27. 6. 2019

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

# Konec dynamického biometrického podpisu v ČR?

Používání dynamického biometrického podpisu („DBP“) namísto tradičního podpisu na papír je v České republice stále populárnější. Tento způsob podepisování využívají např. finanční instituce či telefonní operátoři. Důvodem je zejména urychlení smluvních procesů, úspora nákladů a především vyšší úroveň autenticity dokumentů podepsaných DBP.

Cílem tohoto článku je zhodnotit, nakolik je uvedený trend ohrožen aktuálním postojem a rozhodovací praxí Úřadu pro ochranu osobních údajů („**Úřad**“).

**Co je DBP?**

Zjednodušeně lze říci, že DBP vedle samotné grafické podoby podpisu obsahuje i informace o tom, jak byl podpis vytvořen.

RANDA HAVEL ■ LEGAL

DBP vzniká snímáním vlastnoručního podpisu s využitím speciálního zařízení (tablet nebo tzv. signpad). Ten zachycuje dynamické vlastnosti podpisu, jako jsou čas, tlak, rychlost, forma a tvar, křivky, celková velikost atd. Uvedené vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce. Oproti běžnému podpisu tak DBP umožňuje lépe ověřit a potvrdit, že dokument skutečně podepsala deklarovaná osoba.

Z právního hlediska je DBP druh elektronického podpisu. Ve smyslu nařízení eIDAS[1] a zákona o službách vytvářejících důvěru pro elektronické transakce[2] se jedná o tzv. prostý elektronický podpis, který je postaven naroveň klasickému vlastnoručnímu podpisu na papír.

Stejně jako klasický podpis představuje i DBP osobní údaj ve smyslu čl. 4 bodu 1) obecného nařízení o ochraně osobních údajů[3] („**GDPR**“). Jelikož DBP zachycuje biometrickou stopu podepisující osoby, patří DBP mezi tzv. biometrické údaje ve smyslu čl. 4 bodu 14) GDPR[4].

**Dosavadní postoj Úřadu k DBP**

K DBP se opakovaně vyjadřoval též Úřad. Názory Úřadu ve vztahu k DBP přitom prošly značným vývojem.

Ve svém stanovisku č. 3/2009 se Úřad nezabýval přímo DBP, ale obecně systémy, které zpracovávají biometrické údaje. Úřad tyto systémy rozdělil na (a) systémy zpracovávající „běžné“ osobní údaje a (b) systémy zpracovávající tzv. citlivé údaje[5], které vyžadují přísnější režim ochrany. Klíčovým hlediskem pro zařazení konkrétního systému do jedné z těchto kategorií byla skutečnost, zda jsou v jeho rámci zpracovávány (i) úplné biometrické údaje nebo (ii) pouze jejich šablony[6]. V prvním případě se podle stanoviska Úřadu jednalo o zpracování citlivých údajů, ve druhém pak o zpracování běžných osobních údajů.

Stanovisko č. 2/2014 se již zaměřilo na problematiku DBP z pohledu tehdy platného zákona o ochraně osobních údajů[7] („**ZOOÚ**“). Úřad zde konstatoval, že v případě DBP dochází ke zpracování citlivých údajů. Právním titulem umožňujícím takové zpracování realizovat byl podle Úřadu pouze souhlas dotčené osoby.

V červnu 2017 Úřad uveřejnil na svých stránkách zprávu s názvem Změna v hodnocení úrovně právní ochrany biometrických údajů[8]. V této zprávě s odvoláním na novou právní úpravu (GDPR) opustil dosavadní dělení systémů s biometrickými údaji, které představil ve svém stanovisku č. 3/2009. Úřad deklaroval, že jakýkoliv systém, který shromažďuje biometrické údaje za účelem identifikace fyzické osoby, bude považovat za systém zpracovávající zvláštní kategorie osobních údajů[9]. Současně Úřad přislíbil, že k biometrickým údajům zveřejní nové stanovisko[10].

**Rozhodnutí Úřadu**

K využití DBP se Úřad vyjádřil i ve svém rozhodnutí z března 2019[11] („**Rozhodnutí**“). Rozhodnutí bylo vydáno v návaznosti na kontrolu zpracování osobních údajů u finanční instituce („**Kontrolovaná osoba**“). Ta zpracovávala DBP na základě souhlasů svých klientů. Kontrolovanou osobou stanoveným účelem zpracování DBP bylo uzavření a uchovávání smluvní dokumentace, zjednodušení tohoto procesu a v případě potřeby určení, zda se jedná o podpis té které osoby.

Úřad v rámci kontroly a navazujícího správního řízení dospěl k závěru, že Kontrolovaná osoba zjevně zpracovávala DBP za účelem jedinečné identifikace klientů, a jednalo se tedy o zpracování zvláštní kategorie osobních údajů. Dále konstatoval, že zpracování DBP není nezbytné k účelům zpracování, které odsouhlasili klienti Kontrolované osoby[12].

V návaznosti na svou úvahu o nikoli nezbytném zpracování DBP Úřad uzavřel, že Kontrolovaná osoba porušila zásadu minimalizace údajů[13]. Za porušení povinností při zpracování osobních údajů klientů[14] pak Úřad uložil Kontrolované osobě pokutu ve výši 250.000 Kč.

**Co dál?**

Podle autorů tohoto článku by bylo chybou závěry Úřadu uvedené v Rozhodnutí zobecnit a plošně aplikovat na všechny systémy založené na DBP. Takový přístup by mohl mít za následek konec používání DBP v České republice, včetně ztráty benefitů DBP (především vyšší míry jistoty při zpochybnění pravosti podpisu).

Zejména považujeme za nezbytné zdůraznit, že biometrické údaje představují osobní údaje zvláštní kategorie pouze tehdy, jsou-li zpracovávány za účelem jedinečné identifikace fyzické osoby[15]. To však u DBP zpravidla neplatí. Ve většině případů DBP není zpracováván s cílem identifikovat[16] podepisující osobu, ale umožnit její (následnou) autentizaci[17].

Rizika plynoucí z Rozhodnutí tak lze minimalizovat již vhodným nastavením systému DBP. Pokud bude systém založený na DBP sloužit k autentizaci podepisující osoby, nebude se jednat o zpracování zvláštních kategorií osobních údajů a zpracování bude probíhat mimo režim čl. 9 GDPR[18].

V závislosti na konkrétním nastavení systému pak podle našeho názoru může docházet ke zpracování DBP i bez souhlasu dotčené fyzické osoby. Zpracování DBP se může opírat např. o oprávněné zájmy správce[19]. Tento účel zpracování považujeme za legitimní, neboť DBP pomáhá správci předcházet či řešit případné spory o pravost podpisu. Zpracování DBP pro tyto účely lze považovat za přiměřené, relevantní a neporušující zásadu minimalizace údajů podle GDPR.

**Závěr**

Podle autorů článku zpracování DBP za účelem autentizace fyzické osoby (a) nezakládá zpracování zvláštních kategorií osobních údajů ve smyslu článku 9 GDPR a (b) je možné i bez souhlasu dotčené fyzické osoby.

Do doby vyjasnění aktuálního postoje a rozhodovací praxe Úřadu k DBP nicméně nelze zaručit, že Úřad bude na systémy založené na DBP nahlížet stejným způsobem. V tomto směru bude klíčové avizované stanovisko Úřadu k biometrickým údajům.

**Mgr. Matyáš Kužela**,
partner

**Mgr. Tomáš Zwinger**,
advokát

ŘANDA HAVEL LEGAL advokátní kancelář s.r.o.

Truhlářská 13-15
110 00  Praha 1

Tel.:  +420 222 537 500 – 501
Fax:  +420 222 537 510
e-mail:  office.prague@randalegal.com

---

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, čl. 3 bod 10.
[2] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, § 7.
[3] 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).
[4] Biometrickými údaji se 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.
[5] Citlivým údajem se rozumí osobní údaj 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. Viz § 4 písm. b) tehdy platného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[6] Převedené do číselného údaje bez možnosti zpětné rekonstrukce zpět na úplný biometrický údaj.
[7] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[8] K dispozici >>> zde.
[9] Zvláštní kategorií osobních údajů se podle čl. 9 odst. 1 GDPR rozumí údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
[10] To však dosud nebylo uveřejněno.
[11] Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. března 2019, č.j. UOOU-10138/18-8, k dispozici >>> zde.
[12] Tedy uzavření a uchovávání smluvní dokumentace, zjednodušení tohoto procesu a v případě potřeby určení, zda se jedná o podpis té které osoby.
[13] Jedná se o jednu ze základních zásad zakotvenou v čl. 5 odst. 1 písm. c) GDPR.
[14] Zpracování DBP klientů nebylo jediným porušením Kontrolované osoby deklarovaným v Rozhodnutí.
[15] Srov. článek 9 odst. 1 GDPR.
[16] Identifikace je proces určení identity subjektu. Tento proces je založen na výběru konkrétního subjektu z řady ostatních osob. Proces identifikace tak probíhá nad celou databází (její částí), výběrem jednoho z řady záznamů (porovnání 1:n). V případě DBP by proces identifikace probíhal tak, že systém by po zachycení DBP provedl výběr nad databází více záznamů DBP a z těchto záznamů vybral jeden odpovídající záznam.
[17] Autentizace (verifikace) je proces ověření (deklarované) identity subjektu. Identita je přitom ověřována pouze ve vztahu k deklarovanému subjektu. Proces autentizace tedy neprobíhá nad celou databází záznamů, ale pouze ve vztahu k záznamu konkrétní osoby (porovnání 1:1). V případě DBP proces autentizace probíhá tak, že systém porovná zachycený záznam DBP s konkrétním záznamem vedeným v databázi. Výběr záznamu z databáze je přitom proveden na základě jiných údajů/vlastností než je DBP.
[18] Pro úplnost uvádíme, že se jedná o rozdíl oproti minulé právní úpravě, která považovala za citlivé i biometrické údaje umožňující autentizaci fyzické osoby; srov. § 4 písm. b) ZOOÚ. V tomto ohledu lze konstatovat, že GDPR je ke zpracování biometrických údajů benevolentnější než byl ZOOÚ.
[19] Podle čl. 6 odst. 1 písm. f) GDPR.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

## Další články:


- Pozemkové úpravy aneb „malé“ vyvlastnění
- Nová éra v boji proti nekalým obchodním praktikám: Co přinese nové procesní nařízení EU?
- Licence LUC v podnikatelské strategii provozovatelů dronů
- Péče rodičů po novele od 1.1.2026
- K ukončování služebního poměru po novele zákona o státní službě
- Aktuality z práva internetu: kybernetická bezpečnost a online řešení sporů
- Zelené standardy pro výstavbu a renovace: jaké povinnosti přinese nová evropská úprava?

- Byznys a paragrafy, díl 25.: Započtení
- Zrušení bytového spoluvlastnictví včetně limitů soudní ingerence
- 2. díl ze série Pravidla a odpovědnost při provozování zimních sportů: Povinnosti provozovatele při závodech a trénincích: zabezpečení tratí a oddělení veřejného a sportovního provozu
- Protokol o předání díla jako podmínka zaplacení jeho ceny a k možné změně soudní praxe