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-02062/19-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle 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 13. května 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, tento příkaz:

I. Je prokázáno, že účastník řízení: společnost

jako správce osobních údajů svých klientů podle čl. 4 bodu 7 nařízení (EU) 2016/679,

1. tím, že dne 21. června 2017 použil osobní údaje v rozsahu jméno, příjmení, rodné číslo, datum narození, pohlaví, místo narození, občanství, adresa trvalého pobytu, číslo občanského průkazu včetně jeho platnosti a úřadu, který ho vydal, které měl k dispozici na základě skutečnosti, že byl u účastníka řízení veden jako statutární zástupce společnosti a byl tedy disponentem jejího bankovního účtu, k založení běžného účtu (č. ú. na jeho jméno, a to bez jeho vědomí, a jeho osobní údaje v souvislosti s vedením tohoto účtu zpracovával až do 20. listopadu 2018, kdy byl účet zrušen,

   a) porušil zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“),

   b) a dále porušil zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažují za neslučitelné s původními účely („účelové omezení“),

2. a dále tím, že nejméně ve vztahu k založení a vedení výše specifikovaného běžného účtu nezajistil dostatečnou kontrolu dodržování vnitřních předpisů upravujících zabezpečení osobních údajů,

   porušil čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce provést vhodná technická a organizační opatření,

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

pokuta ve výši 80.000 Kč
(slovy osmdesát 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-10246/18-9 ze dne 4. března 2019 pořízený podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a nařízení (EU) 2016/679 Mgr. Danielem Rovanem, inspektorem Úřadu pro ochranu osobních údajů (dále jen „Úřad“), v rámci kontroly provedené u účastníka řízení ve dnech 20. prosince 2018 až 27. února 2019 a spisový materiál shromážděný v rámci této kontroly.

K aplikaci právních předpisů je nezbytné uvést, 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, musel správní orgán s ohledem na trvající charakter porušení specifikovaných ve výroku tohoto příkazu posuzovat odpovědnost účastníka řízení za jeho protiprávní jednání dle právní úpravy účinné v době, kdy došlo k dokončení jednání, tedy k datu zrušení běžného účtu, tj. 20. listopadu 2018. Dále je nutno konstatovat, že dne 24. dubna 2019 nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, který navazuje na přímo použitelný předpis Evropské unie, tj. výše uvedené nařízení (EU) 2016/679. 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. Správní orgán posoudil obě právní úpravy a dospěl k závěru, že novější právní úprava obsažená v zákoně č. 110/2019 Sb. není pro účastníka řízení příznivější, proto celou věc posuzoval podle nařízení (EU) 2016/679.

Ze spisového materiálu shromážděného v rámci kontroly vyplývá, že od roku 2012 zpracovával účastník řízení osobní údaje jako statutárního zástupce u bankovního účtu společnosti a to v rozsahu jméno, příjmení, rodné číslo, datum narození, pohlaví, místo narození, občanství, adresa trvalého pobytu, číslo občanského průkazu včetně jeho platnosti a úřadu, který ho vydal. Dne 10. října 2018 bylo od účastníka řízení doručeno Oznámení o nepovoleném debetním zůstatku běžného účtu (č. ú.), o jehož založení ale nevěděl. Účastník řízení doložil identifikační kartou klienta, že byl dne 21. června 2017 stěžovateli na pobočce v Praze Holešovicích založen běžný účet, nebyla k němu ale nalezena žádná smluvní

dokumentace. Sám účastník řízení v rámci vyřízení stížnosti klienta uvedl, že se případ jeví jako neoprávněné a účelové založení účtu.

Protože účastník řízení reklamaci uznal, účet byl ke dni 20. listopadu 2018 zrušen.

Dále ze spisového materiálu vyplývá, že účastník řízení má upravenu ochranu a zpracování osobních údajů svých klientů v dokumentu „ “ ( ) a v interním předpisu „ “ ( ). K tomu účastník řízení uvedl, že .

Dále účastník řízení předložil interní dokumenty, ze kterých je zřejmý způsob a pravidla nakládání s osobními údaji klientů, a které stanovují pravidla, rozsah a způsob ochrany osobních údajů, jenž jsou závazná minimálně pro všechny zaměstnance účastníka řízení.

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. Účastník řízení tak nepochybně zpracovává osobní údaje svých klientů.

Dle 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, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Účastník řízení v rámci své podnikatelské činnosti v souvislosti s poskytováním bankovních služeb nepochybně zpracovává osobní údaje klientů, neboť je shromažďuje, uchovává a v případě potřeby dále používá (a to včetně jejich zpřístupnění třetím subjektům). Je tedy i správcem údajů svých klientů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své podnikatelské činnosti určil účel a prostředky zpracování.

K výroku 1 tohoto příkazu správní orgán uvádí, že zpracování osobních údajů musí být vždy v souladu se základními zásadami, které jsou zakotveny v čl. 5 nařízení (EU) 2016/679. Tyto zásady představují základní pravidla, od nichž se odvíjejí všechny procesy zpracování, a zároveň jsou též nejdůležitějšími principy, které správci určují, jak má s osobními údajů

nakládat. Jedna ze základních zásad pro zpracování osobních údajů je vyjádřena v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, podle kterého musí být osobní údaje zpracovávány ve vztahu k subjektu údajů korektně a zákonným a transparentním způsobem. Na tuto zásadu pak navazuje čl. 6 odst. 1 nařízení (EU) 2016/679, dle kterého je zpracování zákonné, pouze pokud je splněna nejméně jedna z podmínek stanovených v písm. a) až f) tohoto ustanovení a pouze v odpovídajícím rozsahu. V případě specifikovaném ve výroku tohoto příkazu by bylo zpracování možné jen tehdy, pokud by subjekt údajů uzavřel s účastníkem řízení smlouvu o zřízení běžného účtu. Vzhledem k tomu, že subjekt údajů o založení běžného účtu nevěděl, ani k němu neexistuje žádná jím podepsaná smluvní dokumentace, má správní orgán zato, že smlouva nebyla uzavřena, a proto takové zpracování nelze považovat za korektní ani zákonné.

Další základní zásadou zpracování je zásada účelového omezení zakotvená v čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679, podle které musí být osobní údaje shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažují za neslučitelné s původními účely. Z předložených dokumentů (např. Poučení o zpracování osobních údajů) je zřejmé, že účastník řízení určuje účely zpracování osobních údajů (jednání o smlouvě, poskytování bankovních služeb apod.). Prvotním shromažďováním a zpracováváním osobních údajů byla jeho dispoziční práva k účtu společnosti, ve které vystupoval jako statutární orgán. Tím, že účastník řízení využil tyto osobní údaje a použil je k založení osobního běžného účtu, zjevně překročil účel původního zpracování, a tedy porušil zásadu účelového omezení.

K výroku 2 tohoto příkazu správní orgán konstatuje, že mezi další základní zásady zpracování osobních údajů patří zásada integrity a důvěrnosti stanovená v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, která stanoví, že osobní údaje musí být zpracovány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Na tuto zásadu pak navazuje čl. 32 odst. 1 nařízení (EU) 2016/679, dle kterého musí správce, popř. zpracovatel s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku. Z dokumentů, které účastník řízení v rámci kontroly předložil a které upravují způsob zabezpečení osobních údajů, vyplývá, že má účastník řízení zpracovaná technická a organizační opatření k zajištění ochrany osobních údajů. Na druhou stranu se v případě prokázalo, že u účastníka řízení chybí kontrola dodržování interních předpisů, tedy že nezajistil dodržování zavedených technických a organizačních opatření minimálně po dobu od 21. června 2017 do listopadu 2018. To, že smlouva o zřízení běžného účtu byla uzavřena bez vědomí smluvní strany, se totiž účastník řízení dozvěděl až přímo od dotčeného subjektu údajů, a to více než rok poté, co měla být smlouva uzavřena. Je tedy zcela zjevné, že žádný z nastavených kontrolních mechanismů u správce v tomto případě nezajistil ani to, že nebude smlouva protiprávně uzavřena, ani to, že takto uzavřená smlouva bude správcem odhalena.

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. a) nařízení (EU) 2016/679, neboť existence odpovídajícího právního titulu pro zpracování je základní zásadou pro zpracování osobních údajů, které je nutno vnímat jako nejdůležitější principy určující, jak může správce s osobními údaji nakládat. 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, která hodnota je vyšší.

Při stanovení sankce tak správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, zejména k tomu, že protiprávní jednání trvalo po delší dobu (cca 1 rok a 5 měsíců). Závažnost jednání je zvýšena též skutečností, že obviněný je bankou, tedy profesionálem v oboru, kde dochází k rozsáhlému zpracování osobních údajů. Založení účtu bez vědomí klienta je přitom protiprávním zpracováním osobních údajů, jehož dopad do práv subjektu údajů je zcela zásadní. Přitěžující okolností je též skutečnost, že jednáním účastníka řízení bylo porušeno více povinností stanovených mu nařízením (EU) 2016/679. Závažnost protiprávního jednání naopak snižuje především fakt, že bylo porušení povinnosti prokázáno pouze u jedné dotčené osoby. Po souhrnném zhodnocení všech okolností byla pokuta uložena při samé dolní hranici sazby, kterou nařízení (EU) 2016/679 stanoví a která, jak je výše uvedeno, činí 20 000 000 eur.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že obviněný porušil svým jednáním povinnosti stanovené v čl. 5 odst. 1 písm. a), b) a čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost zpracovávat osobní údaje ve vztahu k subjektu údajů korektně a zákonným a transparentním způsobem, dále povinnost shromažďovat osobní údaje pro určité, výslovně vyjádřené a legitimní účely a povinnost je dále nezpracovávat způsobem, který je s těmito účely neslučitelný, a dále povinnost provést vhodná technická a organizační opatření, a proto rozhodl podle § 150 odst. 1 správního řádu ve spojení s § 90 odst. 1 zákona č. 250/2016 Sb. 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 13. května 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního