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-10138/18-8

ROZHODNUTÍ

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) v řízení o porušení povinností podle nařízení (EU) 2016/679, vedeném podle zákona č. 500/2004 Sb., správní řád, rozhodl dne 21. března 2019 takto:

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)

III. a dále podle § 79 odst. 5 správního řádu povinnost nahradit **náklady řízení ve výši 1.000 Kč**,

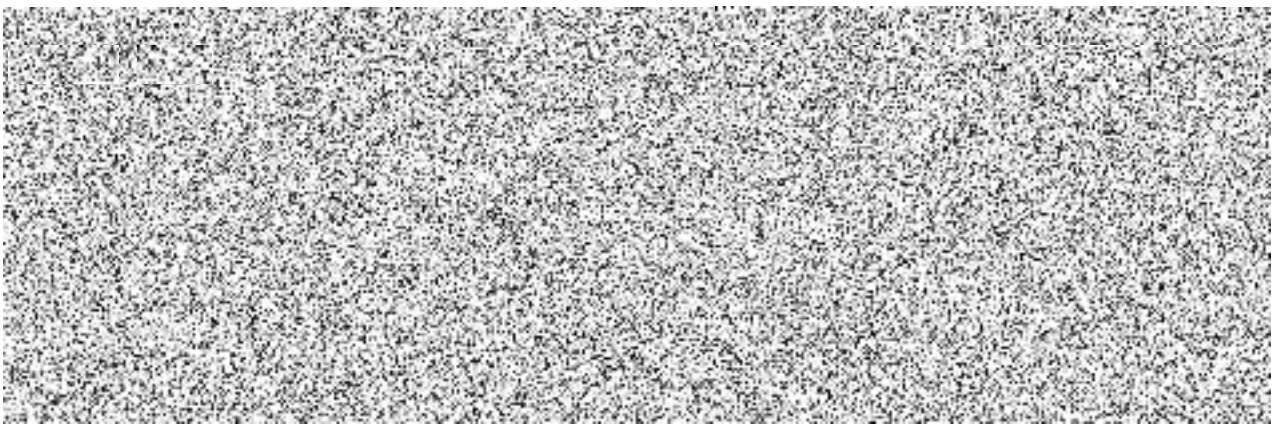
obojí splatné do 30 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Řízení ve věci porušení povinností stanovených v čl. 5 odst. 1 písm. c) a e) nařízením (EU) 2016/679 bylo zahájeno příkazem Úřadu pro ochranu osobních údajů (dále jen „Úřad“), který byl účastníkovi řízení, [redacted] doručen dne 28. ledna 2019. Podkladem pro zahájení řízení 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 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. Dne 31. ledna 2019 byl Úřadu doručen odpor účastníka řízení proti výše uvedenému příkazu. V souladu s § 150 odst. 3 zákona č. 500/2004 Sb. byl podaným odporem příkaz zrušen a správní orgán pokračoval ve správním řízení.

K aplikaci právních předpisů je nezbytné dodat, že ode dne 25. května 2018 je účinné nařízení (EU) 2016/679. Vycházeje z principů evropského práva, tj. přímé aplikovatelnosti nařízení dle čl. 288 Smlouvy o fungování Evropské unie a aplikační přednosti evropského práva před právem vnitrostátním (viz rozsudek Soudního dvora Evropské unie ze dne 15. července 1964, *Costa v ENEL*, 6/64), se úprava obsažená v tomto nařízení použije přednostně před úpravou zakotvenou v zákoně č. 101/2000 Sb. Podle čl. 40 odst. 6 Listiny základních práv a svobod se trestnost činu posuzuje a trest se ukládá podle zákona účinného v době, kdy byl čin spáchán. Pozdějšího zákona se použije, jestliže je to pro pachatele příznivější. Tato ústavněprávní zásada je promítnuta i do § 2 odst. 2 zákona č. 40/2009 Sb., trestní zákoník, podle kterého, jestliže se zákon změní během páchání činu, užije se zákona, který je účinný při dokončení jednání, kterým je čin spáchán. Dle rozsudku Nejvyššího správního soudu ze dne 31. května 2007, čj. 8 As 17/2007 – 135, se trestnost správních deliktů řídí obdobnými principy jako trestnost trestných činů. Jednání účastníka řízení specifikovaná ve výroku I bod 1. a bod 2. tohoto rozhodnutí jsou svým charakterem trvajícím správním deliktem. Ohledně problematiky

tzv. trvajícího deliktu správní orgán odkazuje na judikaturu Nejvyššího správního soudu, konkrétně na rozsudek čj. 5 A 164/2002-44 ze dne 22. února 2005, podle kterého je trvajícím správním deliktem: *„takový správní delikt, jímž pachatel vyvolá protiprávní stav, který posléze udržuje, popřípadě jímž udržuje protiprávní stav, aniž jej vyvolal. Jednání, jímž pachatel udržuje protiprávní stav, závadný z hlediska správního práva, tvoří jeden skutek a jeden správní delikt až do okamžiku ukončení deliktního jednání, tj. až do okamžiku odstranění protiprávního stavu. Lhůta pro uložení pokuty, případně pro zahájení řízení o uložení pokuty, začne běžet teprve od okamžiku ukončení trvajícího správního deliktu. Pokaždé, když se správní orgán dozví, že delikvent i nadále udržuje protiprávní stav, tj. že stále nedošlo k ukončení trvajícího jiného správního deliktu, počne vždy běžet nová subjektivní lhůta k uložení pokuty, resp. k zahájení řízení o uložení pokuty.“* Per analogiam lze též odkázat na definici trvajícího přestupku dle § 8 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, tedy trvající přestupek je takový přestupek, jehož znakem je jednání pachatele spočívající ve vyvolání a následném udržování protiprávního stavu nebo jednání pachatele spočívající v udržování protiprávního stavu, který nebyl pachatelem vyvolán. K době spáchání u trvajícího deliktu, resp. u trvajícího trestného činu Komentář k trestnímu zákoníku uvádí, že: *„je dobou spáchání též doba ukončení trestného činu, kterým se rozumí okamžik ukončení protiprávního stavu, jehož udržování je zákonným znakem trvajícího trestného činu. Jestliže protiprávní stav byl odstraněn až za účinnosti nového zákona, kvalifikuje se čin podle tohoto zákona, i když udržování protiprávního stavu započalo a část doby pokračovalo za účinnosti předchozího trestního zákona či zákonů“*.[1] Analogicky lze odkázat na § 2 odst. 4 zákona č. 250/2016 Sb. upravující časovou působnost právních norem správního trestání tak, že jestliže se zákon změní během páchání trvajícího přestupku, použije se zákon účinný v době, kdy došlo k odstranění protiprávního stavu. Vzhledem ke všemu výše uvedenému a k časovému vymezení skutku obsaženém ve výroku tohoto rozhodnutí posuzoval správní orgán odpovědnost účastníka řízení za jeho protiprávní jednání dle právní úpravy účinné od 25. května 2018, tedy dle úpravy účinné v době, kdy nejdříve došlo k dokončení jednání, tj. ke dni 22. října 2018. Vedení kontroly ani vyhotovení protokolu o kontrole dle zákona č. 101/2000 Sb. nemá vliv na aplikaci právních předpisů pro toto správní řízení, neboť, jak bylo výše uvedeno, odpovědnost účastníka řízení za jeho protiprávní jednání se posuzuje podle zákona účinného v době spáchání správního deliktu, resp. k okamžiku ukončení protiprávního stavu. Pro úplnost pak správní orgán dodává, že jednání účastníka řízení popsané ve výroku tohoto rozhodnutí bylo jak v rozporu se zákonem č. 101/2000 Sb., tak je v rozporu i s nařízením (EU) 2016/679 (podrobněji dále v odůvodnění tohoto rozhodnutí).



[1] viz ŠÁMAL, P. a kol. *Trestní zákoník: komentář*. 2.vyd., Praha: Nakladatelství C. H. Beck, 2012, s. 52

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 u odštěpného závodu účastníka řízení, společnosti [redacted]. Hlavní činností účastníka řízení je zejména přijímání vkladů, poskytování úvěrů a platebních služeb. S ohledem na skutečnost, že účastník řízení je bankou (resp. odštěpný závod účastníka řízení je pobočkou zahraniční banky), 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 aplikace [redacted] (systém, kde jsou osobní údaje klientů zpracovávány po celou dobu jejich uchování účastníkem řízení, přičemž jednotlivé systémy účastníka řízení čerpají přímo ze systému [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 (tzv. Telematika) nebo v písemné podobě prostřednictvím pošty. V případě sjednání úvěru na pobočce účastníka řízení jsou osobní údaje klientů zadávány přímo do aplikace [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 domácnosti). 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 společnosti [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 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.

Dne 14. listopadu 2018 vydal Úřad úřední záznam o neuložení opatření k odstranění zjištěných nedostatků, čj. UOOU-01892/18-40, neboť již v průběhu kontroly a následně po předání protokolu o kontrole ze dne 14. září 2018 byl Úřad informován o přípravě opatření, která účastník řízení v souvislosti s konstatovaným porušením připravuje. Změny se měly týkat opatření v souvislosti s délkou uchování zvukových záznamů a opatření týkajících se kontrolou namítaného zpracování biometrického podpisu klienta vyplývající z vyjádření účastníka řízení k protokolu o kontrole ze dne 1. října 2018 a z reakce na výzvu Úřadu před zahájením správního řízení ze dne 22. října 2018. S ohledem na výše uvedené proto nebylo důvodné ukládat účastníkovi řízení opatření k odstranění zjištěných nedostatků.

Dne 28. ledna 2019 byl vydán a téhož dne doručen příkaz (čj. UOOU-1038/18-3) účastníkovi řízení, který proti tomuto příkazu podal dne 31. ledna 2019 odpor. V uvedeném odporu účastník řízení nejprve namítal, že jednání specifikované ve výroku tohoto rozhodnutí se nemělo posuzovalo dle nařízení (EU) 2016/679, ale dle úpravy zakotvené v zákoně č. 101/2000 Sb., neboť účastník řízení byl poučen na počátku kontroly i v jejím průběhu, zejména během ústního jednání konaného dne 4. dubna 2018, že předmětná kontrola byla zahájena a prováděna dle zákona č. 101/2000 Sb., a tedy i veškerá dokumentace předkládaná účastníkem řízení odpovídala právní regulaci podle tohoto zákona. K tomu účastník řízení dále uvedl, že ačkoliv měnil své interní postupy, procesy a dokumentaci ke dni 25. května 2018 tak, aby odpovídala nařízení (EU) 2016/679, nebyla tato dokumentace a postupy v rámci kontroly požadovány, předkládány a kontrolovány. Dle tvrzení účastníka řízení mu v rámci řízení nebyl nesoulad s nařízením (EU) 2016/679 jakkoliv vytýkán, a účastník řízení tedy ani nemohl využít argumentaci dle tohoto nařízení. S ohledem na výše uvedené je účastník řízení přesvědčen, že aplikace nařízení (EU) 2016/679 v rámci této kontroly je nepovolenou retroaktivitou.

Druhým bodem odporu proti příkazu pak byl nesouhlas účastníka řízení s výší uložené sankce, neboť je přesvědčen, že sankce by v tomto řízení neměla být vyměřena ve výši a dle pravidel nařízení (EU) 2016/679, ale dle zákona č. 101/2000 Sb. S ohledem na způsob a rozsah porušení zákona č. 101/2000 Sb. se účastník řízení domnívá, že sankce by měla být uložena v nižší částce, protože vyměřená pokuta je v nepoměru se sankcemi, které byly správním orgánem ukládány v závažnějších případech. Na podporu svých tvrzení pak účastník řízení uvedl jako příklad [redacted], které byla za odcizení databáze zákazníků uložena pokuta ve výši 1 500 000 Kč, a [redacted], které byla za přeprodávání rozsáhlé zákaznické databáze uložena pokuta ve výši 800 000 Kč. Účastník řízení tak má za to, že uložením sankce ve výši 250 000 Kč byla porušena zásada předvídatelnosti správních rozhodnutí. Dle názoru účastníka řízení by pokuta za porušení zákona č. 101/2000 Sb. měla být nižší zejména z důvodu, že uvedené porušení nemělo žádný přímý vliv na práva či bezpečnost subjektů údajů, neboť tyto údaje nebyly narušeny, zveřejněny ani předány třetí osobě.

Dne 12. února 2019 byl účastník řízení seznámen se skutečností, že byly shromážděny všechny potřebné podklady k vydání rozhodnutí a též byl náležitě poučen o svých právech účastníka správního řízení plynoucích mu ze zákona č. 500/2004 Sb. Účastník řízení využil svého práva nahlédnout do spisu dne 19. února 2019 (viz úřední záznam čj. UOOU-10138/18-6).

Dne 20. února 2019 bylo správnímu orgánu doručeno vyjádření účastníka řízení, kterým doplnil podaný odpor. Součástí vyjádření byl též dopis účastníka řízení ze dne 19. února 2019 adresovaný Úřadu ve věci stavu splnění opatření k nálezům v rámci kontroly prováděné Úřadem. Účastník řízení nejprve ve svém vyjádření zopakoval, že nesouhlasí s aplikací nařízení (EU) 2016/679 na posuzované jednání a na určení výše sankce, a to včetně zcela shodné argumentace uvedené v odporu.

Dále v rámci svého vyjádření účastník řízení vyslovil názor, že správní orgán není z právního hlediska k aplikaci nařízení (EU) 2016/679 na daný případ v okamžiku správního řízení oprávněn, a to z toho důvodu, že dle čl. 51 a násl. tohoto nařízení je monitorováním plnění povinností dle nařízení a ukládáním sankcí pověřen dozorový orgán stanovený příslušným členským státem. Vzhledem k tomu, že nebyl v České republice přijat prováděcí zákon, a tím pádem nebyl dosud ani takový dozorový orgán zákonem určen, není dle účastníka řízení Úřad k aplikaci sankce dle nařízení (EU) 2016/679 oprávněn.

K otázce výše pokuty účastník řízení uvedl, že s přihlédnutím k okolnostem a rozsahu porušení zákona č. 101/2000 Sb., provedeným nápravným opatřením ze strany účastníka řízení a dosavadní rozhodovací praxi by měla být tato sankce nižší.

K problematice biometrických podpisů se účastník řízení vyjádřil tak, že zpracování této kategorie osobních údajů nemělo dopad na práva subjektů údajů, neboť bylo prováděno s jejich předchozím souhlasem. Dle účastníka řízení je otázka nutnosti či nadbytečnosti daného zpracování též sporná, neboť v případě zrušení zpracování biometrických údajů účastník řízení nebude schopen prokázat pravost podpisu klientů na smlouvách, nicméně i přes to (s vědomím případných právních rizik neplatnosti smluv) účastník řízení názor Úřadu přijal a ukončení tohoto zpracování implementoval a do budoucna ponese obchodní riziko toho, že pokud někdo zpochybní svůj podpis na smlouvě uzavřené prostřednictvím tzv. Signpadu, nebude účastník řízení schopen prokázat pravost podpisu a smlouva bude neplatná. Účastník

je proto toho názoru, že při rozhodování o udělení finanční sankce a případně její výši by správní orgán měl vzít uvedené okolnosti v potaz.

Co se týká porušení povinnosti spočívající v archivaci telefonních hovorů po dobu deseti let, účastník řízení konstatoval, že přijal názor správního orgánu, že původně nastavená 10letá archivační lhůta na všechny typy hovorů není nutná a nastavil nový systém pro archivaci hovorů. Účastník řízení dále uvedl, že se domnívá, že původně nastavená archivační lhůta, která byla dle názoru Úřadu příliš dlouhá, neměla významný dopad na práva subjektů údajů, a tato skutečnost, by měla být vzata v potaz při určení výše případné sankce.

Dále účastník řízení sdělil, že neprodleně po obdržení protokolu o kontrole ze dne 14. září 2018 zahájil veškeré kroky, aby všechna shledaná porušení byla odstraněna v nejbližším možném termínu. O aplikaci příslušných opatření byl Úřad informován vyjádřením ze dne 22. října 2018 a dále dopisem ze dne 19. února 2019.

Účastník řízení dále navrhl, aby při rozhodování o uložení sankce a její případné výši byla vzata v úvahu i skutečnost, že Úřad vydal na základě postupu provádění nápravných opatření dne 14. listopadu 2018 rozhodnutí o nezahájení uložení opatření k odstranění zjištěných nedostatků. Dle účastníka řízení svědčí vydání tohoto rozhodnutí mimo jiné o nízké závažnosti shledaných porušení a o tom, že nápravná opatření neprodleně přijatá ze strany účastníka řízení byla dostatečná a pro Úřad uspokojivá.

Na závěr účastník řízení sdělil, že pokud správní orgán rozhodne o uložení finanční sankce, pak by její výše měla odpovídat dosavadní rozhodovací praxi správního orgánu. Následně účastník řízení uvedl shodnou argumentaci ohledně výše pokuty jako v podaném odporu ze dne 31. ledna 2019, a to včetně příkladů ukládání správních pokut jiným společnostem.

Z přiloženého dopisu ze dne 19. února 2019 týkající se stavu plnění opatření vztahujících se ke kontrolním zjištěním uvedeným v protokolu o kontrole, čj. UOOU-01892/18-35, vyplývá následující. Opatření k ukončení systematického shromažďování a následného ukládání biometrických dat, která jsou součástí dynamického biometrického podpisu klienta, bylo implementováno dne 1. února 2019. Od uvedeného data smluvní dokumentace uzavíraná v elektronické podobě obsahuje již pouze prostý otisk podpisu klienta a časové razítko. Dále byl upraven dokument „Informace o zpracování osobních údajů a o ochraně bankovního tajemství“, prostřednictvím kterého dochází k informování klientů o způsobu zpracování osobních údajů účastníkem řízení. V rámci smluvní dokumentace uzavírané s novými klienty, jsou změny tohoto dokumentu z technických důvodů postupně implementovány až do 13. března 2019. Vzhledem k úpravě výhradně technického charakteru nebylo nutné měnit interní předpisy účastníka řízení.

K opatření týkající se úpravy délky doby uchovávání telefonních hovorů s klienty bylo sděleno, že je účastníkem řízení připraven návrh klasifikace hovorů přes všechny provozní oddělení, kde zaměstnanci komunikují s klienty. Archivační lhůty telefonních hovorů mají být od 1 roku až po dobu 10 let od ukončení trvání smlouvy uzavřené při daném telefonním hovoru. Součástí úprav je i pořízení nové verze softwaru, ve kterém se hovory nahrávají a archivují, protože stávající software neumožňoval aplikovat různou délku archivace hovorů. Implementace opatření je dle účastníka řízení naplánována na 1. březen 2019. Dále byla též upravena

odpovídající část dokumentu „Informace o zpracování osobních údajů a o ochraně bankovního tajemství“ a došlo též k aktualizaci interních předpisů a pokynů pro zaměstnance.

Správní orgán k tomuto řízení a jeho předmětu uvádí následující. K argumentaci účastníka řízení ohledně toho, že Úřad není oprávněn k ukládání sankce dle nařízení (EU) 2016/679, neboť dosud nebyl přijat prováděcí zákon, který by určil dozorový orgán, lze uvést následující. V souladu s čl. 51 odst. 1 nařízení (EU) 2016/679 ve spojení s § 2 odst. 2 a 3 zákona č. 101/2000 Sb. je Úřad kontinuálně ústředním správním úřadem pro oblast ochrany osobních údajů i po nabytí účinnosti nařízení (EU) 2016/679. Jeho postavení jako dozorového orgánu pro oblast ochrany osobních údajů bylo potvrzeno i rozsudkem Nejvyššího správního soudu ze dne 9. srpna 2018, čj. 9 Azs 49/2018-50: *„Na relevanci výše uvedeného podle přesvědčení soudu nic nemění ani nová úprava nařízení GDPR. Úřad pro ochranu osobních údajů nadále zůstává dozorovým a kontrolním orgánem na úseku ochrany osobních údajů (k tomu viz zejména čl. 51, čl. 57 odst. 1, čl. 58 a čl. 77 nařízení GDPR).“*

K nesouhlasu účastníka řízení s aplikací nařízení (EU) 2016/679 na jednání specifikovaná ve výroku I bod 1. a bod 2. tohoto rozhodnutí, která se dle názoru účastníka řízení měla posuzovat podle zákona č. 101/2000 Sb., správní orgán odkazuje na výše uvedené odůvodnění vztahující se k aplikaci právních předpisů obsažené v druhém odstavci odůvodnění tohoto rozhodnutí, ze kterého vyplývá, že správní orgán posuzoval odpovědnost účastníka řízení za jeho protiprávní jednání dle úpravy účinné v době spáchání deliktu, tj. v případě trvajícího správního deliktu, jakým jsou obě jednání specifikovaná ve výroku tohoto rozhodnutí, k okamžiku ukončení protiprávního stavu, tedy dle právní úpravy účinné ke dni 22. října 2018. Správní orgán k této otázce uzavírá, že jiný způsob posouzení mu právní předpisy ani neumožňují.

K námitkám účastníka řízení, že v rámci kontroly mu nebyl nesoulad s nařízením (EU) 2016/679 jakkoliv vytýkán a účastník řízení tak nemohl využít argumentaci dle tohoto nařízení, a dále, že aplikace nařízení (EU) 2016/679 „v rámci této kontroly“ je nepovolenou retroaktivitou, správní orgán konstatuje následující. Kontrola a správní řízení jsou dva zcela samostatné procesní instituty, které slouží každý jinému cíli (viz rozsudek Vrchního soudu v Praze ze dne 27. prosince 2001, čj. 7 A 98/99-37). Cílem kontroly je ve smyslu § 2 zákona č. 255/2012 Sb. „pouze“ zjistit skutečný stav věci a porovnat ho se stavem žádoucím, tedy zjistit, jak kontrolovaný dodržuje právní povinnosti, nikoliv však ukládat kontrolovanému, aby stav napravil nebo odstranil protiprávní stav či ho trestat za zjištěné nedostatky. Ukládání opatření k nápravě nedostatků nebo ukládání správních trestů za zjištěná porušení právních předpisů, nejsou součástí kontroly, ale představují samostatný proces navazující na kontrolní zjištění. I když mezi kontrolou a správním řízením (o uložení správního trestu nebo opatřením k nápravě) navazujícím na výsledky kontroly jsou určité vazby, není účelem kontroly opatřovat podklady pro správní řízení, resp. pro vydání rozhodnutí ve správním řízení (viz též Stanovisko odboru veřejné správy, dozoru a kontroly Ministerstva vnitra č. 3/2018). Současně ale platí, že skutečnosti zjištěné při kontrole mohou sloužit a být využity jako podklad pro vydání rozhodnutí v navazujícím správním řízení. Nad to je nutné uvést, že zjištění uvedená v protokolu o kontrole nejsou, na rozdíl od rozhodnutí ve správním řízení, právně závazná. S ohledem na výše uvedené správní orgán shrnuje, že tvrzení účastníka řízení, že aplikace nařízení (EU) 2016/679 „v rámci této kontroly“ je nepovolenou retroaktivitou, je chybné, neboť se již nejedná o kontrolu, ale o správní řízení. K samotné aplikaci právních předpisů v rámci tohoto správní řízení pak správní orgán odkazuje opětovně na druhý odstavec

odůvodnění tohoto rozhodnutí. K námitce účastníka řízení, že mu nebyl během kontroly nesoulad s nařízením (EU) 2016/679 jakkoliv vytýkán, správní orgán uvádí, že i toto tvrzení účastníka řízení je chybné, neboť přímo v protokolu o kontrole, čj. UOOU-01892/18-35, ze dne 14. září 2018 je konstatováno porušení povinností stanovených v § 5 odst. 1 písm. d) a e) zákona č. 101/2000 Sb. U obou těchto kontrolních zjištění bylo dále konstatováno, že uvedené závěry by pak dle kontrolujících byly beze změny i v případě, kdy by se na daný případ aplikovalo nařízení (EU) 2016/679. Nicméně dle správního orgánu a v souladu s výše uvedeným je nezbytné poukázat na samotný účel kontroly, kterým je zjistit skutečný stav věci, nikoli napravit či trestat zjištěné nedostatky. K další námitce účastníka řízení ohledně nemožnosti využít argumentaci dle nařízení (EU) 2016/679 správní orgán sděluje, že účastník řízení byl v rámci tohoto řízení o skutečnosti, že je vedeno pro podezření z porušení nařízení (EU) 2016/679, informován prostřednictvím vydaného příkazu a následně byl dne 12. února 2019 prostřednictvím seznámení s poklady rozhodnutí, čj. UOOU-10138/18-5, řádně poučen o svých právech, a to včetně práva dle § 36 zákona č. 500/2004 Sb., tedy práva navrhovat důkazy, činit jiné návrhy, vyjádřit své stanovisko a vyjádřit se k podkladům rozhodnutí.

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 14 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. 14 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 rozhodnutí 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.

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.

K argumentaci účastníka řízení ohledně zpracování biometrického podpisu klienta uvedené v doplnění odporu doručeného správnímu orgánu dne 20. února 2019, tedy že toto zpracování nemělo dopad na práva subjektů údajů, neboť bylo prováděno s jejich souhlasem, 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). Dále je též nezbytné poukázat na skutečnost, že byla tímto zpracováním dotčena zvláštní kategorie osobních údajů. Zpracování těchto osobních údajů může již z jejich samotné povahy vážně ohrozit základní právo subjektu údajů na soukromí. Nicméně správní orgán již při rozhodování o uložení sankce a její výši v příkazu ze dne 28. ledna 2019, čj. UOOU-10138/18-3, přihlédl jako k okolnosti snižující závažnost jednání, ke skutečnosti, že účastník řízení disponoval souhlasem subjektů údajů pro zpracování jejich biometrických podpisů.

Účastník řízení ve svém doplnění odporu ze dne 20. února 2019 dále namítal ohledně zpracování biometrického podpisu klienta, že nadbytečnost zpracování tohoto osobního údaje je též sporná, neboť v případě zrušení zpracování biometrických údajů nebude účastník řízení schopen prokázat pravost podpisů klientů na smlouvách v případě jeho zpochybnění, což může vést ve svém důsledku k neplatnosti smlouvy. Správní orgán odkazuje na již výše uvedené ohledně rozsahu osobních údajů nezbytných pro identifikaci subjektu údajů pro účely smluvního vztahu, a to zejména na skutečnost, že sám účastník řízení ve svém vyjádření ze dne 25. července 2018 sdělil, že jediným účelem využívání dynamického biometrického podpisu klienta při podepisování dematerializované smluvní dokumentace je vytvoření

věrohodné grafické podoby podpisu klientů na smlouvách, dále ve svém vyjádření ze dne 17. srpna 2018 uvedl, že nedisponuje technologiemi, která by čtení zmíněných biometrických dat umožňovala a data mohou být tedy vytěžena pouze technologiemi dodavatele, a též na skutečnost, že sám účastník řízení neměl povědomí o tom, že dochází ke zpracování biometrického podpisu i po bezprostředním vytvoření elektronického obrazu podpisu. Správní orgán tedy shrnuje, že zpracování podpisu klientů u smluv uzavíraných v elektronické podobě v jeho biometrické podobě není nezbytným pro vytyčené účely, a to jak z hlediska objektivního, tak i subjektivního z pohledu správce, neboť takový účel nebyl nijak proklamován, ani není v technických možnostech účastníka řízení jeho naplnění, a proto se tato nová argumentace jeví správnímu orgánu jako ryze účelová.

Správní orgán pouze podotýká, že i přes časové vymezení skutku ve výroku tohoto rozhodnutí, tj. do 22. října 2018, je z vyjádření účastníka ze dne 19. února 2019 zřejmé, že i po této době docházelo ke zpracování biometrických údajů klientů, a to až do 1. února 2019.

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 rozhodnutí 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).

K argumentaci účastníka řízení uvedené v doplnění odporu, že původně nastavená 10letá archivační lhůta neměla významný dopad na práva subjektů údajů, správní orgán uvádí, že již samotné uchování telefonních hovorů po takto dlouho dobu bez jakéhokoli rozlišení jejich obsahu a charakteru představuje značný zásah do soukromí subjektů údajů.

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. Správní orgán pouze na okraj podotýká, že i když řízení bylo zahájeno pro porušení povinností s časovým vymezením skutku do 22. října 2018, je z vyjádření účastníka řízení ze dne 19. února 2019 zřejmé, že nejméně do 1. března 2019 nebylo implementováno opatření, které by rozlišovalo jednotlivé typy hovorů a délku jejich archivace.

K námitce účastníka řízení ohledně nepřiměřenosti sankce správní orgán uvádí, že v souladu s čl. 83 odst. 1 nařízení (EU) 2016/679 má být ukládání správních pokut v každém jednotlivém případě nejen účinné a přiměřené, ale též odrazující. Má-li správní trestání efektivně přispívat ke svému základnímu společenskému účelu, totiž být prostředkem prevence páchání deliktů a mít dostatečný odstrašující charakter pro společnost i delikventa, stejně jako být určitou formou represe za společensky nepřijatelné jednání, je třeba při stanovení výměry trestu ukládat sankce v takové výši, aby pro delikventa znamenala dostatečnou újmu – ať už na majetku, či na jiných hodnotách, avšak přitom nesmí mít tzv. likvidační charakter (viz Pl. ÚS 3/02 ze dne 13. srpna 2002). K samotné výši sankce za spáchaný protiprávní jednání se správní orgán vyjádří níže.

K argumentaci účastníka řízení, že uložená pokuta by měla být nižší s ohledem na skutečnost, že uvedené porušení nemělo žádný přímý vliv na práva či bezpečnost subjektů údajů, neboť tyto údaje nebyly narušeny, zveřejněny nebo předány třetí osobě, správní orgán uvádí, že povinnost stanovená správci v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 je formulována tak, že již samotným uchováním osobních údajů, které nejsou ke stanovenému účelu nezbytné, dochází k jejímu porušení, obdobně u povinnosti správce zakotvené v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 dochází k porušení již samotným uchováním osobních údajů po dobu delší než je nezbytná pro stanovené účely. Samu skutečnost, že nedošlo k některé z událostí uvedených účastníkem řízení, tj. k narušení, zveřejnění nebo předání osobních údajů třetí osobě, nelze hodnotit jako polehčující okolnost, či okolnost snižující závažnost jednání. Tyto události, v případě, že by nastaly, by bylo možno vyhodnotit spíše jako samostatné porušení dalších povinností stanovených správci nařízením (EU) 2016/679. Nicméně správní orgán při stanovení sankce a její výše přihlédl (a již v původně vydaném příkazu), jako k okolnosti snižující závažnost jednání, k tomu, že sice docházelo ke shromažďování a ukládání

biometrických údajů klientů, avšak nikoli k dalšímu nakládání s nimi, které by zvyšovalo riziko jejich možného zneužití.

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.

K hodnocení výše uložené sankce správní orgán na okraj uvádí, že skutečnost, že účastníkovi řízení nebyla v návaznosti na kontrolu provedenou podle zákona č. 255/2012 Sb. uložena žádná opatření k nápravě, nemá vliv na skutečnost, že došlo k porušení povinností účastníkem řízení, popř. tato skutečnost sama bez dalšího neznamená, že by na porušení povinností účastníkem řízení šlo pohlížet jako porušení mající nízkou společenskou závažnost

(resp. škodlivost). Na doplnění lze uvést, že z úředního záznamu o neuložení opatření k odstranění zjištěných nedostatků ze dne 14. listopadu 2018 vyplývá, že nápravná opatření nebyla uložena proto, že účastník řízení přislíbil brzkou nápravu konstatovaných porušení, nicméně reálně k nápravě těchto porušení došlo až 1. února 2019 a 1. března 2019.

K předkládaným příkladům uložení správních pokut v uváděné výši jiným společnostem, správní orgán uvádí, že jde o zcela irelevantní argumentaci účastníka řízení, neboť se jedná o odlišné případy s odlišným skutkovým stavem, které nemají jakoukoliv souvislost s tímto řízením (s výjimkou skutečnosti, že se jednalo o porušení právních předpisů při zpracování osobních údajů). Uložení správní sankce a její výše za protiprávní jednání účastníka řízení uvedená ve výroku tohoto rozhodnutí je dle správního orgánu zcela dostatečně posouzeno, zhodnoceno a odůvodněno a správní orgán neshledává žádnou okolnost, kterou by měla být jakkoliv narušena zásada předvídatelností jeho správního rozhodování.

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

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z § 79 odst. 5 správního řádu, který správnímu orgánu ukládá uložit účastníkovi řízení, který řízení vyvolal porušením své povinnosti, náklady řízení paušální částkou, a z § 6 odst. 1 vyhlášky č. 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, podle kterého paušální částka nákladů správního řízení, které účastník vyvolal porušením své právní povinnosti, činí 1.000 Kč.

Poučení: V souladu s § 152 odst. 1 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedkyni Úřadu pro ochranu osobních údajů.

Rozhodnutí je doručeno 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 rozhodnutí do datové schránky.

Praha 21. března 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního