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-10138/18-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako věcně příslušný orgán podle § 46 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a čl. 58 odst. 2 písm. i) 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) vydává dne 28. ledna 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, tento příkaz:

I. Je prokázáno, že účastník řízení: [redacted], jako správce osobních údajů svých klientů podle čl. 4 bodu 7 nařízení (EU) 2016/679,

1. tím, že od blíže nezjištěné doby nejméně do 22. října 2018 zpracovával při uzavírání smluv s klienty týkajících se poskytování úvěru v elektronické podobě za účelem uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu též biometrický podpis klientů, který nebyl nezbytný pro uzavření příslušné smlouvy ani pro její plnění, kdy ke dni 23. července 2018 uchovával ve svém informačním systému 217 274 tímto způsobem podepsaných smluv,

   porušil zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“),

2. a dále tím, že od blíže nezjištěné doby nejméně do 22. října 2018 uchovával veškeré záznamy telefonních hovorů s klienty, kteří s ním měli uzavřenou rámcovou smlouvu o poskytování bankovních produktů a služeb nebo smlouvu o klasickém a/nebo revolvingovém úvěru, a to po celou dobu trvání smlouvy a dále po dobu dalších 10 let od splnění veškerých závazků klienta,

porušil základní zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („omezení uložení“),

II. za což se mu podle čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

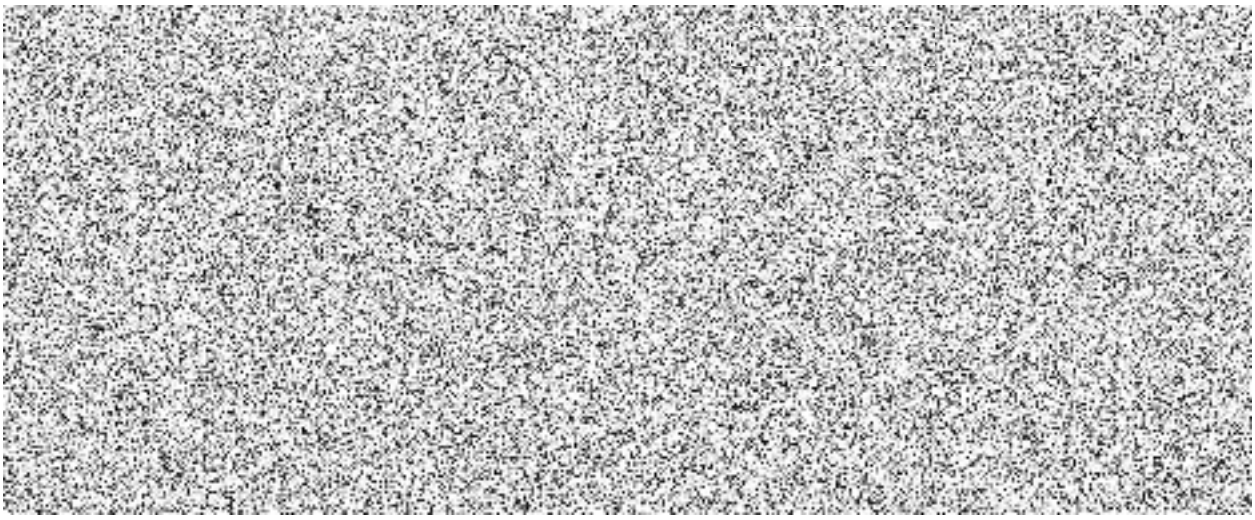
pokuta ve výši 250.000 Kč
(slovy dvě stě padesát tisíc korun českých)

splatná do 30 dnů ode dne nabytí právní moci tohoto příkazu bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání příkazu je protokol o kontrole čj. UOOU-01892/18-35 ze dne 14. září 2018 pořízený podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a zákona č. 101/2000 Sb. inspektorkou Úřadu pro ochranu osobních údajů (dále jen „Úřad“) Mgr. et Mgr. Boženou Čajkovou v rámci kontroly provedené u odštěpného závodu účastníka řízení ve dnech 22. března 2018 až 1. října 2018 a spisový materiál shromážděný v rámci této kontroly.

K aplikaci právních předpisů je nezbytné dodat, že dne 25. května 2018 nabylo účinnosti nařízení (EU) 2016/679. Vzhledem ke skutečnosti, že během páchání protiprávního jednání účastníka řízení došlo ke změně právní úpravy, správní orgán s ohledem na trvající charakter obou porušení specifikovaných ve výroku tohoto příkazu, posuzoval odpovědnost účastníka řízení za jeho protiprávní jednání dle právní úpravy účinné v době, kdy nejdříve došlo k dokončení jednání, tj. k datu uvedeném ve výroku tohoto příkazu, které vyplývá z vyjádření účastníka řízení ze dne 22. října 2018, i když kontrola byla vedena a kontrolní protokol byl vyhoven dle zákona č. 101/2000 Sb.



Ze spisového materiálu vyplývá, že kontrola byla zahájena na základě kontrolního plánu Úřadu pro rok 2018. Předmětem kontroly bylo dodržování povinností při zpracování osobních údajů

klientů v souvislosti s poskytováním úvěru [redacted]. Hlavní činností účastníka řízení je zejména přijímání vkladů, poskytování úvěrů a platebních služeb. S ohledem na skutečnost, že účastník řízení je bankou [redacted], musí při poskytování úvěrů klientům dodržovat veškeré povinnosti stanovené mu ve zvláštních právních předpisech, zejména v zákoně č. 21/1992 Sb., o bankách, v zákoně č. 257/2016 Sb., o spotřebitelském úvěru, a v zákoně č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

Ze shromážděné dokumentace vyplývá, že 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 případě sjednání úvěru online vyplňuje klient údaje samostatně do aplikace, ze které jsou přeneseny do [redacted] (systém, kde jsou osobní údaje klientů zpracovávány po celou dobu jejich uchování účastníkem řízení, přičemž jednotlivé systémy účastníka řízení čerpají přímo ze [redacted]. V případě sjednání úvěru prostřednictvím obchodního partnera jsou osobní údaje shromažďovány obchodním partnerem. Obchodní partner předává údaje buď účastníkovi řízení prostřednictvím zabezpečeného online kanálu [redacted] nebo v písemné podobě prostřednictvím pošty. V případě sjednání úvěru na pobočce účastníka řízení jsou osobní údaje klientů zadávány přímo do [redacted].

V rámci žádosti o úvěr je od klienta vyžadováno vyplnění a podpis rámcové smlouvy o poskytnutí bankovních produktů a služeb, žádosti/smlouvy o klasickém a/nebo revolvingovém úvěru včetně přihlášky k pojištění pro klasický a revolvingový úvěr, formuláře pro standardní informace o spotřebitelském úvěru, příp. dokumentu nazvaného Údaje pro posouzení žádosti o klasický a/nebo revolvingový úvěr a souhlasu se zpracováním osobních údajů. 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 domácnost). Dále jsou k danému klientovi též shromážděny informace z registru klientských informací, tj. údaje vypovídající o bonitě, důvěryhodnosti a platební morálce klienta. 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.

Ze spisové dokumentace dále vyplývá, že při podpisu smluvní dokumentace v elektronické podobě prostřednictvím zařízení Signpad od [redacted] k vytvoření elektronického podpisu zaznamenávajícího kromě grafické podoby podpisu klienta též 50 primárních a druhotných biometrických prvků, jako je např. rychlost a tlak pohybu pera. 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. Podpis je uchováván v informačním systému účastníka řízení. 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.

Dle vyjádření účastníka řízení ze dne 25. července 2018 je účelem využívání dynamického biometrického podpisu klienta při podepisování dematerializované smluvní dokumentace vytvoření věrohodné grafické podoby podpisu na smlouvách (např. zaznamenání šíře linie podpisu). Technologie Signpad je využívána z toho důvodu, že jiný typ technologie zaznamenání podpisů, např. podpis na běžném tabletu, neumožňuje zaznamenání tak vysoké důvěryhodnosti podpisu klientů. Účastník řízení též uvedl, že ke dni 23. července 2018 evidoval 217 274 tímto způsobem podepsaných smluv. Účastník řízení dále uvedl, že biometrická data jsou bezprostředně po vytvoření elektronického obrazu klientova podpisu ze Signpadu vymazána a účastník řízení ve svých systémech již tyto informace dál nezpracovává a má k dispozici pouze „obrázky" podpisů klientů. Toto své tvrzení účastník řízení ve svém dalším vyjádření ze dne 17. srpna 2018 upravil, neboť uvedl, že po detailní konzultaci s dodavatelem, který sběr biometrického podpisu implementoval, bylo zjištěno, že biometrická data jsou sbírána a stávají se součástí metadat ukládané smluvní dokumentace s klientem. Ze shromážděné dokumentace tak vyplývá, že po podpisu dochází k šifrování dat v Signpadu a k jejich následnému připojení k pdf dokumentu. Biometrické údaje, které obsahují metadata ukládané smluvní dokumentace s klientem, však mohou být vytěženy pouze technologiemi dodavatele, neboť účastník řízení nedisponuje technologií potřebnou k jejich přečtení. Účastník řízení tedy de facto využívá elektronický obraz podpisu klienta, k němuž jsou v důsledku zvolené technologie připojeny také biometrické charakteristiky. Součástí spisového materiálu je též znalecký posudek předložený účastníkem řízení, jehož závěrem je, že nedochází při zpracování biometrického podpisu k porušování právních předpisů. 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. Forma smluvní dokumentace nemá vliv na práva a povinnosti z ní vyplývající pro smluvní strany.

Ze spisové dokumentace vyplývá, že údaje o klientech jsou uchovávány v elektronické i listinné podobě. Účastník řízení má, v souladu s úpravou obsaženou ve speciálních právních předpisech, stanoveny zákonné lhůty pro uchování informací o klientech, a to zejména dle § 16 zákona č. 253/2008 Sb., podle kterého je povinen uchovat identifikační údaje klienta (včetně případných kopií dokladů předložených k identifikaci) po dobu 10 let od ukončení obchodního vztahu. Dle § 21 odst. 2 zákona č. 21/1992 Sb. je povinen uchovávat doklady o uskutečněných obchodech rovněž po dobu nejméně 10 let. Po uplynutí lhůty k uchovávání údajů dochází v případě elektronicky uchovávaných dokumentů k jejich anonymizaci bez možnosti obnovy, v případě listinných dokumentů k jejich skartaci.

Účastník řízení dále, jak též dokládá spisová dokumentace, pořizuje a uchovává zvukové záznamy telefonických hovorů s klienty. Tyto záznamy jsou uchovávány v informačním systému účastníka řízení po dobu 1 roku ode dne pořízení záznamu, avšak je-li s klientem uzavřena smlouva, uchovává účastník řízení záznamy po celou dobu trvání smluvního vztahu a dále po dobu 10 let od jeho ukončení, resp. splnění závazků klienta vůči účastníkovi řízení bez ohledu na to, o jaký typ telefonního hovoru se jedná (např. servisní poradenství, příkaz k transakci). Účastník řízení délku uchovávání zvukových záznamů odvozuje právě od § 21

odst. 2 zákona č. 21/1992 Sb., neboť předmětná komunikace dle něj může obsahovat příkazy k transakcím. Z protokolu z ústního jednání ze dne 20. června 2018 vyplývá, že účastník řízení disponuje pouze prostou nahrávkou telefonického rozhovoru bez možnosti rozboru hlasového projevu klienta.

Z vyjádření účastníka řízení doručeného Úřadu dne 22. října 2018 v návaznosti na výzvu před zahájením správního řízení o uložení opatření k nápravě vyplývá, že účastník řízení, jak ve vztahu ke zpracování biometrických dat při podpisu, tak ve vztahu k uchovávání zvukových záznamů telefonních hovorů s klienty, bude realizovat opatření k odstranění nedostatků. V případě biometrického podpisu účastník řízení uvedl, že bylo rozhodnuto o ukončení systematického shromažďování a následného ukládání biometrických dat a smluvní dokumentace bude napříště obsahovat pouze prostý otisk podpisu klienta. S ohledem na časovou, technickou a finanční náročnost bude daného řešení bude tato změna včetně její právní úpravy ve smluvní dokumentaci implementována na počátku roku 2019. K archivační 10leté lhůtě telefonních záznamů pak účastník řízení uvedl, že náprava bude spočívat v rozdělení telefonních hovorů na různé kategorie s rozdílnou archivační lhůtou. Předpokládaným termínem realizace takové úpravy je též počátek roku 2019.

K předmětu řízení lze konstatovat, že dle čl. 4 bodu 1 nařízení (EU) 2016/679 se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Informace, které zpracovává účastník řízení o svých klientech, kterým je poskytnut úvěr, včetně zvukových záznamů telefonických hovorů s klienty a biometrických podpisů, jsou osobními údajů ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

Dle čl. 4 bodu 13 nařízení (EU) 2016/679 se biometrickými údaji rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci. Podpis smlouvy, která je uzavírána v elektronické formě, kdy prostřednictvím elektronického zařízení dochází k zachycení a následnému uchovávání jednotlivých znaků podpisu, např. rychlost a tlak pohybu pera, je biometrických údajem ve smyslu čl. 4 odst. 13 nařízení (EU) 2016/679.

Podle čl. 4 bodu 2 nařízení (EU) 2016/679 se zpracováním rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. 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.

K výroku 1. tohoto příkazu správní orgán uvádí, že podle zásady zpracování osobních údajů uvedené v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 musí být osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“). Tato základní zásada upravená v nařízení (EU) 2016/679 pak zcela odpovídá povinnosti, kterou byl správce osobních údajů povinen dodržovat i dle zákona č. 101/2000 Sb., a to povinnosti správce shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu dle § 5 odst. 1 písm. d) zákona č. 101/2000 Sb.

S ohledem na výše uvedenou zásadu je nezbytné nejprve definovat účel, pro který jsou osobní údaje účastníkem řízení zpracovávány. 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.

V rámci tohoto účelu zpracování je pak určitý rozsah osobních údajů účastníkovi řízení stanoven přímo zvláštními právními předpisy (zákon č. 253/2008 Sb., zákon č. 257/2016 Sb., atd.), tj. zpracování konkrétních osobních údajů je zákonnou povinností účastníka řízení jakožto banky. 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.

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. Zpracování zvláštní kategorie osobních údajů je, s ohledem na jejich zvláštní charakter a hrubý zásah do soukromého a osobního života subjektu údajů v případě jejich zneužití, 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 úvěru je primárně plnění smlouvy, jejíž smluvní stranou je subjekt údajů dle čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679. 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) nařízení (EU) 2016/679, 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.

V této souvislosti správní orgán uvádí, 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).

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, je dle správního orgánu zcela dostačující rozsah osobních údajů, které musí účastník řízení shromažďovat v souvislosti s plněním zákonných požadavků dle zvláštní právní úpravy. 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. K předloženému znaleckému posudku správní orgán konstatuje, že samotný znalecký posudek nemůže nezávislému orgánu, jakým je Úřad, předkládat závazné právní hodnocení vztahující se k posouzení konkrétních skutkových ani právních otázek.

Z výše uvedeného je zřejmé, že 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.

K výroku 2. tohoto příkazu správní orgán konstatuje, že podle zásady zpracování osobních údajů uvedené v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 musí být osobní údaje uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po dobu delší, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického významu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických nebo organizačních opatřeních požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“). S touto základní zásadou upravenou v nařízení (EU) 2016/679 pak zcela koresponduje povinnost správce, která mu byla stanovená již v § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., a to povinnost správce uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely

vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné.

Ze shromážděné dokumentace je zřejmé, že účastník řízení uchovává ve svém informačním systému veškeré zvukové záznamy telefonních hovorů s klienty, kteří s ním uzavřeli rámcovou smlouvu o poskytování bankovních produktů a služeb nebo smlouvu o klasickém a/nebo revolvingovém úvěru, po dobu trvání smluvního vztahu a poté ještě 10 let od jeho ukončení, resp. od splnění všech závazků klienta vůči účastníkovi řízení. Takto stanovenou délku uchovávání zvukových záznamů komunikace s klienty odvozuje účastník řízení od povinnosti stanovené v § 21 odst. 2 zákona č. 21/1992 Sb., dle kterého banka a pobočka zahraniční banky je povinna evidovat v rámci účetnictví odděleně obchody na účet klienta a obchody na účet banky nebo zahraniční banky. Doklady o uskutečněných obchodech jsou banky a pobočky zahraničních bank povinny uschovávat po dobu nejméně 10 let, a to s ohledem na skutečnost, že předmětná komunikace s klienty může obsahovat příkazy k transakcím. K tomu správní orgán uvádí, že účastník řízení žádným způsobem nerozlišuje, zda během hovoru s klientem skutečně dochází k uskutečnění obchodu či nikoli (např. jedná se o hovor pouze informativního charakteru, servisní poradenství).

Správní orgán tak má za prokázané, že účastník řízení s ohledem na výše popsané svým jednáním porušil povinnost obsaženou v základní zásadě stanovené v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679, neboť řádně neodlišil jednotlivé typy telefonních hovorů a tomu odpovídající účel jejich uchovávání (např. číselným odlišením jednotlivých typů hovorů dle jejich obsahu a účelu, přičemž v průběhu hovoru by zaměstnanec zaznamenal o jaký typ hovoru se v konkrétním případě jedná, kdy pro každou skupina hovorů by pak byla nastavena odlišná doba likvidace). Uvedená doba uchovávání telefonních záznamů v délce 10 let od ukončení obchodního vztahu je relevantní pouze v případech, kdy mu je tato povinnost přímo stanovena ve zvláštních právních předpisech.

Podle čl. 83 odst. 2 nařízení (EU) 2016/679 se při rozhodování o uložení sankce a její výši přihlédne zejména k povaze, závažnosti a délce trvání porušení, k povaze, rozsahu a účelu dotčeného zpracování, k počtu dotčených subjektů údajů a míře škody, která jim byla způsobena a k dalším okolnostem porušení stanoveným v tomto článku.

Podle čl. 83 odst. 3 nařízení (EU) 2016/679 pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení. Správní orgán tak aplikuje tzv. absorpční zásadu, v jejímž rámci musel posoudit porušení kterého ustanovení je nejzávažnější. Dospěl přitom k závěru, že je jím v tomto konkrétním případě porušení čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, neboť se jedná o jednu ze základních zásad pro zpracování osobních údajů, které je nutno vnímat jako nejdůležitější principy určující, jak může správce s osobními údaji nakládat. Správní orgán přitom vzal v úvahu i skutečnost, že byla v rozporu s touto zásadou zpracovávána zvláštní kategorie osobních údajů. Za porušení této základní zásady dle čl. 83 odst. 5 nařízení (EU) 2016/679 lze uložit správní pokutu až do výše 20 000 000 EUR, jedná-li se o podnik, až do výše 4 % z celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, které hodnota je vyšší.

Při stanovení sankce tak správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, zejména k vysokému počtu dotčených subjektu údajů (ke dni 23. července 2018 se jednalo o 217 274 smluv obsahujících biometrický podpis subjektů údajů, což sice nelze směšovat s počtem dotčených subjektů údajů, neboť některé subjekty mohly uzavřít více smluv, ale je zjevné, že se jednalo o desítky tisíc dotčených osob). Jako další přitěžující okolnost pak správní orgán vyhodnotil skutečnost, že došlo protiprávně ke zpracování biometrického podpisu, jakožto zvláštní kategorie osobních údajů, jehož případné zneužití by znamenalo značný zásah do soukromého a osobního života subjektů údajů. Správní orgán též přihlédl k přitěžující okolnosti, že jednáním účastníka řízení bylo porušeno více povinností, resp. základních zásad, které představují základní principy, na jejichž řádném dodržování spočívá každé zpracování osobních údajů. Pokud se týká povahy činnosti účastníka řízení, je dle správního orgánu profesionálem v oboru, kde dochází k rozsáhlému zpracování osobních údajů, což míru škodlivosti protiprávního jednání zvyšuje. Za skutečnost snižující závažnost protiprávního jednání účastníka řízení pak správní orgán považuje skutečnost, že sice docházelo ke shromažďování a ukládání biometrických údajů klientů, avšak nikoli k dalšímu nakládání s nimi, které by zvyšovalo riziko jejich možného zneužití. Dále správní orgán přihlédl, jako k okolnosti snižující závažnost jednání, ke skutečnosti, že účastník řízení disponoval souhlasem subjektů údajů pro zpracování jejich biometrických podpisů. Za skutečnost snižující závažnost jednání považuje správní orgán též spolupráci odštěpného závodu účastníka řízení s dozorovým úřadem za účelem nápravy zjištěného porušení.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnost stanovenou v čl. 5 odst. 1 písm. c) a e) nařízení (EU) 2016/679, a proto rozhodl podle § 150 odst. 1 správního řádu ve věci příkazem.

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 ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání příkazu do datové schránky.

Praha 28. ledna 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního