnutí na základě neaktuálních dat (např. zaslání rozhodnutí na neaktuální adresu osobu, či nevyužití datové schránky fyzické osoby, pokud ji má osoba zřízenu). Zde je nutné poznamenat, že každý orgán veřejné moci, který při své činnosti využívá některé referenční údaje vedené v registru obyvatel, je oprávněn rovněž využívat údaj o adrese, na kterou mají být doručovány písemnosti, o typu datové schránky a identifikátoru datové schránky, je-li tato datová schránka zpřístupněna(§18 odst. 5) zákona 111/2009 Sb. o základních registrech).

Uvedené architektonické požadavky musí být provedeny na databázové a aplikační úrovni tak, aby uživatelé informačního systému nebyli omezováni ve výkonu podporovaných agend. Současně při nutné datové analýze musí být stanoveno, jaké údaje je nezbytně nutné vést v rámci informačního systému. Opět je nutné vzít do úvahy, že ačkoli zákonné ustanovení umožňuje vedení údaje, nemusí být tento údaj veden ve své hodnotě, ale může být veden formou referenční či jiné vazby. Konkrétní rozhodnutí věcného správce agendy musí vycházet s procesních požadavků agendy a není zde možné

stanovit paušální jednoznačné pravidlo.

Příkladem může být vedení adres v rámci České republiky, kdy je **doporučeným postupem** vedení tohoto údaje formou referenční vazby do Registru územní identifikace (RUIAN) či lokální kopie adresních míst, která je udržována aktuální v souladu s RUIAN. Tím je následně vyloučen chybný správní postup, kdy je použita neplatná adresa.

Dalším příkladem je situace, kdy v agendě není využíváno například datum narození osoby pro vyhledávání či třídění, pak toto datum narození je možné vést ve formě referenční vazby do registru obyvatel a konkrétní údaj získávat pouze v potřebných případech.

Pseudonymizace, AIFO, Identifikátor, Tematická oblast