ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-00982/21-5

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle čl. 58 odst. 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) a § 60 zákona č. 110/2019 Sb. o zpracování osobních údajů, rozhodl dne 3. března 2021 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, takto:

Účastníku řízení, [redacted] (dále jen „účastník řízení"), se v souvislosti s porušením povinností uložených v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 při zpracování osobních údajů prostřednictvím dynamického biometrického podpisu v souvislosti s uzavíráním smluv se svými klienty, ukládá povinnost:

1. Neshromažďovat a neuchovávat dynamické biometrické podpisy svých klientů,

   a to ve lhůtě do 60 dnů od právní moci tohoto příkazu.

2. Podat Úřadu pro ochranu osobních údajů zprávu o splnění uloženého opatření uvedeným ve výroku č. 1.,

   a to ve lhůtě 15 dnů od jeho splnění.

Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál shromážděný v rámci kontroly č.j. UOOU-09654/18, provedené Úřadem pro ochranu osobních údajů (dále jen „Úřad") u účastníka řízení ve dnech 24. října 2018 do 31. srpna 2020, včetně vyřízení námitek předsedkyní Úřadu čj. UOOU-09654/18-13, ze dne 31. srpna 2020.

Kontrolou bylo zjištěno, že hlavní aktivitou účastníka řízení je poskytování finančního poradenství a zprostředkování uzavírání životního pojištění, investic a hypoték, přičemž za účelem vedení smluvní dokumentace využívá dynamický biometrický podpis (dále také „DBP“). DBP je datová struktura, která vzniká v okamžiku, kdy se klient účastníka řízení podepisuje na podepisovacím zařízení (tzv. signature pad), které kromě výsledné grafické podoby samotného podpisu sleduje a zaznamenává i rychlost, sklon, křivky, posloupnost a přítlak tahů apod., které jsou pro každého člověka charakteristické a jedinečné. DPB obsahuje nejen samotné vyobrazení podpisu, ale současně i jeho skryté, jedinečné dynamické vlastnosti a individuální charakteristiky vlastnoručního podpisu, který v sobě obsahuje biometrické informace ve smyslu čl. 4 bodu 14 nařízení (EU) 2016/679.
Kontrolou bylo zjištěno, že účastník řízení využívá DBP jako správce osobních údajů ve vztahu k dokumentům účastníka řízení, a dále jako zpracovatel ve vztahu k některým dokumentům svých obchodních partnerů, pro které provádí zprostředkování služeb. Dle účastníka řízení je účelem zpracování DBP jako biometrického údaje stvrzení platnosti právního jednání učiněného v písemné formě, a to způsobem, který zejména zjednodušuje proces poskytování finančně-poradenských služeb a zároveň ho zatraktivňuje pro zákazníky. Účelem zpracování je potvrzení a uchovávání smluvní dokumentace, a to včetně jejího nepochybného ověření/verifikace klienta.

V rámci kontroly bylo zjištěno, že účastník řízení zpracovává DBP, tedy biometrické údaje za účelem jedinečné identifikace fyzické osoby. Jedná se o zpracování zvláštní kategorie osobních údajů dle čl. 9 odst. 1 nařízení (EU) 2016/679, při kterém s ohledem na jejich zvláštní charakter a zásah do soukromí a osobního života subjektu údajů je obecně zakázáno. 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) nařízení (EU) 2016/679. Zároveň je vždy nezbytné mít pro zpracování osobních údajů také obecný právní titul pro zpracování dle čl. 6 odst. 1 nařízení (EU) 2016/679. Právním titulem pro zpracování osobních údajů klientů při poskytování finančních služeb je primárně plnění smlouvy, jejíž smluvní stranou je subjekt údajů dle čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679. Ve vztahu k DBP, 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) nařízení (EU) 2016/679. neboť klienti dali výslovný souhlas se zpracováním této zvláštní kategorie osobních údajů pro účely uzavření a uchování smluvní dokumentace, včetně biometrického podpisu. Souhlas se zpracováním konkrétních osobních údajů, resp. v daném případě DBP 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).
Kontrolou bylo zjištěno, že účastník řízení může využívat podpis získaný prostřednictvím elektronického zařízení, převedený do grafické podoby, nikoliv však z tohoto podpisu získávat a v uložištích uchovávat a zpracovávat z něj získané biometrické údaje, a to ani v zašifrované podobě.

K rozsahu osobních údajů nezbytných pro identifikovatelnost subjektu údajů pro účely smluvního vztahu, jakož i pro plnění dalších povinností vyplývajících z něj pro účastníka řízení, a to bez ohledu na to, zda osobní údaje shromažďuje a zpracovává jako správce, resp. zpracovatel osobních údajů, je zcela dostačující rozsah osobních údajů, které musí shromažďovat v souvislosti s plněním zákonných požadavků dle zvláštní právní úpravy.

Kontrolou bylo konstatováno, že biometrický podpis klientů, není pro účely uzavření a uchování smluvní dokumentace, či zjednodušení tohoto procesu nezbytný, neboť v případě uzavírání smluv v listinné podobě není také vyžadován. Jako dostatečný pro výše uvedené účely je prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné formě, čímž účastník řízení nedodržel základní zásadu minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 když shromažďoval a následně uchovával biometrické podpisy svých klientů.

Účastník řízení podal proti protokolu o kontrole dne 18. března 2019 námitky, evidované pod č.j. UOOU-09654/18-11. Účastník řízení podal námitku proti kontrolnímu zjištění č. 2, dle kterého nedodržel základní zásadu minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, když shromažďoval a následně uchovával biometrické podpisy svých klientů.
Účastník řízení v námitkách uvedl, že byl rozhodnutím Úřadu odkázán na zastaralé a ekologicky zatěžující metody písemného podpisu. Dále připomenul, že i vlastnoruční podpis v sobě nese biometrické prvky a tento podpis je dle jeho názoru daleko méně chráněn, než jak je tomu v případě biometrického dynamického podpisu. Ke konstatování kontrolujících v Protokolu o kontrole, že *„odvolání souhlasu se týká pouze odvolání zpracování biometrických údajů, a ne obsahu smluvního ujednání“* kontrolovaný namítl, že lze předpokládat, že Úřad tímto vyjádřením mínil, že případné odvolání souhlasu subjektem údajů se nedotkne funkce autentizační, ale toliko funkce identifikace subjektu údajů. V této souvislosti upozornil, že tato myšlenka je v zásadě revoluční a v žádném případě nelze očekávat, že by byla takto chápána samotnými subjekty údajů, a pravděpodobně ani soudy České republiky. Kontrolovaný dále uvedl, že tvrzení Úřadu o dostatečnosti „prostého obrazu podpisu“ není slučitelné s rozhodovací praxí soudů a dalších příslušných veřejných orgánů České republiky, a tudíž je zjevně neopodstatněné, pročež mu v závěrech učiněných kontrolním zjištěním nelze přiznat žádnou relevanci. Také konstatoval, že sám standardně neprovádí dešifrování uložených dynamických biometrických podpisů a nemá k nim de facto sám přístup, čímž není ochrana soukromí subjektu údajů nijak dotčena a uvedl účely, pro které zpracování dynamických biometrických podpisů využívá. Kontrolovaný se odvolal i na jím doložený znalecký posudek [redacted], jehož byl zadavatelem, podle kterého jsou biometrické údaje řádně zabezpečeny a jsou tak chráněna práva a oprávněné zájmy subjektů údajů. Biometrické podpisy pak mají být zabezpečeny maximálním stupněm ochrany (nesrovnatelně více než vlastnoruční podpisy) a přístup kontrolovaného k nim je omezen na minimum, které je nutné pro možnost bránit se stížnosti či jinému sporu s klientem v budoucnu.

V závěru podané námitky účastník řízení uvedl, že aplikace kontrolního zjištění č. 2 by mu de facto odepřela možnost používat elektronické prostředky při jednání s klienty, protože při absenci dynamického biometrického podpisu jsou tyto nepoužitelné, a potřeba obstarat písemný podpis by negovala všechny výhody užití elektronických prostředků.

Předsedkyně Úřadu v rámci vyřízení námitek ze dne 31. srpna 2020, č.j. UOOU-0965/19-13, proti kontrolním zjištěním uvedeným v protokolu o kontrole čj. UOOU-09645/18-10, ze dne 5. března 2019 uvedla, že podle definice čl. 4 odst. 14 nařízení Evropského parlamentu a Rady (EU) 2016/679 se *„biometrickými osobními 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 stopy". Z výše uvedeného je tedy patrné, že pokud účastník řízení, jako poskytovatel a zprostředkovatel finančních služeb, v pozici správce a zpracovatele osobních údajů zachycuje a následně uchovává jednotlivé znaky podpisu (např. rychlost, tlak, dynamiku pohybu pera, resp. pohybu ruky), jedná se o zpracovávání biometrického osobního údaje ve smyslu výše uvedeného ustanovení, neboť je prostřednictvím uchovávaných znaků možná jedinečná identifikace fyzické osoby.

Zpracování biometrických osobních údajů je pak považováno za zpracování zvláštní kategorie osobních údajů dle čl. 9 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679, které je až na výjimky stanovené v čl. 9 odst. 2 písm. a) až j) výše uvedeného nařízení, zakázáno. Tento výčet výjimek, představující prolomení obecného zákazu zpracování zvláštní kategorie osobních údajů, je taxativní. V daném případě, jak je uvedeno v rámci kontrolního zjištění č. 2 v protokolu o kontrole, klienti kontrolovaného dali výslovný souhlas se zpracováním této zvláštní kategorie osobních údajů pro účely uzavření a uchování smluvní dokumentace dle čl. 6 odst. 1 písm. b) nařízení Evropského parlamentu a Rady (EU) 2016/679, (viz str. 13 protokolu o kontrole), jedná se o právní titul (podmínku) zpracování osobních údajů ve smyslu recitálu 51 nařízení Evropského parlamentu a Rady (EU) 2016/679. Pro účely uzavírání smluv dle čl. 6 odst. 1 písm. c) nařízení není nutný souhlas, ovšem pro zpracování biometrických osobních údajů musí být splněna některá z výjimek stanovených v čl. 9 odst. 2 písm. a) až j) nařízení Evropského parlamentu a Rady (EU) 2016/679, mezi kterou patří i výslovný souhlas subjektu údajů. Takový souhlas se zpracováním biometrických údajů udělený subjektem těchto údajů však nezbavuje kontrolovaného, ať již v pozici správce či zpracovatele osobních údajů, povinnosti dodržet všechny základní zásady zpracování osobních údajů, tedy i zásadu minimalizace osobních údajů obsaženou v čl. 5 odst. 1 písm. c) nařízení Evropského parlamentu a Rady (EU) 2016/679. Tato zásada ukládá kontrolovanému jako správci a zpracovateli osobních údajů zpracovávat osobní údaje *„přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány"*.

Jak je zřejmé z kontrolního spisu, účelem zpracování dynamického biometrického podpisu jako zvláštní kategorie osobních údajů v daném případě je, dle vyjádření kontrolovaného, stvrzení platnosti právního jednání učiněného v elektronické formě, a to způsobem, který zejména zjednodušuje proces poskytování finančně-poradenských služeb a zároveň ho zatraktivňuje pro zákazníky (subjekty údajů) (viz str. 4 protokolu o kontrole). Účastník řízení tedy jako správce i zpracovatel zpracovává osobní údaje včetně dynamického biometrického podpisu (a to jako alternativu k listinné podobě) za účelem uzavírání smluv.

Dynamický biometrický podpis klientů není pro účely uzavření a uchování smluvní dokumentace, či zjednodušení tohoto procesu nezbytný, neboť v případě uzavírání smluv v listinné podobě není kontrolovaným vyžadován. Dle ustanovení § 561 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, … *„K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat."* Tímto zvláštním právním předpisem byl myšlen zákon č. 227/2000 Sb., o elektronickém podpisu, jež přestal platit dne 19. září 2016, který však výslovnou právní úpravu dynamického biometrického podpisu a jeho užití neobsahoval a byl nahrazen tzv. adaptačním zákonem k 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 (nařízení eIDAS), tedy zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který rovněž právní úpravu biometrického podpisu a jeho užití neobsahuje. Občanský zákoník ani zvláštní právní úprava tedy vysloveně nevyžadují pro platnost právního jednání v písemné formě dynamický biometrický podpis. Dostatečný pro výše uvedené účely je tak prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné podobě. Nadbytečnost biometrického dynamického podpisu potvrzuje i vyjádření samotného kontrolovaného ze dne 25. ledna 2019, že *„od počátku smlouvy s* [redacted] *nebyl postup dešifrování použit ve vztahu k žádnému klientovi“*. Potřebnost zpracovávání dynamického biometrického podpisu nebyla doložena ani posudkem znalce.

Dynamický biometrický podpis, který se v praxi objevuje stále častěji (zejména v bankovním sektoru, v telekomunikacích či u doručovacích společností) není v českém právním řádu definován. V oboru informačních a komunikačních technologií je definován dynamický biometrický podpis jako datová struktura, která vzniká působením podepisující osoby na podepisovací zařízení (nejčastěji na podpisovém grafickém tabletu, a to vlastní rukou, případně za pomocí dotykového pera), která kromě výsledné podoby samotného podpisu sleduje a zaznamenává biometrii podepisující se osoby (rychlost tahů, přítlak atp.), která je pro každého charakteristická (ovšem v čase proměnlivá, např. stárnutím ovlivňujícím změny biometrické techniky či aktuálním zdravotním stavem). Dynamický biometrický podpis tak zachycuje nejen samotnou podobu podpisu (statický prvek), ale také dynamický prvek (rychlost, dobu podpisu, délku trvání podpisu). Hlavním problémem zpracovávání dynamického biometrického podpisu obecně je, že podepisující se subjekt (tedy subjekt zvláštní kategorie osobních údajů) zpravidla, na rozdíl od podpisu vlastnoručního, nemůže ověřit, k jakému dokumentu je jeho podpis připojen, nemá tedy nad zpracováním svých osobních údajů kontrolu, neboť s příslušnými prostředky disponuje druhá strana, nikoliv podepisující se osoba.

Ohledně dynamického biometrického podpisu lze dále uvést, že zpravidla bývá označován za druh elektronického podpisu (a to zejména s ohledem na formu jeho pořízení a zpracování), přičemž při této interpretaci bývá odkazováno, na již výše zmíněné nařízení eIDAS. Toto nařízení v čl. 3 odst. 10, které definuje elektronický podpis jako „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“, rozeznává tři druhy těchto podpisů – prostý, zaručený (čl. 3 odst. 11 nařízení eIDAS) a kvalifikovaný (čl. 3 odst. 12 nařízení eIDAS). Právní účinek rovnocenný vlastnoručnímu podpisu přiznává nařízení eIDAS v čl. 25 odst. 2 pouze kvalifikovanému elektronickému podpisu, o jiných podpisech nic neuvádí. Dynamický biometrický podpis by mohl být z pohledu této právní úpravy označen jako podpis prostý, který ovšem nařízení definuje velmi obecně. V každém případě není dynamický biometrický podpis běžným podpisem, neboť je založen na jiných mechanismech, než je tomu u elektronických podpisů a shromažďuje zvláštní kategorii osobních údajů. Biometrická identifikace/autentizace je založena toliko na pravděpodobnosti, nikoliv na 100 % přesnosti. Například schopnost rozlišení biometrické podobnosti mezi sourozenci nebo příbuznými je pro biometrické systémy zhoršená.

Přestože se používání dynamického biometrického podpisu stalo v České republice realitou, nebyly dosud řešeny otázky ochrany osobních údajů. V případě elektronického podpisu však jak nařízení eIDAS, tak vnitrostátní zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro

elektronické transakce, vyžadují, aby ochrana osobních údajů byla zohledněna. Pokud dochází ke zpracovávání biometrických osobních údajů, je vždy potřebné, aby správce zvážil, s ohledem na rizika fyzické osoby, zda je skutečně nezbytné použití této kategorie osobních údajů při daném zpracování. Zejména je nutno brát v úvahu, že zpracování biometrických údajů je spojeno s určitými riziky, jež vyplývají ze samotné podstaty těchto údajů. Takové riziko přestavuje zejména možnost jejich dalšího použití, včetně skrytého shromažďování, a to včetně tzv. inverzních útoků.

K argumentaci účastníka řízení, že nadbytečnost zpracování tohoto osobního údaje je sporná, neboť v případě zrušení zpracování biometrických údajů nebude schopen prokázat pravost podpisů klientů na smlouvách v případě jejich zpochybnění, což může vést ve svém důsledku k neplatnosti smlouvy, námitky odkázaly na již výše uvedené ohledně rozsahu osobních údajů nezbytných pro identifikaci subjektu údajů pro účely smluvního vztahu. Vzhledem k tomu, že biometrický dynamický podpis není povinnou součástí uzavírané smlouvy, nemůže případné odvolání souhlasu založit neplatnost smlouvy. Takový výklad by popíral svobodu udělení souhlasu ve smyslu čl. 9 odst. 2 písm. a) nařízení Evropského Parlamentu a Rady (EU). Blíže viz bod 3.1 pokynů pro souhlas podle nařízení 2016/679 skupiny WP 29. K výše uvedeným účelům tak stačí, aby kontrolovaný využíval podpis získaný prostřednictvím elektronického zařízení, převedený do grafické podoby.

Na základě výše uvedeného, předsedkyně Úřadu námitku účastníka řízení zamítla s tím, že zpracování dynamického biometrického podpisu klientů u smluv uzavíraných v elektronické formě není nezbytným pro vytyčené účely, a to jak z hlediska objektivního, tak i subjektivního pohledu správce osobních údajů. Zásada minimalizace osobních údajů, obsažená v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679.
Správní orgán považuje ve smyslu § 150 správního řádu skutkové zjištění za dostatečné k tomu, aby bylo účastníku řízení uloženo opatření neshromažďovat a neuchovávat dynamické biometrické podpisy svých klientů.
Lhůta pro splnění povinností dle opatření č. 1 byla stanovena na 60 dnů, a to s ohledem na charakter předmětného zpracování, tedy že se jedná o značné množství údajů získaných od většího množství fyzických osob. Současně Úřad přihlédl k tomu, že od doby nabytí právní moci Vyřízení námitek proti kontrolním zjištěním ze dne 31. srpna 2020, č.j. UOOU-09654/20-13, uběhla dostatečná doba, ve které měl účastník řízení možnost připravit se na ukončení zpracování DBP.

S ohledem na výše uvedené, bylo rozhodnuto, jak je uvedeno ve výroku tohoto příkazu.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen dnem převzetí stejnopisu, nejpozději však desátým dnem od jeho uložení u provozovatele poštovních služeb. V případě doručování do datové schránky je příkaz doručen okamžikem přihlášení oprávněné osoby do datové schránky, nejpozději však desátý den ode dne dodání příkazu do datové schránky.

Praha 3. března 2021

otisk
úředního
razítka

MVDr. František Bartoš
inspektor Úřadu
(podepsáno elektronicky)