26. 8. 2019

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Je používání dynamického biometrického podpisu v rozporu s GDPR?

Tento stručný příspěvek je ve své podstatě upozorněním na problém, který vyděsil řadu již dlouholetých provozovatelů dynamického biometrického podpisu a který spočívá v jednom, ryze individuálním rozhodnutí Úřadu pro ochranu osobních údajů (dále jen ÚOOÚ). To bylo vydáno za nepříliš jasných okolností a neprošlo testem ani v podobě řízení o rozkladu, zejména pak ani v podobě soudního přezkumu. Současně je avízem na podrobný rozbor, který autoři tohoto expozé zpracovali a který vyjde v zářijovém čísle Bulletinu advokacie.

Podstatou problému je to, že ve svém rozhodnutí č.j. UOOU-10138/18-8 ze dne 21. března 2019 ÚOOÚ konstatoval mj., že (kráceno autory):

- Účastník řízení je pobočkou zahraniční banky, kde klienti mohou zažádat o úvěr osobně na pobočce, příp. při nákupu zboží na splátky u obchodního partnera účastníka řízení, nebo online prostřednictvím webového portálu účastníka řízení či u obchodního partnera (klient je automaticky přesměrován na webový portál účastníka řízení).
- V rámci žádosti o úvěr je od klienta vyžadováno vyplnění a podpis rámcové smlouvy, přičemž od klienta je v souvislosti s uzavíráním smlouvy vyžadováno poskytnutí údajů v rozsahu: identifikační údaje – jméno, příjmení, datum a místo narození, rodné číslo, pohlaví; kontaktní údaje – adresa trvalého bydliště, korespondenční adresa, způsob bydlení, telefonní číslo, emailová adresa, kontakt do zaměstnání; údaje o dokladu totožnosti – druh, číslo, datum a místo vydání, platnost; ostatní údaje – rodinný stav, počet a věk vyživovaných dětí, zaměstnání, údaje o zaměstnavateli, základní mzda, čistá mzda, výdaje, typ bydlení, informace o bankovním účtu, informace o dalších příjmech klienta (sociální dávky, příjmy z pronájmu včetně celkového příjmu domácnosti). Účastník řízení v souvislosti s uzavřením smlouvy pořizuje kopii občanského průkazu klienta, kterou následně uchovává. V případě sjednání úvěru prostřednictvím webové portálu shromažďuje a dále uchovává též kopii druhého dokladu totožnosti.
- Při podpisu smluvní dokumentace v elektronické podobě prostřednictvím nespecifikovaného zařízení dochází k vytvoření elektronického podpisu zaznamenávajícího kromě grafické podoby podpisu klienta též biometrické prvky. Ze souhlasu se zpracováním osobních údajů předloženého účastníkem řízení vyplývá, že biometrický podpis je zpracováván za účelem uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu, kdy v případě nutnosti odborník v porovnání s jiným podpisem určí, zda podpis učinila táž osoba či nikoliv.
- Souhlas se zpracováním biometrického podpisu se uděluje na 1 rok, a je-li s klientem uzavřena smlouva, je udělen tento souhlas na dobu jejího trvání a na dobu dalších 10 let od splnění veškerých závazků vůči účastníkovi řízení.
- Ze shromážděné dokumentace vyplývá, že po podpisu dochází k šifrování dat v [neuvedeno] a k jejich následnému připojení k pdf dokumentu.
- V případě, že klient odmítne během uzavírání smluvní dokumentace zpracování osobních údajů za účelem vytvoření biometrického podpisu, je elektronická smlouva stornována a následně je uzavřena smluvní dokumentace v listinné formě. Údaje o klientech jsou uchovávány v elektronické i listinné podobě.

Souhrnně řečeno, právní stav byl takový, že pobočka banky uzavírala úvěrové smlouvy s klienty, získala od nich nejrůznější identifikační a další osobní údaje a na závěr tohoto procesu, za účelem zvýšení právní jistoty o tom, zda byla smlouva podepsána a zda tak učinila ve smlouvě uvedená osoba, byl použit k podpisu dynamický biometrický podpis.
V nám dostupném rozhodnutí mj. ÚOOÚ uvedl, že:

- Účastník řízení na základě povinností vyplývajících mu z právních předpisů, jakož i z jeho vnitřních předpisů osobní údaje klientů shromažďuje, ukládá na nosiče informací, dále používá, předává a likviduje, tedy naplňuje definici zpracování osobních údajů dle nařízení (EU) 2016/679, a to i ve vztahu k biometrickým podpisům a záznamům telefonických hovorů, neboť dochází nejméně k jejich shromažďování a ukládání, popř. výmazu, to vše za účelem jejich možného pozdějšího použití.
- Účel zpracování osobních údajů klientů účastník řízení vymezuje zejména v dokumentech nazvaných Souhlas se zpracováním osobních údajů a Informace o zpracování osobních údajů a o ochraně bankovního tajemství, dále ve všeobecných obchodních podmínkách a ve svých vnitřních předpisech. Primárním účelem, pro který účastník řízení osobní údaje klientů poskytujícím úvěr zpracovává, je uzavření smlouvy o finanční službě a její spravování. Z tohoto primárního účelu (tj. uzavření smlouvy o finanční službě) vyplývají též další související účely zpracování např. řádná identifikace a ověření totožnosti klienta, posouzení jeho úvěruschopnosti, plnění povinností v oblasti účetnictví, předcházení legalizace výnosů z trestné činnosti apod.
- Osobní údaje, které účastník řízení zpracovává v tomto režimu, jsou identifikační údaje v rozsahu jméno, příjmení, rodné číslo, datum a místo narození, místo trvalého pobytu, státní občanství, druh číslo a platnost průkazu totožnosti a orgán, který jej vydal, včetně dalších osobních údajů uvedených na kopii dokladu totožnosti (při uzavírání smluvní dokumentace online dokonce kopie dvou dokladů totožnosti) a údaje nezbytné k posouzení úvěruschopnosti klienta (rodinný stav, počet a věk vyživovaných dětí, údaje o zaměstnavateli, výše příjmů a výdajů aj.).
- Nad rámec těchto osobních údajů účastník řízení dále zpracovává v případě uzavření smlouvy v elektronické formě též biometrické podpisy klientů, kteří s tímto zpracováním vyslovili svůj souhlas. Jak vyplývá zejména z předloženého dokumentu nazvaného Souhlas se zpracováním osobních údajů, má být biometrický podpis zpracováván za účelem uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu.

Na tomto výchozím konstatování se lze zřejmě shodnout. S čím už ale nelze souhlasit, je další tvrzení ÚOOÚ o tom, že „Jsou-li biometrické údaje zpracovávány **za účelem jedinečné identifikace fyzické osoby, jako je tomu zcela zjevně v případě účastníka řízení**, jedná se o zpracování zvláštní kategorie osobních údajů dle čl. 9 odst. 1 nařízení (EU) 2016/679.“ Z ničeho, co je uvedeno výše a dále v cit. Rozhodnutí, nevyplývá, že by DBP byl používán pro identifikaci fyzické osoby, natož jedinečnou. Je pochybné, že ve smlouvě jako takové již před jejím podpisem se nachází více než dostatečné množství údajů, které klienta identifikují.

Podle našeho názoru k jednání v rozporu s čl. 9 odst. 1 GDPR nedochází. Podepisující osoba je identifikována údaji uvedenými v otevřené formě v dokumentu, který podepisuje. DBP – tedy biometrické údaje neslouží tedy k identifikaci, ale pouze naplňuje požadavky ust. § 561-562 občanského zákoníku o právním jednání učiněném v písemné formě. Pokud není k dispozici databáze vzorů (šablon) DBP a nedochází k jejich porovnávání za účelem identifikace osoby, pak lze hovořit i o tom, že v takovém případě DBP vůbec nesplňuje pojmové znaky podle čl. 4 bod 14 GDPR a není biometrickým údajem.

Touto problematikou se druhý z autorů zabýval již dříve před vydáním cit. rozhodnutí. V článku

uveřejněném v roce 2017 v Revue pro právo a technologie [1] dospěl k následujícím závěrům:

„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.

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."

ÚOOÚ dále sice konstatuje, že výjimku z obecného zákazu zpracování zvláštní kategorie osobních údajů pak představuje splnění alespoň jednoho z taxativně vyčtených právních důvodů obsažených v čl. 9 odst. 2 písm. a) až j) GDPR a že zároveň je vždy nezbytné mít pro zpracování osobních údajů také obecný právní titul pro zpracování dle čl. 6 odst. 1 GDPR. Nepopírá, že právním titulem pro zpracování osobních údajů klientů při poskytování úvěru je primárně plnění smlouvy, jejíž smluvní stranou je subjekt údajů dle čl. 6 odst. 1 písm. b) GDPR, a ve vztahu ke zpracování biometrického podpisu, jakožto zvláštní kategorie osobních údajů, se pak uplatní právní důvod dle čl. 9 odst. 2 písm. a) ve spojení s čl. 6 odst. 1 písm. b) GDPR, neboť klienti dali výslovný souhlas se zpracováním této zvláštní kategorie osobních údajů pro účely uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu též biometrický podpis klientů.

Dalo by se říci, že je tedy všechno v pořádku. ÚOOÚ ale následně vyjádřil velmi překvapivý a současnému stavu vědy a techniky neodpovídající názor, že „Správní orgán neshledal, že by biometrický podpis klienta byl pro účely uzavření a uchování smluvní dokumentace či zjednodušení tohoto procesu nezbytný, neboť v případě uzavírání smluv v listinné podobě není také vyžadován. **Správní orgán považuje dostatečné pro výše uvedené účely zpracovávat účastníkem řízení pouze prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné formě**. Tento závěr správního orgánu ohledně nadbytečnosti zpracování biometrického podpisu pak potvrzuje i skutečnost, že účastník řízení v praxi shromažďuje a uchovává biometrické parametry podpisu, avšak de facto využívá pouze prostý elektronický obraz podpisu klienta a biometrické parametry podpisu není schopen bez technologií dodavatele vytěžit. **Správní orgán zdůrazňuje, že skutečnost, že si účastník řízení jako správce osobních údajů nebyl ani vědom toho, že dochází ke zpracování biometrického podpisu i po bezprostředním vytvoření elektronického obrazu podpisu sama o sobě dostačuje ke konstatování nadbytečnosti takto zpracovávaných údajů."**

Je nepochybné, že v daném případě chtěl správce zvýšit právní jistotu (svou i subjektu údajů) o tom, že dokument byl skutečně podepsán osobou, jež je na něm uvedena. Lze se domnívat, že tento postup je v souladu s obsahem bodu 47 recitálu GDPR, podle kterého „Oprávněným zájmem

dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům.“. Obyčejný obrázek, který požaduje ÚOOÚ, neposkytuje ani řádově stejné bezpečnostní záruky jako DBP, když zejména neumožňuje provedení dostatečně průkazného znaleckého posudku posuzujícího pravost podpisu v případě pochybností, či v případě rozporování jeho pravosti podepsanou osobou. Použití DBP je tedy podle názoru autorů ve vztahu k danému účelu oprávněné a plně legitimní. Podle názoru autorů je to právě ÚOOÚ, který svým požadavkem na návrat k zastaralému postupu zvyšuje rizika podvodu, a tedy snižuje bezpečnost celé podpisové, resp. smluvní operace, a to, aniž by pro tento svůj požadavek poskytl odůvodnění opírající se o platnou právní úpravu. Tím snižuje právní sílu podpisu, jehož zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků podle čl. 9 odst. 2 písm. f) GDPR.

Tím ale všechna překvapení obsažená v cit. Rozhodnutí ÚOOÚ nekončí. K argumentaci účastníka řízení, že toto zpracování nemělo dopad na práva subjektů údajů, neboť bylo prováděno s jejich souhlasem, ÚOOÚ uvedl, že ani **souhlas subjektu údajů se zpracováním konkrétních osobních údajů nezbavuje účastníka řízení povinnosti dodržovat všechny základní zásady zpracování osobních údajů, neboť soulad sledovaného účelu a k němu se vztahujícího minimálního rozsahu osobních údajů je nutno hodnotit objektivně, nikoli subjektivně (tj. jako možný předmět dohody uzavřené mezi účastníkem řízení a subjektem údajů).**

GDPR obecně klade na souhlas vyšší požadavky, nežli tomu bylo u předchozí právní úpravy, jak vyplývá především ze čl. 7. Musí se jednat o souhlas nejen svobodný, ale také informovaný, který tak subjekt údajů poskytuje při plném vědomí toho, s čím souhlasí, kromě toho má být odlišitelný od jiných skutečností a srozumitelný. GDPR v čl. 7 odst. 2 výslovně stanoví důsledek porušení těchto požadavků na souhlas tak, že jakákoli část prohlášení, která by představovala porušení GDPR, *„není závazná“*.

Základní zásady GDPR, včetně zásady minimalizace údajů, podle které musí být osobní údaje *„přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány“*, se aplikují na každé zpracování, bez ohledu na jeho právní základ. Použijí se tak i na zpracování založené na souhlasu subjektu údajů. Způsob použití této zásady v rozebíraném rozhodnutí ÚOOÚ, který je ve svém důsledku de facto zpochybněním práva osoby jinak svéprávné souhlas poskytnout, považují autoři za nesprávný a postrádající oporu v platné právní úpravě GDPR. Dle hodnocení autorů platí, že jsou-li splněny požadavky kladené GDPR na souhlas a účel zpracování, k němuž byl souhlas udělen, je legitimním, nadále trvá a zpracování daných kategorií osobních údajů je k danému účelu potřebné, pak není možno udělený souhlas bagatelizovat závěrem o nadbytečnosti zpracování. Autoři navíc považují za zcela nesprávné dovodit nadbytečnost zpracování osobních údajů z existence alternativní možnosti zpracování, kterou správce nabízí těm osobám, které souhlas dobrovolně neposkytly.

Bod 42 recitálu GDPR mj. uvádí, že *„Lze předpokládat, že souhlas není svobodný, není-li možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů, i když je to v daném případě vhodné, nebo je-li plnění smlouvy, včetně poskytnutí služby učiněno závislým na souhlasu, i když to není pro toto plnění nezbytné.“ Podobně uvádí čl. 7 odst. 4 „Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.“*

Právě alternativní možnost je základní podmínkou skutečně svobodného souhlasu. Posouzení její existence jako důkazu o nadbytečnosti zpracování založeného na souhlasu pak autoři neváhají označit jako zcela absurdní. Platná právní úprava GDPR ani zákona č. 110/2019 Sb. o zpracování osobních údajů nedává dle hodnocení autorů ÚOOÚ oprávnění zpochybnit zpracování kategorií údajů

zahrnutých v poskytnutém souhlase, pro účely v souhlase vymezené, v situaci, kdy se jedná o zpracování legitimní, pro daný účel přiměřené, relevantní a omezené na nezbytný rozsah a také souhlas splňuje požadavky stanovení GDPR. Autoři jsou přesvědčeni, že v případě zpracování založeném na souhlasu, resp. výslovném souhlasu subjektu údajů, je obecně aplikace zásady minimalizace do jisté míry limitována právě poskytnutým souhlasem, a tedy nemožností ingerence orgánu dozoru do právního jednání učiněného svéprávnou fyzickou osobou; posuzování přiměřenosti, relevantnosti a nezbytného rozsahu se tak zaměří především na aspekt časový, tedy na to, zda zpracovávané údaje ještě stále tato kritéria splňují. Opačný závěr by totiž v praxi vedl k absurdním situacím, kdy by orgán dozoru byl oprávněn de facto negovat právní jednání svéprávné fyzické osoby, kterýmžto oprávněním ho zákonodárce (ani evropský zákonodárce) vybavit zajisté nemínil a ani z textu GDPR, či jiného relevantního předpisu tak nelze usuzovat. V posuzovaném případě však autoři nepovažují za nutné tuto úvahu dále rozvíjet, když podpis, v případě dokumentů v elektronické formě DBP, je dle hodnocení autorů zcela jednoznačně údajem přiměřeným, relevantním a omezeným na nezbytný rozsah ve vztahu k účelu zpracování, a to zvláště v případě, kdy je DBP zpracováván na základě výslovného souhlasu podepisující osoby. Ostatně i zákon č. 89/2012 Sb. občanský zákoník je postaven na zásadě uplatňující se na posuzování soukromoprávních jednání, vyjádřené v § 574, dle které *„Na právní jednání je třeba spíše hledět jako na platné než jako na neplatné.“*

Jak je uvedeno výše, návrat k používání pouhého obrázku, navíc v digitální formě, kde nelze rozlišit originál a kopii, extrémním způsobem zvyšuje riziko zhotovení padělku nebo popírání pravosti vlastního podpisu. Požadavek na náhradu DBP prostým obrázkem podpisu na základě důvodu jeho údajné „nadbytečnosti“ je v rozporu s požadavky na snižování rizika a zvýšení spolehlivosti podepisovacího procesu. Proto je třeba tento krok hodnotit jako požadavek, který je v rozporu nejen se zájmy smluvních stran, ale i se současným požadavkem na zvyšování právní jistoty a bezpečnosti transakcí.

Nelze samozřejmě vyloučit, že se jedná o hluboké nedorozumění způsobené nedostatečným seznámením s technickou stránkou DBP, a to na straně účastníka řízení a následně ÚOOÚ a z toho vyplývajícím závěrem o tom, že DBP je biometrickým údajem ve smyslu čl. 4 odst. 14 GDPR na základě pouhého výskytu slova "biometrický" v názvu DBP. Mohla by tomu nasvědčovat i skutečnost, že jde o ryze české národní rozhodnutí, které se neopírá o žádné z autorům známých doporučení Evropského sboru pro ochranu osobních údajů. Tím spíše je třeba věnovat tomuto rozhodnutí a jeho analýze mimořádnou pozornost.

Závěrem považují autoři za vhodné ocitovat rozhodnutí Nejvyššího správního soudu, které souvisí s podepisováním.[2] Ve svém rozhodnutí NSS poměrně přiléhavě uvedl k podpisu jako takovému:
„Podpis, není-li úředně ověřen, totiž za běžných okolností není nic víc než omezeně spolehlivý autentifikační prostředek – jeho přítomnost na podání obvykle zvyšuje pravděpodobnost, že je učinil vskutku ten, kdo v něm je za podatele označen, ale málokdy o tom dává jistotu. Za normálních okolností, chovají-li se lidé rozumně a poctivě, z čehož je nutno vycházet, je nepochybně jakousi "originální značkou" toho, kdo se podepsal. Není však příliš obtížné běžný (neověřený) podpis padělat, napodobit či vytvořit (ať ve zlém či dobrém úmyslu) podání pouze navenek vypadající jako učiněné osobou, jež je v něm za podatele deklarována, a toto podání podepsat zcela jiným podpisem, než jaký skutečně užívá osoba, jíž je podání přičítáno.“ Právě proto, že – jak konstatuje NSS – je podpis pouze omezeně spolehlivý autentifikační prostředek, je tím plně odůvodněno v zájmu zvýšení právní jistoty všech smluvních stran používání DBP místo obyčejného obrázku, když DBP výrazně zvyšuje možnost ověření jeho pravosti. Pokus o zamezení používání DBP, který by se dal dovozovat z předmětného rozhodnutí ÚOOÚ, tedy dle názoru autorů není v souladu s celospolečenskými zájmy.

JUDr. Martin MAISNER, Ph.D., MCIArb,
advokát, len představenstva České advokátní komory, předseda Odborné skupiny ČAK pro právo informačních technologií a GDPR,

Prof. Ing. Vladimír SMEJKAL, CSc., LL.M., DrSc.,
mezinárodně uznávaný odborník, vysokoškolský pedagog (Fakulta podnikatelská VUT v Brně) a soudní znalec v Praze, člen Legislativní rady vlády v letech 2004-2014

JUDr. Miroslav UŘIČAŘ,
AK LEGALITÉ, rozhodce, člen Komise pro správní právo Legislativní rady vlády ČR a rozkladové komise ERÚ

_____

[1] Smejkal, V. Dynamický biometrický podpis a nařízení GDPR. Revue pro právo a technologie, VIII., 2017, č. 16, s. 89–112. ISSN 1804-5383 (Print), ISSN 1805-2797 (Online).
[2] Rozsudek Nejvyššího správního soudu ze dne 27. 7. 2017, spis. zn. 2 As 80/2017.

Další články:

- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory
- Jak fungují plánovací smlouvy v reálných situacích (2. díl)