Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7, Tel.: 234 665 111, Fax: 234 665 444; e-mail: posta@uoou.cz

STANOVISKO č. 2/2014

červenec 2014[1]

Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů

Úvod

Úřad pro ochranu osobních údajů (dále jen "Úřad") se v rámci své konzultační činnosti setkává s problematikou tzv. dynamického biometrického podpisu, často označovaným také jako digitální nebo elektronický podpis umožňující automatické rozpoznávání biometrických prvků. Jedná se o nahrazení tradičního podepisování se na papír za podepisování se na speciální zařízení (tablet nebo tzv. signpad) pro snímání podpisu, prostřednictvím kterého dochází jak k zachycení grafické podoby vlastnoručního podpisu na obrazovce tohoto zařízení, tak i k zachycení tzv. dynamických parametrů pohybu ruky jako je tlak, rychlost, sklon, křivky, posloupnost tahů apod. Následně je tento podpis, resp. jeho grafická podoba, společně s dynamickými parametry pohybu ruky převeden do elektronické podoby, většinou zašifrovaně, a takto je připojen k podepisovanému dokumentu. Tento nový způsob podepisování začínají již v praxi využívat při jednání se zákazníky například někteří telefonní operátoři, banky či pojišťovny anebo také poskytovatelé poštovních služeb.

Využití technologie biometrického podpisu může sice přinést značnou úsporu nákladů především v oblasti uchovávání smluvní dokumentace, úsporu času spočívající ve zrychlení obchodních a smluvních procesů, vyšší míru jistoty při ověřování pravosti podpisů a zvýšení celkové efektivity činnosti. Jsou s ním však také spojena rizika týkající se mimo jiné ochrany osobních údajů podepisovaných osob. Lze předpokládat, že k zavedení této technologie budou přistupovat i další subjekty, a proto Úřad považuje za nezbytné se souvisejícími otázkami ochrany osobních údajů zabývat.

Aplikace zákona o ochraně osobních údajů

Pravidla zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, ve smyslu ustanovení § 3 vymezujícího působnost tohoto zákona je nutné aplikovat, pokud dané jednání naplňuje definiční znaky zpracování a předmětem takového jednání je informace spadající do kategorie osobních údajů, přičemž současně není dán důvod pro vyloučení takového jednání z působnosti tohoto zákona.

Osobním údajem podle § 4 písm. a) zákona č. 101/2000 Sb. je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, pokud jej lze na základě poskytnutých informací přímo či nepřímo identifikovat. Podpis lze považovat za jakousi jedinečnou osobní značku člověka, kterou nejen v závazkových vztazích projevuje svoji vůli, tj. vyjadřuje svůj souhlas s danou smlouvou. Jak na základě vlastnoručního podpisu na papír, tak i dynamického biometrického

[1] Podle stavu právních předpisů k 1. červenci 2014.

podpisu s použitím dalších údajů, kterými správce údajů ve smluvních vztazích obvykle disponuje, je podepsaná osoba bezesporu identifikovatelná. V obou případech proto podpis naplňuje znaky osobního údaje dle citovaného ustanovení zákona.

Existence osobního údaje však sama o sobě ještě nezakládá působnost zákona č. 101/2000 Sb., a proto je nutné, aby s takovým údajem byla za určitým účelem prováděna jakákoliv operace nebo soustava operací odpovídajících pojmu zpracování podle § 4 písm. e) zákona č. 101/2000 Sb. Těmito operacemi s osobními údaji se rozumí zejména jejich shromažďování, ukládání na datové nosiče, uchovávání, zpřístupňování, zveřejňování, třídění apod.[2] V kontextu ochrany osobních údajů je u uvedených operací důraz kladen na účelovost jejich provádění. Pro naplnění definice zpracování osobních údajů je rozhodující, aby předmětné jednání spočívající v nakládání s osobními údaji představovalo cílené využívání osobních údajů.

Při shromažďování osobních údajů klientů v rámci smluvní dokumentace, která obsahuje i podpisy, a při dalších operacích prováděných s těmito údaji, tedy uchovávání, využívání pro ověřování podpisů při běžných transakcích nebo v případě sporu o platnost podpisu atd., dochází ke zpracování osobních údajů, a to všech předmětných informací včetně podpisu.

Samotné podepsání se ještě sice není zpracováním osobních údajů, ale při užívaní technologie biometrického podepisování, na rozdíl od klasického podpisu na papír, je automaticky speciálním zařízením (tablet, signpad) již při podepsání nejdříve snímaná a poté zaznamenána grafická podoba podpisu, přičemž jsou současně vygenerovány a uloženy dynamické parametry pohybu ruky podepisující se osoby. Tímto způsobem dochází cíleně ke sběru údajů, jejich shromažďování, ukládání na datové nosiče, uchovávaní [tzn. jejich zpracování ve smyslu § 4 písm. e) zákona č. 101/2000 Sb.], a to vše za účelem, aby údaje mohly být v případě potřeby dále použity. Údaje jsou většinou současně převedeny do elektronického formátu v určitém např. číselném vyjádření, přičemž zůstává zachována i grafická podoba vlastnoručního podpisu.

Pokud jsou naplněny všechny předpoklady pro aplikaci zákona č. 101/2000 Sb., zbývá ještě určit subjekt, který bude za zpracování osobních údajů odpovídat, tedy správce osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb. Ve smyslu tohoto ustanovení bude správcem ten subjekt, který určuje účel zpracování, a nezmocní-li nebo nepověří-li zpracováním zpracovatele, také zpracování provádí a odpovídá za něj. V praxi bude tímto správcem například banka nebo telefonní operátor, který technologii biometrického podpisu zavede do své činnosti a bude jí při styku s klienty využívat, neboť evidentně právě tento subjekt určuje jak účel, tak i prostředky daného zpracování. Jako správce osobních údajů pak musí plnit všechny povinnosti stanovené zákonem č. 101/2000 Sb.

Dynamický biometrický podpis jako citlivý údaj

Zvláštní kategorií osobních údajů tvoří citlivé údaje. Ustanovení § 4 písm. b) zákona č. 101/2000 Sb. citlivý údaj definuje jako informaci týkající se identifikované či identifikovatelné fyzické osoby, která současně spadá do některé ze zde taxativně uvedených zvláštních kategorií osobních údajů, mj. se jedná také o biometrické údaje umožňující přímou identifikaci nebo autentizaci konkrétního člověka.[3] V případě, že následně dochází ke zpracování citlivých údajů, je nutné aplikovat přísnější režim, protože právě takové zpracování může způsobit mnohem závažnější zásah do soukromí subjektu údajů, než je tomu v případě zpracování „obyčejných“ osobních údajů.

[2] Blíže k pojmu zpracování osobních údajů viz stanovisko Úřadu č. 4/2013 K pojetí zpracování osobních údajů.
[3] Viz § 4 písm. b) zákona č. 101/2000 Sb.

Písmo a stejně tak i podpis, zachyceny v jakékoliv podobě, lze považovat za jedinečný znak každého jednotlivce. Podrobnou analýzou vlastnoručního podpisu lze zpracovávat nejrůznější informace o pohybu ruky v době pořízení podpisu, jako například sklon písma, tlak ruky, rychlost psaní, velikost písma apod., z nichž pak znalec dokáže tuto osobu s větší, či menší mírou pravděpodobnosti identifikovat nebo autentizovat. Tyto informace, resp. dynamické rysy odpovídají definici biometrického, a tedy i citlivého údaje ve smyslu zákona 101/2000 Sb. Klasický podpis zachycený na papír, a stejně tak i dynamický biometrický podpis obsahují odpovídající sumu informací (sklon písma, tlak a rychlost psaní atd.), a jsou tedy nositeli biometrických údajů.

Při posuzování další aplikace zákona č. 101/2000 Sb. je nezbytné vycházet z toho, co je o zpracování údajů výše uvedeno. Samotné pořizování a uchovávání podpisu bez jeho využití jako citlivého údaje proto nelze bez dalšího považovat za zpracování citlivých údajů. K takovému zpracování dochází až tehdy, pokud je podpis např. podroben písmoznalecké analýze za účelem ověření jeho pravosti v případě sporu. O zpracování citlivých údajů obsažených v podpisu se jedná, pokud tyto údaje jsou správcem aktivně využívány. Takový názor lze analogicky dovodit i ze stanoviska WP29 č. 5/2009[4], ve kterém je uvedeno, že samotná fotografie fyzické osoby zveřejněná na internetu, která je bezpochyby také nositelem biometrických a dalších citlivých údajů, není citlivým údajem, pokud taková fotografie není jasně užita k dalším účelům, např. k odhalení v ní obsažených citlivých údajů. Bez dalšího tedy nelze ani na klasický podpis na papír nahlížet jako na citlivý údaj ve smyslu zákona č. 101/2000 Sb.

V případě dynamického biometrického podpisu však ke zpracování citlivých údajů dochází automaticky. Dynamické prvky jsou speciální technologií cíleně vygenerovány a zachyceny jako přidaná hodnota k samotnému grafickému znázornění podpisu, takže grafické znázornění a biometrické údaje existují vedle sebe a v této podobě jsou s nimi prováděny i následné operace. Zpracování citlivých údajů se při použití technologie biometrického podepisování lze vyhnout pouze v případě, kdy zařízení zaznamená pouze grafickou podobu podpisu, tedy pokud nedojde ke zpracování biometrických údajů. V případech kdy budou správci prostřednictvím technologie vytvářet podpisové vzory a databáze těchto vzorů, je z podstaty věci zřejmé, že musí docházet i ke zpracování citlivých údajů, a je proto nezbytné, aby takové zpracování vždy probíhalo v přísnějším režimu § 9 zákona č. 101/2000 Sb.

Povinnosti při zpracování údajů podle zákona č. 101/2000 Sb.

Zákon č. 101/2000Sb. stanoví každému správci řadu povinností, přičemž většina z nich se aplikuje stejně na zpracování „obyčejných“ osobních údajů i citlivých údajů. Základní povinnosti správce jsou uvedeny v § 5 odst. 1 zákona č. 101/2000 Sb. Ještě před započetím daného zpracování je nutné ve smyslu § 5 odst. 1 písm. a) a b) zákona č. 101/2000 Sb. nejdříve stanovit základní parametry zpracování, tedy účel, k němuž mají být údaje zpracovány a pak způsob a prostředky tohoto zpracování. Právě splnění těchto povinností předurčuje charakter daného zpracování. V průběhu zpracování je správce povinen dodržet všechny další podmínky stanovené v odst. 1, přičemž je zejména nutné dbát na dodržení § 5 odst. 1 písm. d) zákona č.101/2000 Sb., tedy vždy zpracovávat pouze údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

Nezbytnou podmínkou každého zpracování je existence zákonem uznaného právního titulu pro zpracování údajů. Zpracování osobních údajů může v souladu s § 5 odst. 2 zákona č. 101/2000 Sb. probíhat buď na základě souhlasu subjektu údajů, nebo na základě

[4] Dokument Pracovní skupiny pro ochranu dat podle článku 29 (WP 29) směrnice 95/46/ES je dostupný na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

některého z dalších právních titulů uvedených pod písm. a) až g) tohoto ustanovení. Pokud je podpis zpracováván pouze jako „obyčejný“ osobní údaj, lze aplikovat především právní titul podle § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., který se uplatní právě v případě zpracování nezbytného pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

V případě dynamického biometrického podpisu je však vzhledem k citlivému charakteru zpracovaných údajů nutné postupovat v přísnějším režimu § 9 zákona č. 101/2000 Sb. Ze zde uvedeného výčtu možných právních titulů pro zpracování citlivých údajů pak v případě dynamického biometrického podpisu přichází v úvahu pouze souhlas dotčené osoby. Oproti souhlasu se zpracováním „obyčejných“ osobních údajů je zde navíc stanovená kvalifikovaná forma souhlasu, spočívající v jeho výslovnosti. Správce, který bude prostřednictvím technologie biometrického podepisování zpracovávat citlivé údaje fyzické osoby, tedy musí disponovat jejím jednoznačným a výslovným souhlasem.

Podle názoru Úřadu na cílené zpracování citlivých údajů prostřednictvím dynamického biometrického podpisu v zásadě žádný jiný právní titul podle § 9 zákona č. 101/2000 Sb. aplikovat nelze.

Při zpracování citlivých údajů na základě výslovného souhlasu podle § 9 písm. a) zákona č. 101/2000 Sb. musí správce vůči subjektu údajů ještě před udělením tohoto souhlasu splnit informační povinnost v tomto ustanovení uvedenou, která se fakticky shoduje s informační povinností podle § 11 zákona č. 101/2000 Sb. Subjekt údajů musí být informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Obsahem plnění informační povinnosti u dynamického biometrického podepisování musí být i informace o tom, že prostřednictvím technologie pro automatické rozpoznávání biometrických prvků jsou jako neoddělitelná součást grafické podoby podpisu zaznamenávány i další informace, a jaké, tedy dynamické parametry pohybu ruky podepisující se osoby, které splňují definici citlivého údaje podle § 4 písm. b) zákona č. 101/2000 Sb. Tuto povinnost lze v praxi plnit například prostřednictvím smluvních podmínek. Správce musí subjekt údajů také poučit o právu na přístup k informacím o zpracování podle § 12 zákona č. 101/2000 Sb. a povinnostech správce související s ochranou práv subjektu údajů podle § 21 zákona č. 101/2000 Sb. K poskytnutí těchto informací musí dojít nejpozději současně s udělením výslovného souhlasu, přičemž správce tento souhlas musí být schopen prokázat po celou dobu zpracování. Pokud subjekt údajů odmítne správci udělit souhlas ke zpracování citlivých údajů, musí mu správce umožnit podepsat se klasickým způsobem přímo na papírový dokument.

Vzhledem k povaze zpracování údajů v případě dynamického biometrického podpisu, je nutné upozornit na povinnosti týkající se zabezpečení osobních údajů podle § 13 zákona č. 101/2000 Sb. Toto ustanovení správci ukládá, aby zajistil, že k údajům nebude moci mít žádná třetí osoba neoprávněný nebo nahodilý přístup a že nedojde k jejich změně, zničení, ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpracování. Odpovědnost za plnění této povinnosti je zákonem konstruována jako objektivní, tzn. v případě, kdy osobní údaje například budou přístupné neoprávněné osobě, budou v průběhu přenosu ztraceny, změněny apod., bude jednání správce porušením § 13 zákona č. 101/2000 Sb., a tedy správním deliktem, za který nebude odpovídat pouze v případě, že prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil (viz § 46 odst. 1 zákona č. 101/2000 Sb.). Vzhledem k citlivému charakteru zpracování biometrických údajů je nutné právě u tohoto zpracování klást na zabezpečení údajů zvláštní důraz. V praxi to znamená zejména užívání kvalitní a ověřené technologie pro pořizování dynamického biometrického podpisu, náležité šifrování surových biometrických údajů, zajištění bezpečnosti přenosu údajů a jejich dalšího uchovávání, zajištění nevratné likvidace atd.

Je také nutné zmínit oznamovací povinnost vůči Úřadu podle § 16 zákona č. 101/2000 Sb. Tuto povinnost správce nemusí plnit pouze v případě, že se na něj vztahuje některá výjimka z oznamovací povinnosti podle § 18 tohoto zákona. Zpracování klasického podpisu jako osobního údaje sice Úřadu není potřeba oznamovat, avšak v souvislosti s výše uvedenými pravidly pro posuzování zpracování údajů prostřednictvím technologie biometrického podepisování lze konstatovat, že v případě zpracování biometrických údajů se již jedná o kvalitativně odlišné, a tedy nové zpracování. Na takové zpracování nelze uplatnit žádnou z výjimek z oznamovací povinnosti dle § 18 odst. 1 zákona č. 101/2000 Sb., a správce tak bude povinen ještě předtím, než zpracování zahájí, tuto skutečnost Úřadu oznámit.

Vzhledem k povaze dynamického biometrického podpisu jako neměnného, resp. obtížně změnitelného údaje, je třeba upozornit na značná rizika spojená s jeho odcizením resp. s přístupem neoprávněné osoby k těmto údajům. Proto je třeba, aby před poskytnutím biometrických údajů o podpisu a udělením souhlasu s jejich zpracováním, každý důkladně posoudil důvěryhodnost správce, kterému tyto osobní údaje poskytuje.

Závěr

Podpis v jakékoliv podobě je osobním údajem a ve smluvních vztazích dochází k jeho zpracování. Klasický a stejně tak i dynamický biometrický podpis obsahují biometrické údaje, při využívaní technologie dynamického biometrického podepisování však dochází k jejich automatickému zpracování, které může probíhat pouze v režimu § 9 zákona č. 101/2000 Sb. Jediným právním titulem, na základě kterého je takové zpracování obecně realizovatelné, je výslovný a informovaný souhlas každého subjektu údajů podle § 9 písm. a) zákona č. 101/2000 Sb., který musí být správce schopen prokázat po celou dobu zpracování. O zpracování citlivých údajů tedy musí být subjekt údajů řádně informován a správce musí plnit všechny další povinnosti, které se vztahují jak na zpracování osobních, tak i citlivých údajů podle zákona č. 101/2000 Sb. Zvýšenou pozornost je nutné věnovat zejména plnění informační a oznamovací povinnosti a zabezpečení biometrických údajů. Vzhledem k současnému vývoji a novým trendům je potřeba uvést, že výše uvedená pravidla ochrany osobních údajů budou obdobně platit i pro další technologie zpracovávající biometrické údaje umožňující identifikaci či autentizaci subjektů údajů.