https://doi.org/10.5817/RPT2017-2-5

DYNAMICKÝ BIOMETRICKÝ PODPIS A NAŘÍZENÍ GDPR

VLADIMÍR SMEJKAL[1]

ABSTRAKT

Nařízení GDPR ve svém čl. 9 velmi omezuje možnost zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Protože nařízení nahradí dosud platný zákon č. 101/2000 Sb., o ochraně osobních údajů, podle některých názorů nebude možno nadále postupovat v mezích dosavadního stanoviska Úřadu pro ochranu osobních údajů o zpracování biometrických údajů, podle kterého u dynamického biometrického podpisu jde o zpracování probíhající ve stejném právním režimu jako u klasického podpisu. Jde tedy o zpracování osobních, ale nikoliv citlivých údajů. Příspěvek analyzuje, zda je skutečně namístě měnit dosavadní výkladovou praxi pro tuto specifickou oblast používání biometrických údajů po nabytí účinnosti GDPR, a dochází k závěru, že nikoliv. Jsou zde rovněž uvedeny obecné možnosti a limity pro používání biometrik z hlediska platného zákona a GDPR.

KLÍČOVÁ SLOVA

Biometrické údaje, dynamický biometrický podpis, nařízení GDPR, zákon o ochraně osobních údajů, identifikace, autentizace, autorizace

[1] Prof. Ing. Vladimír Smejkal, CSc., LL.M. je rektorem Moravské vysoké školy Olomouc a profesorem na Fakultě podnikatelské Vysokého učení technického v Brně. Kontaktní e-mail vladimir.smejkal@mvso.cz.

ABSTRACT

General Data Protection Regulation (GDPR) in its Article 9 greatly limits the possibility to process biometric data for the purpose of uniquely identifying a natural person. This Regulation will replace the current Act No. 101/2000 Coll. of Laws, on protection of personal data and therefore, according to some opinions, it will no longer be possible to proceed within the limits of the existing position of the Office for Personal Data Protection concerning the processing of biometric data that considers the processing of the dynamic biometric signature to be in the same regime as a classic signature. It means that personal data not the sensitive ones are being processed. This contribution analyses whether it is really necessary to change the current interpretative practice on the use of biometric data in this specific area after GDPR will apply and concludes that it is not the case. There are also mentioned general possibilities and limits for use of biometrics from the point of view of the applicable law and GDPR.

KEYWORDS

Biometric Data, Dynamic Biometric Signature, Regulation GDPR, Act on the Protection of Personal Data, Identification, Authentication, Authorization

1. ÚVOD

Dosavadní právní úprava týkající se biometrických údajů zákonem č. 101/2000 Sb., ve znění pozdějších předpisů, se nahrazuje obecným nařízením EU o ochraně osobních údajů[2] (dále také jen „GDPR“), které nabývá účinnosti 25. května 2018. Ve fázi návrhu je kromě toho zákon o zpracování osobních údajů, který navazuje na GDPR a na další předpis EU – směrnici EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů.[3]

[2] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). CELEX 32016R0679, *Úřední věstník Evropské unie* L 119, 4. 5. 2016, s. 1–88.

Zavádění dynamických biometrických podpisů (dále také jen „DBP“) se v českém právním řádu doposud nesetkalo prakticky s žádnými problémy, neboť jejich konformita s legislativou jak z hlediska podepisování (podle předchozího i stávajícího občanského zákoníku), tak s ochranou osobních údajů nebyla zpochybněna ani v teorii, ani v praxi. Lze předpokládat, že zavedení DBP do používání ve finančních institucích nebo u telekomunikačních operátorů je jen prvním krokem a bude následovat jeho plošné nasazení v dalších odvětvích – typicky ve zdravotnictví.

Je tedy na místě otázka, zda GDPR mění nějakým způsobem postavení DBP v české legislativě, případně zda je třeba provést nějaká opatření či se něčeho obávat.

2. TECHNOLOGICKÁ SPECIFIKACE DBP

Biometrie je soubor vědních poznatků založených především na statistickém a analytickém přístupu, jejichž předmětem je zkoumání a následné praktické využití měřitelných charakteristik živých organismů (tedy biometrik) s cílem jejich jednoznačné identifikace (zjištění identity) nebo verifikace (ověření identity) člověka.[4] Pro identifikaci a/nebo verifikaci se využívají anatomicko-fyziologické nebo behaviorální charakteristiky každého člověka, přičemž je můžeme členit různým způsobem.

Klasické dělení biometrických metod (a charakteristik) je následující:

1. statické,
2. statické s testováním přítomnosti osoby (tzv. projev živosti[5]),
3. dynamické.

---

[3] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. CELEX 32016L0680, *Úřední věstník Evropské unie* L 119, 4. 5. 2016, s. 89–131.

[4] RAK Roman; MATYÁŠ, Václav; ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada Publishing, a.s., 2008. ISBN 9788024723655.

[5] U biometrických systémů je testování projevu živosti základním způsobem, jak eliminovat pokusy o podvrhnutí falešného vzorku – např. pomocí gelového otisku prstu nebo obrázku duhovky oka zhotoveného na kontaktní čočce atd., nebo vzorku odebraného dané osobě – uříznutý prst. Provádí se obvykle zjišťováním tělesné teploty nebo na sofistikovanější úrovni snímáním cirkulace krve v cévách nebo měřením koncentrace oxyhemoglobinu.

Přesto i u statických biometrik budeme rozlišovat ty, které se nemění za žádných okolností (oční duhovka, topografie žil, DNA, otisk prstu), a v čase proměnlivé (váha, rozměry a geometrie různých částí těla, obsah solí v těle apod.).

Dynamické biometrické metody vyhodnocují chování člověka, resp. jeho projev určitým způsobem – mimikou, chůzí, psaním, gestikulací, hlasem a jsou exteriorizací interiorizovaných struktur člověka. V případě pohybů těla nebo jeho částí, ale i u psaní jde o motorickou činnost jako cílevědomý a systematický proces řízený centrální nervovou soustavou uskutečňovaný v interakci mezi člověkem a okolím za pomoci pohybové soustavy.

Dynamické biometrické metody používané pro identifikaci a/nebo verifikaci spočívají ve využití behaviorálních charakteristik, které jsou unikátní pro každého člověka, jako jsou pohyb rtů, hlasový projev, dynamika stisku počítačových kláves nebo pohybu myší, gesta prováděná v prostoru, rytmus chůze nebo vlastnoruční podpis. Při posledním způsobu autentizace se *de facto* jedná o to, co každý považuje za běžnou činnost, nicméně v nové kvalitě. Od podpisového vzoru v podobě neobratného a omylného srovnávání obrázků s podpisy (pozorováním ověřující osobou), poskytujícího minimální záruky, přes relativně bezpečné, ale komplikované postupy asymetrické kryptografie, jsme se opět vrátili k podpisovým vzorům, ale vzorům „chytrým“, skrývajícím oku neviditelnou a nezfalšovatelnou biometrickou vrstvu.

Na rozdíl od klasické trojice autentizačních faktorů, kdy při autentizaci subjektu dochází k ověření jeho identity na základě:

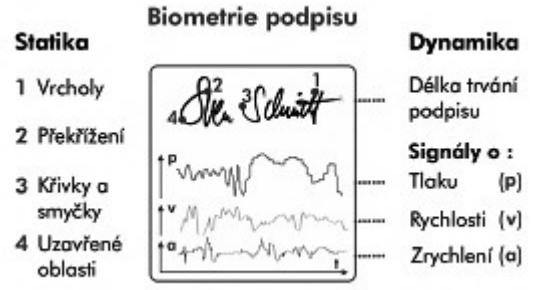
- vlastnictví – magnetická nebo čipová karta, token, autentizační kalkulačka, nebo
- znalosti – heslo, PIN, tajný klíč, nebo
- charakteristiky – viditelná nebo neviditelná biometrická informace,[6]

[6] K tomu viz SMEJKAL, Vladimír a Jindřich KODL. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*. Prague, Czech Republic, 13–16 October 2008, s. 1–6. ISBN 9781424418169.

v případě DBP i dalších behaviorálních biometrik se dostáváme do situace, kdy uživatel „neví co ví“, resp. ani jemu není známa biometrická informace použitelná pro autentizaci podpisu.

DBP vzniká tak, že je snímán vlastnoruční podpis s využitím speciálního digitalizačního snímače (padu), zaznamenávajícího data, která umožní analyzovat jak statické, tak zejména dynamické vlastnosti podpisu spojeného s typickým chováním podepisující se osoby. Jedná se o základní rysy vlastnoručního podpisu, jako jsou:

- čas trvání podpisu, včetně trvání mezi jednotlivými tahy,
- body a křivky v jednotlivých částech podpisu,
- tlak působící perem na podložku v různých dobách procesu podpisu,
- celková velikost podpisu,
- forma a tvar podpisu,
- délka a úhel čáry, oblouky a křivky, počet smyček,
- rychlost při jednotlivých tazích, zrychlení, zpomalení.



Obr. č. 1: Statické a dynamické charakteristiky podpisu[7]

DBP obsahuje informace o tom, jak byl podpis vytvořen, odráží tedy charakteristické znaky podepisující se osoby, její návyky a projevy chování. Tyto vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována (na rozdíl od

[7] SIGNOSOFT. *Jak to funguje* [online]. [cit. 2017-11-21]. Firemní dokumentace společnosti SignoSoft s.r.o. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php.

samotného obrázku podpisu, který zde tvoří pouze jeden z parametrů biometrické stopy).[8]

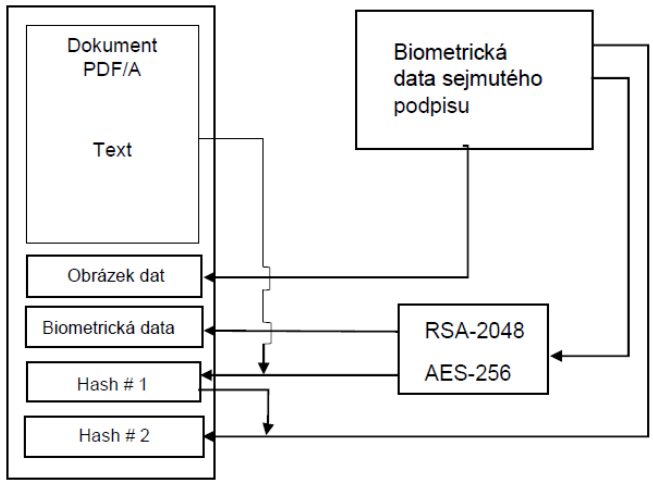
Zabezpečení DBP je řešeno takto: vektor dat, reprezentujících DBP, opustí snímací zařízení pouze v zašifrovaném tvaru. Na zabezpečený přenos biometrických dat ze snímače do počítače bezprostředně navazuje požadavek na jednoznačné a zabezpečené spojení DBP s podepisovaným dokumentem. Pro tyto účely je opět možné použít kryptografickou metodu, a to jak pro vytvoření hashe dokumentu[9], tak pro ochranu integrity podepsaného hashe standardním (kryptografickým) elektronickým podpisem.

Podstatným rozdílem nicméně je, že použití asymetrické kryptografie (tedy vytvoření podpisu pomocí soukromého klíče) není požadováno na straně klienta (uživatele), ale je otázkou řešení celého systému, tj. chová se z hlediska uživatele (podepisující osoby) jako „černá skříňka" a nezatěžuje jej žádnými technicko-organizačními požadavky.

Výrobci zařízení zajišťují bezpečnost DBP tak, že vytvářejí řadu hashů a provádějí podepisování a šifrování například takto:

[8] Viz experimenty popsané v SMEJKAL, Vladimír a Jindřich KODL. Assessment of the authenticity of Dynamic Biometric Signature. The results of experiments. In: *Proceedings of the 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, s. 45–49, ISBN 9781479935307.

[9] Hashováním nazýváme převod obsahu dokumentu matematicko-kryptografickou metodou na jeho reprezentaci řetězcem čísel s pevně definovanou délkou pomocí jednocestné funkce, dnes např. SHA-256. Tím získáme standardní otisk (hash) z jakéhokoliv dokumentu, který je následně jedním ze vstupů do procesu podepsání. Více viz např. MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice. Právní a technologické aspekty*. 2. vydání. Praha: Leges, 2012, s. 286 a násl. ISBN 9788087576366.



Obr. č. 2: Schéma provázání DBP s dokumentem typu PDF

1. Aplikace (dále též „AP“) ustaví šifrovanou komunikaci s podepisovacím zařízením (v tomto případě algoritmem AES-256). Výměna klíče proběhne pomocí Diffie-Hellman-Merkle protokolu. Během podpisu jsou tímto zabezpečeným kanálem přenášena biometrická data do AP.
2. Uživatel se podepíše na podepisovací tablet. Data reprezentující podpis jsou šifrovaným kanálem ad 1. přenesena do paměti počítače.
3. Na základě biometrických dat AP vytvoří (viditelný) obrázek podpisu a vloží jej do dokumentu.
4. K biometrickým datům jsou připojeny další údaje (sériové číslo zařízení, časové razítko), což zajistí, že biometrická data nemohou být umístěna do jiného dokumentu, resp. že toto zneužití je možné zjistit.

5. V zařízení jsou zašifrována biometrická data symetricky (AES-256) a symetrický klíč pak AP zašifruje pomocí veřejného klíče asymetricky (RSA-2048).[10]
6. AP vloží zašifrovaná biometrická data do dokumentu ve formátu PDF.
7. AP spočítá HASH1 (algoritmem SHA-256) z obsahu dokumentu a zašifrovaných biometrických dat. HASH1 slouží pro kontrolu integrity dokumentu a zašifrovaných biometrických dat. HASH1 je podepisován veřejným klíčem.
8. AP vloží podepsanou HASH1 a příslušný veřejný klíč do dokumentu.
9. AP spočítá HASH2 (algoritmem SHA-256) z HASH1 a nezašifrovaných biometrických dat a uloží jej do dokumentu. HASH2 zajišťuje propojení dokumentu a biometrického podpisu.
10. AP smaže z paměti počítače nezašifrovaná biometrická data a všechny spočítané hashe (HASH1 a HASH2).

Souhrnně lze tedy říci, že:

1. biometrická data jsou ihned po sejmutí šifrována a nikdy nejsou zobrazena v otevřeném tvaru; výjimkou je forenzní zkoumání – viz níže,
2. jsou používána výlučně pro vytvoření elektronického podpisu, tedy nikoliv pro identifikaci nebo autentizaci subjektu údajů,
3. jediná možnost, jak se dostat k původním biometrickým údajům, je mimořádná situace – dokazování v rámci soudního sporu. V takovém případě je třeba získat přístup ke klíči, kterým byla biometrická data zašifrována, což absolutní většina projektů řeší úschovou

[10] AES-256 je algoritmus používaný k symetrickému šifrování dat, šifrující I dešifrující stejným klíčem na obou stranách, o délce klíče 256 bitů. Diffie-Hellman-Merkle protokol je kryptografická metoda, která umožňuje přes nezabezpečený kanál vytvořit šifrované spojení mezi komunikujícími stranami, a to bez nutnosti předchozího dohodnutí šifrovacího klíče. Výsledkem je vytvoření symetrického šifrovacího klíče, který je efektivnější a může být použit pro šifrování další komunikace. RSA-2048 je algoritmus používaný k asymetrickému šifrování dat, který se dá používat pro podepisování i šifrování dokumentů, protože používá soukromý a veřejný klíč o délce 2048 bitů. Viz např. SINGH, Simon. *Kniha kódů a šifer*. 1. vydání. Praha: Argo 2003. ISBN 8086569187.

klíče u třetí osoby, obvykle u certifikační autority, která klíč střeží. Formalizovaným postupem za účasti notáře a soudního znalce je v takovém případě podpis extrahován z konkrétního dokumentu a lze jej prověřit buď pomocí softwarového nástroje nebo předat písmoznalci.

3. PRÁVNÍ ÚPRAVA PODLE ZÁKONA Č. 101/2000 SB.

Stávající právní úprava zavedla v rámci zákona č. 101/2000 Sb. kategorii tzv. citlivých údajů, což jsou osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; **citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů (§ 4 písm. b) zákona o ochraně osobních údajů**. Podle § 9 tohoto zákona citlivé údaje je možné zpracovávat, jen jestliže podle písm. a) subjekt údajů dal ke zpracování výslovný souhlas, nebo jestliže podle písm. h) je zpracování nezbytné pro zajištění a uplatnění právních nároků.

Identifikaci lze stručně definovat jako zjištění identity (totožnosti) subjektu, které se provádí porovnáváním osobních údajů nebo projevů osobní povahy fyzické osoby s jinými, které jsou obvykle zachyceny na nějakém nosiči, zatímco autentizaci jako ověření, že subjekt je tím, za koho se prostřednictvím této identity vydává. V praxi se identifikace na písemném dokumentu provádí nejčastěji uvedením jména, příjmení, adresy, případně jiných údajů o dotčené osobě. Autentizace, tj. ověření, že dokument skutečně podepsala uvedená osoba, se provádí podpisem, podpisem před svědky, ověřením totožnosti pověřenou osobou; nejjistější je zatím stále legalizace formou úředně ověřeného podpisu nebo notářského zápisu.[11]

Jak uvádí Nejvyšší správní soud, *„Obecně lze fyzickou osobu považovat za "identifikovanou", jestliže je ve skupině osob odlišena ode všech ostatních příslušníků této skupiny. V souladu s tím je fyzická osoba "identifikovatelná", jestliže je možné ji identifikovat (přípona "-elná" vyjadřuje možnost), ačkoli dosud*

[11] Více viz MATES, Pavel a Vladimír SMEJKAL, op. cit., s. 272 a násl.

identifikována nebyla. Tato druhá alternativa proto v praxi představuje prahovou podmínku určující, zda informace vyhovuje definici osobního údaje.“[12] Co se týká biometrik, pak aby byla osoba podle nějaké biometrické charakteristiky identifikovatelná, musí existovat seznam (databáze), v níž bude k určité biometrické charakteristice nebo souboru charakteristik přiřazen jednoznačný identifikátor konkrétní osoby. Podle toho, o kterou biometriku se bude jednat, může se zde také nacházet pravděpodobnostní údaj určující, s jakou pravděpodobností se jedná o tuto osobu (bude přicházet v úvahu zejména u dynamických metod). V případě pochybnosti bude muset ověřující osoba provést další identifikaci či autentizaci na základě jiného parametru dané osoby.

V odpovědi na konkrétní dotaz v souvislosti se zaváděním DBP se dne 8. srpna 2016 Úřad pro ochranu osobních údajů (dále též „Úřad“) vyjádřil tak, že **pokud tzv. dynamický biometrický podpis bude využíván stejně jako podpis klasický, tzn. jeho využití nebude spojeno s dalším automatickým zpracováním biometrických údajů (např. porovnávání podpisu s podpisovým vzorem za využití biometrických dat), bude se jednat o zpracování probíhající ve stejném právním režimu, jako při zpracování klasického podpisu**.[13]

Jinak řečeno, podle tohoto názoru Úřadu se při shromažďování a dalším využívání podpisu v rámci běžné smluvní či klientské agendy jedná o zpracování osobních, nikoliv citlivých údajů dle definic v § 4 písm. a) a b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Zákon o ochraně osobních údajů v § 5 odst. 2 obsahuje konečný výčet právních titulů pro možné zpracování osobních údajů. Jedním z nich je i titul upravený v § 5 odst. 2 písm. b) zákona o ochraně osobních údajů, dle kterého lze osobní údaje bez souhlasu dotčené osoby zpracovávat tehdy, pokud je zpracování nezbytné pro uzavření či plnění smlouvy, jejíž smluvní stranou je právě dotčená osoba. Rovněž lze poukázat na právní titul uvedený v § 5 odst. 2 písm. e) zákona, podle nějž lze osobní údaje zpracovávat i bez souhlasu tehdy, pokud je to nezbytné pro ochranu práv správce, pří-

[12] Rozsudek Nejvyššího správního soudu ze dne 27. února 2014, spis. zn. 4 As 132/2013.

[13] Archiv autora, důvěrný zdroj.

jemce či jiné dotčené osoby. Pokud je tedy podpis fyzické osoby vyžadován, jelikož je nezbytný pro uzavření či realizaci smluvního vztahu, případně pro ochranu práv a právem chráněných zájmů správce či další osoby, pak jej lze, spolu s dalšími nezbytnými údaji, shromažďovat a dále zpracovávat i bez souhlasu daného subjektu údajů. V případě sporu o pravost podpisu, ať už učiněného klasicky, nebo za využití zmíněné technologie, je pak obecně přípustné využít v podpise obsažené biometrické údaje, a to na základě § 9 písm. h) zákona č. 101/2000 Sb., tedy rovněž bez nutnosti vymáhat k tomu souhlas dotčené osoby.

V I. pololetí 2017 vydal Úřad informaci „Změna v hodnocení úrovně právní ochrany biometrických údajů“[14], v níž se zejména uvádí: *„Dne 25. května 2018 nabývá účinnosti evropský předpis, který nově nastavuje ochranu osobních údajů mj. z důvodu proměn a rychlého rozvoje technologií, tzv. obecné nařízení o ochraně osobních údajů (nařízení Evropského parlamentu a Rady, č. 2016/679). Ve svém čl. 9 upravuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Tato úprava přináší podstatnou změnu v právním pohledu na technologie zpracovávající biometrické údaje, mj. také v tom, že uchovávání biometrických šablon (template) a jejich zpracování za účelem identifikace osob považuje za zpracování zvláštní kategorie osobních údajů. (…) Obecné nařízení v otázkách zpracování biometrických údajů plně nahradí dosud platné ustanovení zákona o ochraně osobních údajů, nebude tedy možno postupovat v mezích dosavadního stanoviska Úřadu pro ochranu osobních údajů.“*

Za pozornost stojí část, kde se výslovně hovoří o šablonách a jejich použití při zpracování za účelem identifikace osob. Podle normy ČSN ISO/IEC 19795-1 se šablonou rozumí uložená referenční míra uživatele, založená na rysech extrahovaných ze zaznamenaných vzorků.[15] Čili pro jiný přístup k posuzování zpracování po nabytí účinnosti GDPR je tedy třeba splnění těchto dvou podmínek:

---

[14] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Změna v hodnocení úrovně právní ochrany biometrických údajů* [online]. [cit. 2017-21-11]. Dostupné z: https://www.uoou.cz/zmena-v-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850.

[15] ČSN ISO/IEC 19795-1. *Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura.*

1. existence šablony,
2. použití za účelem identifikace osob.

Následně dne 8. června 2017 publikoval Úřad Stanovisko č. 1/2017 – Biometrická identifikace nebo autentizace zaměstnanců.[16] Toto stanovisko je psáno v mantinelech platného zákona o ochraně osobních údajů, nicméně v poznámkovém aparátu se v některých případech odkazuje na úpravu podle GDPR.

Je pravdou, že celé stanovisko vychází z předpokladu použití biometrických údajů v podobě otisků prstů (případně otisku dlaně) pro přístupové a docházkové systémy, ale lze je aplikovat i obecně. Stanovisko přitom nakládá s pojmem „přístupové a docházkové systémy" jako s notorietou, nicméně je vhodné se shodnout na vlastnostech obou typů systémů a rozdílu mezi nimi.

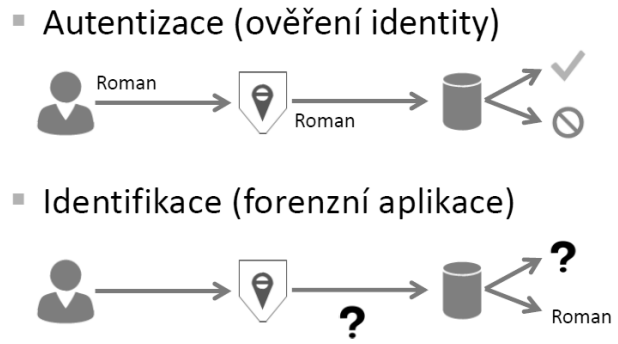
Přístupový systém, jak vyplývá z názvu, umožňuje někam přístup. Tedy sejme identifikační údaje osoby a provede autentizaci (také se říká verifikaci), tj. ověření, že osoba je tím, za koho se vydává, a podle toho následně uskuteční autorizaci, tj. ověří, jaké má daná osoba oprávnění, např. ke vstupu do určitého objektu nebo jeho části. **Identifikací tedy rozumíme rozpoznání entity systémem**, a to na základě určitého identifikátoru, který je spojen s určitou osobou, reprezentuje jeho identitu a může být znám jiným osobám. (Jméno a příjmení, případně další identifikátory, odstraňující zaměnitelnost… rodné číslo, číslo sociálního pojištění, bezvýznamový identifikátor atd.) **Právně je identifikace určení osoby, která učinila určitý úkon. Autentizace potom znamená ověřování proklamované identity subjektu.** (V normě ČSN ISO/IEC 19795-1 se nazývá verifikací.)

V prvním případě jde tedy o situaci, kdy identita osoby je známa, přesně řečeno osoba tvrdí, že je XY, případně to něčím prokazuje (např. čipovou kartou) a úkolem je ověření této identity, tedy zjištění, zda údaje, které osoba uvádí (jméno, heslo, PIN apod.), vykazuje (biometrika) nebo vlastní

[16] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Stanovisko č. 1/2017 - Biometrická identifikace nebo autentizace zaměstnanců* [online]. [cit. 2017-21-11]. Dostupné z: https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849/p1=1099.

(čipová karta), odpovídají v databázi uvedené identitě. Hovoříme proto o porovnávání 1:1.

V druhém případě, kdy se osoba neprohlásí, tj. nezadá žádný identifikátor, probíhá identifikace na základě určitých sejmutých charakteristik dané osoby, například biometrických, kdy jsou tyto charakteristiky porovnávány vůči celé databázi osob; jedná se tedy o porovnávání 1:n – viz Obr. č. 2[17]. To je ale postup, který se nevyskytuje v běžném životě, např. v zaměstnaneckých vztazích, a je využíván např. v oblasti národní bezpečnosti.



Obr. č. 3: Rozdíl mezi autentizací a identifikací

Identifikace obvykle zahrnuje:

- získání vzorku,
- segmentaci a extrakci rysů,
- kontroly kvality (které mohou zamítnout vzorek/rysy jako nevhodné a vyžadují získání dalších vzorků),
- porovnání proti některým nebo všem šablonám v databázi registrovaných, produkující skóre podobnosti pro každé porovnání,
- rozhodnutí, zda je každá shodná šablona potenciálním identifikátorem kandidáta uživatele, založené na tom, zda skóre podobnosti překročí určitou hodnotu,

[17] Obrázek je převzatý z CINKAIS, Roman a Jiří VÁBEK. *Důležité otázky při výběru biometrické modality*. Přednáška na konferenci SECURITY 2015, 18. února 2015. [online]. [cit. 2017-21-11]. Dostupné z: http://docplayer.cz/34431484-Dulezite-otazky-pri-vyberu-biometricke-modality-roman-cinkais-jiri-vabek-wincor-nixdorf-s-r-o.html.

- identifikační rozhodnutí, založené na seznamu kandidátů z jednoho nebo více pokusů, což je předepsáno v rozhodovací politice.[18]

Úřad ve stanovisku č. 1/2017 uvádí, že *„Pokud se jedná o možnosti využití výjimky v § 9 písm. b) až i) zákona o ochraně osobních údajů pro zpracovávání biometrických údajů zaměstnanců, dá se využít toto ustanovení jen velmi omezeně. Z hlediska zákona o ochraně osobních údajů jde v tomto případě zejména o zpracování citlivých údajů, které je nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem ve smyslu § 9 písm. d), a dále se může jednat o zpracování nezbytné pro zajištění a uplatnění právních nároků ve smyslu § 9 písm. h), když tato možnost vyplývá ze zvláštních právních předpisů. (…) V praxi však u přístupových systémů, kde zajištění bezpečnosti zpracováním citlivých biometrických údajů není stanoveno zvláštním zákonem nebo spojeno se zvláštním zákonem předvídanou prováděcí vyhláškou, lze biometrické identifikace s vyhledáváním biometrických údajů v databázi použít jen s výslovným souhlasem jejich nositele podle § 9 písm. a) zákona o ochraně osobních údajů.“*

U docházkového systému jde o rozšířenou variantu přístupového systému, tj. kromě provedení autentizace a nastavení autorizace se uloží záznamy o příchodu a odchodu osoby. Mělo by se tedy jednat o rozšířený přístupový systém. Úřad nicméně vnímá docházkový systém jinak, když ve stanovisku uvádí, že *„V přístupových systémech by v návaznosti na uvedené mělo vždy platit pravidlo, že jde o mimořádné opatření kdy, kromě ze zvláštního zákona vyplývající povinnosti zajistit bezpečnost přístupu, se zpravidla zpracovávají biometrické údaje omezeného okruhu oprávněných osob, na rozdíl od plošného zpracování biometrických údajů všech zaměstnanců v docházkových systémech.“*. V uvedeném stanovisku Úřadu se dále uvádí, že *„(…) nelze použití systémů, v jejichž paměti dochází k uchovávání biometrických údajů v podobě, která umožňuje jejich další zpracování, považovat za nezbytné pro jakoukoliv běžnou evidenci, např. pro evidenci docházky do zaměstnání. Zpracování biometrických údajů zejména v docházkových systémech lze proto posu-*

[18] ČSN ISO/IEC 19795-1. *Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura.*

zovat jako nepřiměřené ve vztahu k rozsahu a účelu zpracovávání, který je povinen stanovit každý správce.“

S tím nelze zcela souhlasit ze dvou důvodů:

a) proč by se měl přístup k posuzování zpracování lišit podle toho, jak velká je množina dotčených osob, pokud se stále jedná o uzavřenou množinu, která vznikla na základě nějakého právního vztahu (pracovní smlouva),
b) v případě, že bude zpracování probíhat na základě souhlasu (čl. 9 odst. 2 písm. a) GDPR);

pak se bude jednat o shodný postup jak u přístupového, tak u docházkového systému. Počet dotčených osob není naprosto rozhodující.

Úřad dále tvrdí, že *„Prvním podstatným hlediskem je, zda dochází k uchovávání úplných biometrických údajů, nebo zda systém vybírá z úplných biometrických údajů některé rysy specifické pro jednotlivce tak, aby vytvořil biometrickou šablonu, která je redukcí úplného biometrického obrazu.“* Není zcela jasné, co se tím myslí. Nevíme, co to jsou „úplné biometrické údaje“ a rovněž nevíme, jaký postup se předpokládá v rámci popsaného vytváření šablony. Pokud se tím myslí, že šablona obsahuje pouze některé biometrické údaje osoby nebo sice všechny, ale nějakým algoritmem upravené (redukované?), pak odpověď pravděpodobně nalezneme v dalším textu stanoviska, podle kterého se požaduje, aby šablony byly před uložením v systému zpracovávány matematickými operacemi (kódování, algoritmy nebo hash funkce) tak, aby nebyly volně čitelné nebo zpětně rekonstruovatelné. *„Důležité přitom je, že různé systémy mají různé způsoby bezpečného převodu šablony otisku prstů do číselného vyjádření, které je uloženo v systému. Nelze proto říci, že určité takto získané číselné vyjádření je pro subjekt údajů ve všech systémech jednoznačné. Zpracování takovýchto číselných vyjádření šablon tedy nelze posuzovat jako zpracování biometrických údajů.“* Je zvláštní, že v poznámce pod čarou ve stanovisku č. 1/2017 přitom toto tvrzení Úřad sám relativizuje tím, že podle něj je uvedené vyjádření již v současnosti nutno s ohledem na technologický vývoj považovat za neúplné a nelze je vztáhnout na všechny moderní biometrické systémy. Nelze odhadnout, co

Úřad tímto pythickým vyjádřením myslí. Buď je funkce použitá pro převod jednosměrná, což platí pro hashovací funkce, nebo ne.

Sám Úřad dále totiž ve stanovisku č. 1/2017 uvádí, že *„Jestliže dojde např. při použití jednosměrného hashování k vytvoření číselného údaje, jehož zpětná rekonstrukce na biometrický údaj není možná, nelze již tento údaj považovat za biometrický a využití takového systému může být v určitých případech přípustné, a to při naplnění povinností správce podle § 5 odst. 1 a dále některé z podmínek § 5 odst. 2 písm. a), b) nebo e) zákona o ochraně osobních údajů i bez souhlasu subjektu údajů, protože nedochází k uchovávání citlivého údaje.“* [Zde se Úřad odkazuje na čl. 9 GDPR.]

Technologicky by tedy zřejmě vyhovovalo řešení, podle kterého bude zpracování probíhat takto:

1. získání vzorku např. přiložením prstu, dlaně, sejmutím obrázku obličeje apod.,
2. extrakce rysů potřebných pro vytvoření a kontrola jejich kvality,
3. při vyhovující kvalitě provedení jednosměrné operace, která znemožní zpětnou rekonstrukci biometrických údajů,
4. porovnání se šablonou v databázi (která byla vytvořena stejným způsobem),
5. rozhodnutí o shodě či neshodě, a tedy potvrzení nebo zamítnutí identifikace.

Problémem je, že u některých biometrik, zejména dynamických, to bude obtížněji realizovatelné. Vlastnosti hashovacích funkcí jsou totiž následující:

a) jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup (hash neboli otisk dokumentu), protože jde o funkci, která převádí vstupní posloupnost bitů (obsah dokumentu) na posloupnost bitů o pevné délce (kryptografické hashovací funkce typu SHA existují pro různé délky výstupních hodnot od 256 do 512 bitů),
b) v případě jakékoliv změny vstupních dat dosáhneme změny i na výstupu (tj. výsledný otisk se od původního liší[19]),

[19] Tato vlastnost se využívá pro zajištění možnosti kontroly integrity digitálních dokumentů, a to v souvislosti s elektronickým podpisem, ale i v jiných případech.

c) z hashe není možné rekonstruovat původní text zprávy (jde o jednosměrnou funkci),
d) v praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný hash, jinými slovy pomocí hashe lze v praxi identifikovat právě jednu zprávu (ověřit její správnost).[20]

V případě statické biometrie, kdy jednosměrná funkce dává pro stejná vstupní data stejný výsledek, by měla takto vytvořená šablona poskytovat dostatečnou míru ochrany a současně úspěšně sloužit pro vyhodnocení porovnávání v modu 1:1 i 1:n.[21] V případě dynamických biometrik, které jsou podstatně odolnější proti falšování, napodobení nebo odcizení, je ale situace složitější, neboť biometrická data se pohybují v určitém rozmezí (toleranční úrovni) a jednosměrná funkce buď vůbec nebude schopna převést sejmutý vzorek tak, aby mohl být vyhodnocen, nebo se přinejmenším nebude schopna vypořádat s onou tolerancí (nepodstatnými odlišnostmi v dynamickém projevu osoby).

Protože u dynamických biometrických metod nejsou obsahem sejmutého vzorku vždy zcela stejná data, použití obvyklých hashovacích funkcí může vést k nemožnosti provést porovnání mezi vzorkem a šablonou. Nicméně toto by mělo jít eliminovat použitím jiných postupů, umožňujících zohlednění podobnosti, a nikoliv absolutní shody vstupních dat, jako jsou histogramy nebo metody pro rozhodování za neúplné informace.[22] Přesto tyto postupy mohou vést ke zvýšení chybovosti při vyhodnocování shody vzorku a šablony (odmítnutí pravého nebo přijetí falešného vzorku), a proto je vhodné biometrická data ukládat v úplném tvaru, ale tak, aby byla dostatečně zabezpečena. Tomu nepochybně vyhovuje výše popsaný postup (viz Obr. č. 1) v případě dynamického biometrického podpisu.

---

[20] Teoreticky tato možnost existuje, nazývá se kolize. Použití prověřené hashovací funkce a větší délky klíče tuto pravděpodobnost významně snižuje.

[21] Viz např. ABOUELMEHDI, Karim; BENI-HSSANE, Abderrahim; KHALOUFI, Hayat a Mostafa SAADI. Big data security and privacy in healthcare: A Review. *Procedia Computer Science* [online]. Elsevier B.V, 2017, roč. 113, 2017, s. 73-80. [cit. 2017-10-13]. DOI: 10.1016/j.procs.2017.08.292. ISSN 1877-0509.

[22] Viz např. DRAHANSKÝ, Martin; DOLEŽEL, Michal a Filip ORSÁG. *Biometrie.* Brno: Computer Press, 2011, s. 50 a násl. ISBN 9788025489796.

Pokud má být ale dynamická biometrika použita pro identifikaci a/nebo autentizaci, pak je situace složitější. V příspěvku autorů[23] byla navržena metoda pracující se dvěma databázemi. V prosinci 2014 vydaná norma ČSN ISO/IEC 24745 „Ochrana biometrických informací“[24] popisuje řadu metod pro zabezpečení statických i dynamických biometrických informací. Uvedený postup je v ní detailně propracován v normě v příloze A, popisující bezpečné svázání a oddělení databáze pro identitní reference a databáze pro biometrické reference. V této souvislosti je třeba zmínit i rámec pro obnovitelné biometrické reference, který je popsán v příloze C normy. Obnovitelné biometrické reference jsou revokovatelné (obnovitelné) identifikátory, které reprezentují jednotlivce nebo datový subjekt v rámci určité domény prostřednictvím chráněné binární identity (re)konstruované ze sejmutého biometrického vzorku. Obnovitelná biometrická reference neumožňuje přístup k původním datům biometrického měření, biometrické šabloně nebo pravé identitě jejího vlastníka. Kromě toho nemá obnovitelná biometrická reference žádný význam vně domény služeb.

Souhrnně lze konstatovat, že pokud uživatel bude vyžadovat on-line ověřování provedených DBP, musí řešit mj. správu vysoce zabezpečené databáze vzorů DBP. Požadavek na zabezpečení databáze podpisových vzorů v případě, že budou používány k identifikaci (1:n) je vysoký (viz mj. požadavky uvedené v normě ISO/IEC 15408,[25] ale řešitelný. Zde je třeba zdůraznit, že je adekvátní nutností zabezpečit na stejné úrovni i podpisový certifikát (resp. privátní klíč) vydávaný certifikačními autoritami a zejména jejich vlastní kořenový certifikát,[26] pokud jsou použity.

---

[23] SMEJKAL, Vladimír a Jindřich KODL. Strong authentication using dynamic biometric signature. In: *Proceedings of the 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST)*. Barcelona, Španělsko, 18-21 October 2011, s. 340–344. ISBN 978145770902.

[24] ČSN ISO/IEC 24745. *Informační technologie – Bezpečnostní techniky – Ochrana biometrických informací.*

[25] ISO/IEC 15408-1:2009. *Information technology –- Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[26] SMEJKAL, Vladimír a Jindřich KODL. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16tého ročníku mezinárodní konference Information Security Summit (IS2)*, 27.–28. května 2015, Praha: TATE International, s.r.o., s. 107–119. ISBN 9788086813288.

Úřad dále uvádí, že *„Povinnostem stanoveným zákonem o ochraně osobních údajů pro zpracování citlivých údajů proto nemusí podléhat systém, který pracuje pouze na principech autentizace, tedy metody kontroly příchodu a odchodu zaměstnance, kdy čtecí zařízení, do kterého otisk prstu vkládá na základě požadavku zaměstnavatele na kontrolu docházky sám zaměstnanec, porovnává údaje 1:1. Při příchodu na pracoviště nebo odchodu z něj je po zvolení osobního čísla zaměstnance vložený otisk s přiložením příslušného prstu použit pouze pro ověření totožnosti subjektu údajů. Do dalšího zpracování osobních údajů snímek otisku prstu nebo dlaně však již nevstupuje a systém jeho další zpracování ani neumožňuje. (…) Rozhodné pro posouzení, zda jde o z hlediska zásad ochrany přípustnou autentizaci, nebo o identifikaci, kterou je třeba podrobit přísné regulaci, je, zda účelem použití otisku prstu, je pouze ověření totožnosti porovnáním s přiloženým prstem ruky, nebo v systému dochází v návaznosti na přiložení ruky nebo její části (případně karty s RFID čipem, který již tyto informace obsahuje) k vyhledávání a porovnávání informací s údajem uchovávaným v databázi biometrických údajů, která musí být vždy považována za zpracování citlivých údajů, podléhající režimu § 9 zákona o ochraně osobních údajů.“*

Výše uvedený text lze tedy interpretovat tak, že **pokud dochází k autentizaci (jinak zadané) identity zaměstnance (porovnávání 1:1), je všechno v pořádku a o zpracování citlivých údajů se nejedná**. Pokud by mělo docházet k identifikaci, tj. prohledávání databáze za účelem určení, kdo prst či ruku přiloží (tedy 1:n), jde o zpracování citlivých údajů.

4. PRÁVNÍ ÚPRAVA PODLE GDPR

Podle definičního čl. 4 odst. 14 GDPR se *„biometrickými údaji rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“*. Podle výše zmíněného čl. 9 odst. 1 GDPR *„Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem*

jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“ **Je třeba výslovně upozornit, že zde se již nehovoří ani o podepisování, ani o autentizaci, ale pouze a jen o identifikaci.**

Podle čl. 9 odst. 2 GDPR platí, že *„Odstavec 1 se nepoužije, pokud jde o některý z těchto případů: a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, (…) f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí.“*

V případě ad f) je třeba definovat před zahájením zpracování důvody, pro které by mělo jít o zpracování související s právními nároky a koho. Dle názoru autora by takovým právním nárokem ze strany zaměstnavatele, ale i zaměstnance mohl být důkaz, že se zaměstnanec dostavil na pracoviště a jak dlouho na něm setrval. U zvláštních zaměstnání by se mohlo jednat např. i o sledování, kam vstupoval, jaká zařízení a materiály používal, ale toto by zřejmě muselo mít dostatečnou zákonnou oporu.[27]

Přitom podle čl. 6 odst. 4 *„Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu (…) zohlední správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:*

a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;

b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;

c) povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle článku 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10;

d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;

e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.“

[27] Např. povinnost zajistit jadernou bezpečnost, radiační ochranu a bezpečnost jaderného materiálu podle zákona č. 263/2016 Sb., atomového zákona, ve znění zákona č. 183/2017 Sb.

Dikce čl. 6 GDPR je využitelná v případě, kdy budou biometrické údaje shromážděny za účelem autentizace osoby, ale např. v souvislosti s prováděným šetřením podloženým některým veřejnoprávním předpisem bude třeba prokázat přítomnost určité osoby na určitém místě a v čase.[28]

Dle názoru autora je klíčové a rozhodující to, co Úřad sám ve stanovisku konstatuje, že *„Dalším důležitým hlediskem je, zda je použitý systém založen na autentizaci (verifikaci) fyzické osoby, nebo na identifikaci subjektu údajů v databázi, v níž jsou uchovávány osobní údaje i dalších subjektů údajů. Autentizační (verifikační) systém pouze ověřuje totožnost fyzické osoby porovnáním údajů 1:1. Při identifikaci systém rozpoznává jednotlivce odlišením od ostatních osob, tedy výběrem jednoho z možných případů.“* (V takovém případě tedy hovoříme o identifikaci, kdy dochází k porovnávání 1:n, neboť identita osoby není známa a je třeba vyhodnotit celou databázi registrovaných osob.)

Z hlediska právní jistoty lze pochopit, že se zřejmě většina institucí vydá cestou nejmenšího odporu, tj. obstaráním souhlasu podle čl. 9 odst. 2 písm. a) GDPR. V případě dynamického biometrického podpisu by to nicméně mohlo být jinak.

5. ZÁVĚR

DBP snímá „surová“ biometrická data, která jsou využívána pouze pro podepsání dokumentu, jejich využití nebude spojeno s dalším automatickým zpracováním biometrických údajů a DBP není používán pro identifikaci subjektu údajů.

U dynamického biometrického podpisu se nejedná o identifikaci, neboť je to právě daná osoba, která podpisem stvrzuje svoji identifikaci (uvedením jména podepisující osoby, případně dalších údajů, k nimž je podpis připojen) při určitém úkonu, což dokládá vytvořením svého podpisu.[29]

V případech, kdy DBP budou sloužit jako projev právního jednání, nebo v jiných situacích, kdy je přítomnost podpisu důležitá (zdravotnická dokumentace), pak je nasazení DBP jako jednoduché a neobtěžující formy auten-

[28] Např. trestní zákoník, atomový zákon, zákon o ochraně veřejného zdraví apod.

[29] Viz ust. § 561 odst. 1 občanského zákoníku.

tizace podpisu uživatele vysoce přínosné jak při rutinním využívání, tak při zajištění integrity zpracovávaných podepsaných elektronických dokumentů.

Biometrické údaje jsou šifrovány, chráněny proti neoprávněnému přístupu a jsou zpřístupněny třetí osobě (soudnímu znalci) pouze v případě sporu o pravost podpisu, a to velmi formalizovaným postupem obsahujícím vysoké záruky – viz výše.

Stále jde tedy o postup, který odpovídá dřívějšímu názoru ÚOOÚ z roku 2016, podle kterého dochází k použití DBP ve stejném právním režimu, jako při zpracování klasického podpisu, tj. že **nejde o zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby**.

Podle názoru autora by tedy nemělo dojít k přehodnocení výše citovaného stanoviska ÚOOÚ v souvislosti s použitím DBP pro podepisování dokumentů po nabytí účinnosti GDPR, neboť DBP bude využíván stejně jako podpis klasický, tzn. jeho využití nebude spojeno s dalším automatickým zpracováním biometrických údajů a nebude používán pro identifikaci subjektu údajů.

Pro úplnost je ještě třeba uvést, že návrh nového zákona o ochraně osobních údajů, který by měl platit po nabytí účinnosti GDPR, se této problematiky, stejně jako jiných kogentních ustanovení GDPR, netýká.

6. SEZNAM POUŽITÝCH ZDROJŮ

6.1 LITERATURA

[1] ABOUELMEHDI, Karim; BENI-HSSANE, Abderrahim; KHALOUFI, Hayat a Mostafa SAADI. Big data security and privacy in healthcare: A Review. *Procedia Computer Science* [online]. Elsevier B.V, 2017, roč. 113, 2017, s. 73-80. [cit. 2017-10-13]. DOI: 10.1016/j.procs.2017.08.292. ISSN 1877-0509.

[2] CINKAIS, Roman a Jiří VÁBEK. *Důležité otázky při výběru biometrické modality.* Přednáška na konferenci SECURITY 2015, 18. února 2015 [online]. [cit. 2017-21-11]. Dostupné z: http://docplayer.cz/34431484-Dulezite-otazky-pri-vyberu-biometricke-modality-roman-cinkais-jiri-vabek-wincor-nixdorf-s-r-o.html.

[3] DRAHANSKÝ, Martin; DOLEŽEL Michal a Filip ORSÁG. *Biometrie.* Brno: Computer Press, 2011. 294 s. ISBN 9788025489796.

[4] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice. Právní a technologické aspekty.* 2. vydání. Praha: Leges, 2012, s. 286 a násl. ISBN 9788087576366.

[5] RAK, Roman; MATYÁŠ, Václav, ŘÍHA, Zdeněk a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada Publishing, a.s., 2008. ISBN 9788024723655.

[6] SINGH, Simon. *Kniha kódů a šifer.* 1. vydání. Praha: Argo 2003. ISBN 8086569187.

[7] SMEJKAL, Vladimír a Jindřich KODL. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*. Prague, Czech Republic, 13–16 October 2008, s. 1–6. ISBN 9781424418169.

[8] SMEJKAL, Vladimír a Jindřich KODL. Strong authentication using dynamic biometric signature. In: *Proceedings of the 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST)*. Barcelona, Španělsko, 18-21 October 2011, s. 340-344. ISBN 978145770902.

[9] SMEJKAL, Vladimír a Jindřich KODL. Assessment of the authenticity of Dynamic Biometric Signature. The results of experiments. In: *Proceedings of the 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, s. 45–49, ISBN 9781479935307.

[10] SMEJKAL, Vladimír a Jindřich KODL. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16tého ročníku mezinárodní konference Information Security Summit (IS2)*, 27.–28. května 2015, Praha: TATE International, s.r.o., s. 107–119. ISBN 9788086813288.

6.2 PRÁVNÍ PŘEDPISY, SOUDNÍ ROZHODNUTÍ, TECHNICKÉ NORMY A FIREMNÍ DOKUMENTACE

[11] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). CELEX 32016R0679, *Úřední věstník Evropské unie* L 119, 4. 5. 2016, s. 1–88.

[12] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. CELEX 32016L0680, *Úřední věstník Evropské unie* L 119, 4. 5. 2016, s. 89–131.

[13] Rozsudek Nejvyššího správního soudu ze dne 27. února 2014, spis. zn. 4 As 132/2013.

[14] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Změna v hodnocení úrovně právní ochrany biometrických údajů* [online]. [cit. 2017-21-11]. Dostupné z: https://www.uoou.cz/zmena-v-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850.

[15] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Stanovisko č. 1/2017 - Biometrická identifikace nebo autentizace zaměstnanců* [online]. [cit. 2017-21-11]. Dostupné z: https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849/p1 = 1099.

[16] ČSN ISO/IEC 19795-1. *Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura.*

[17] ČSN ISO/IEC 24745. *Informační technologie – Bezpečnostní techniky – Ochrana biometrických informací.*

[18] ISO/IEC 15408-1:2009. *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[19] SIGNOSOFT. *Jak to funguje* [online]. [cit. 2017-11-21]. Firemní dokumentace společnosti SignoSoft s.r.o. Dostupné z: http://www.signosoft.cz/biometrickepodpisy.php.
