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-03432/20-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, a 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 7. září 2020 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, a § 90 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, tento příkaz:

Společnost [redacted]

I. se uznává vinnou ze spáchání přestupku

1. podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušila některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se jako správce osobních údajů svých potenciálních zákazníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že v době minimálně ode dne podání stížnosti, tedy od 11. prosince 2019, do vyhotovení protokolu o kontrole, tedy do 25. května 2020, nedisponovala právním titulem pro zpracování jejich osobních údajů za účelem kontaktování, nabízení svých služeb a vedení v interní evidenci, a dále právním titulem pro zpracování osobních údajů klientů na webových stránkách obviněné dostupných na adrese [redacted] v souvislosti s využitím tzv. cookies,

   čímž porušila zásadu stanovenou 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“),

2. podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušila některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se jako správce osobních údajů svých potenciálních zákazníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že v době minimálně ode dne

podání stížnosti, tedy od 11. prosince 2019, do vyhotovení protokolu o kontrole, tedy do 25. května 2020, uchovávala osobní údaje těchto subjektů po dobu 2 let, ačkoliv pro jejich vedení neměla žádný důvod,

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

3. podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., neboť porušila některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679, kterého se jako správce osobních údajů svých zákazníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že minimálně v období předcházejícímu 10. března 2020 neměla k prováděnému zpracování řádně uzavřenou smlouvu se zpracovatelem, kterého využívala,

   čímž porušila povinnost stanovenou v čl. 28 odst. 3 nařízení (EU) 2016/679, tedy povinnost správce mít se zpracovatelem uzavřenou smlouvu, která jej zavazuje a v níž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektu údajů, povinnosti a práva správce,

4. podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., neboť porušila některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679, kterého se jako správce osobních údajů svých zákazníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že minimálně v období do 12. března 2020 nevedla záznamy o činnostech zpracování,

   čímž porušila povinnost stanovenou v čl. 30 nařízení (EU) 2016/679, tedy povinnost správce vést písemné záznamy o činnostech zpracování obsahující zde uvedené informace,

5. podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb., neboť porušila některé z práv subjektu údajů podle čl. 12 až 22 nařízení (EU) 2016/679, kterého se jako správce osobních údajů svých klientů podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustila tím, že v době minimálně ode dne podání stížnosti, tedy od 11. prosince 2019, do vyhotovení protokolu o kontrole, tedy do 25. května 2020, v souvislosti s využitím tzv. cookies na svých webových stránkách [redacted] za účelem analýzy návštěvnosti a bezpečného provozování stránek neinformovala návštěvníky těchto stránek o době uložení jednotlivých cookies a dalších případných příjemcích osobních údajů,

   čímž porušila povinnost stanovenou v čl. 13 odst. 1 nařízení (EU) 2016/679, tedy povinnost poskytnout subjektu údajů v okamžiku získání osobních údajů zde uvedené informace (informační povinnost),

II. za což se jí podle § 35 písm. b) ve spojení s § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 5 nařízení (EU) 2016/679 ukládá

pokuta ve výši 10.000 Kč
(slovy deset 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 obviněné, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je protokol o kontrole čj. UOOU-05346/19-16 ze dne 25. května 2020 pořízený podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád) a nařízení (EU) 2016/679 a spisový materiál shromážděný v rámci kontroly provedené Úřadem pro ochranu osobních údajů (dále jen „Úřad“) u obviněné, společnosti [redacted], ve dnech 20. března 2020 až 25. května 2020.

Kontrola byla zahájena na základě podnětu doručeného Úřadu dne 11. prosince 2019. Předmětem kontroly bylo dodržování povinností stanovených obviněné nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb. v souvislosti se zpracováním osobních údajů zákazníků a potenciálních zákazníků v rámci její podnikatelské činnosti, zejména v rozsahu povinností dle čl. 5 odst. 1 písm. a), čl. 6 a čl. 13 – 14 nařízení (EU) 2016/679.

Ze spisového materiálu vyplývá, že obviněná za účelem nabídky služeb skrze call centrum a evidence zákazníků zpracovává údaje v rozsahu jméno, příjmení, adresa, telefonní číslo, e-mailová adresa, případně název společnosti a její IČO. 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 obviněná o svých současných i potenciálních zákaznících jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

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. Obviněná v rámci své podnikatelské činnosti nepochybně zpracovává osobní údaje svých současných i potenciálních zákazníků, neboť je shromažďuje, uchovává a v případě potřeby dále používá. Současně je tedy v této souvislosti i správcem údajů výše uvedených subjektů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své činnosti určil účel (nabídka služeb a evidence) a prostředky zpracování (telefonní marketingové hovory, a zasílání informací o nových produktech či službách).

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 údaji nakládat.

K výroku I. bodu 1. tohoto příkazu správní orgán uvádí, že 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 ve vztahu k subjektu zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“). 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.

Ze spisové dokumentace vyplývá, že obviněná dle svého názoru zpracovávala osobní údaje svých potenciálních zákazníků na základě právních titulů souhlas (čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679) a oprávněný zájem (čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679).

V průběhu kontroly bylo zjištěno, že obviněná zpracovávala osobní údaje oslovených zákazníků, kteří projevili souhlas se zpracováním pouze ústně – telefonicky, přičemž tato skutečnost není nikterak zaznamenána či archivována. Osobní údaje klientů obviněné byly zadávány do elektronického systému [redacted] na základě jimi provedeného souhlasu v rámci hovoru s operátorem call centra. Tento záznam zůstával v elektronickém systému až do doby, než zákazník vyplnil písemnou objednávku (poté byl záznam přetransformován na zákaznický). Jelikož však tyto hovory nebyly nahrávány, neexistuje žádný důkaz provedeného souhlasu ve smyslu čl. 7 odst. 1 nařízení (EU) 2016/679, dle kterého musí být správce schopen doložit, že subjekt údajů udělil se zpracováním svých osobních údajů souhlas.

Obviněná dále využívala při zpracování osobních údajů klientů objednávkový formulář na svých webových stránkách dostupných na adrese [redacted], kdy osobní údaje zákazníků byly i v tomto případě zaznamenány do systému [redacted], přičemž v rámci uvedeného formuláře subjekt projevil souhlas pro účely zařazení do interní [redacted] databáze pomocí zaškrtávacího políčka. V těchto případech byl však souhlas vyžadován nadbytečně s ohledem na to, že charakter formuláře již směřoval k provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů.

Obviněná rovněž zpracovávala osobní údaje stávajících zákazníků, které byly získány na základě dotazníků spokojenosti. Součástí těchto dotazníků byla možnost uvedení dalších kontaktů, které by mohly mít o služby obviněné zájem. Na základě těchto kontaktních informací, které byly opět zavedeny do databáze [redacted], pak pracovník call centra volal subjektu údajů a nabízel mu provedení služeb. Takové zpracování osobních údajů se ovšem nedá podřadit pod právní titul oprávněného zájmu, když nebylo zohledněno přiměřené očekávání subjektů údajů (údaje obviněné poskytoval někdo jiný než subjekt údajů, který o tomto poskytnutí ani nebyl informován, a následně byl součástí rozsáhlé databáze obviněné po dobu až dvou let).

Ze spisové dokumentace dále vyplývá, že obviněná využívá na svých webových stránkách dostupných na adrese [redacted] tzv. cookies za účelem analýzy návštěvnosti

a bezpečného provozování stránek. Za souhlas s jejich využitím byla považována pouhá návštěva webových stránek obviněné, což je však v rozporu s čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679.

S ohledem na uvedené je zřejmé, že obviněná nedodržela základní zásadu zákonnosti stanovenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, když ve výše uvedených případech postrádala právní titul pro zpracování osobních údajů.

K výroku I. bodu 2. tohoto příkazu správní orgán uvádí, že provedenou kontrolou bylo zjištěno, že obviněná uchovávala osobní údaje svých klientů po dobu 10 let (zákazníci) a 2 let (ostatní), přičemž zákazníky byli myšleni „zákazníci, kterým byla poskytnuta a vyúčtována práce“, za „ostatní“ pak lze považovat osoby, které byly obviněnou zaneseny do databáze [redacted] na základě údajů poskytnutých třetími osobami (v rámci dotazníků spokojenosti), či osoby, které byly s obviněnou v kontaktu se zájmem o provedení nabízených služeb (telefonicky či formou e-mailu), nicméně k samotné objednávce a uskutečnění již nedošlo. Doba uchování 2 let u těchto subjektů údajů je ovšem neopodstatněná, když pro samotné zpracování údajů těchto osob za uvedeným účelem bylo nezákonné, a pro vedení jejich osobních údajů nebyl shledán žádný důvod.

Vzhledem k uvedené správní orgán konstatuje, že obviněná nedodržela základní zásadu účelového omezení stanovenou v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679, když ve výše uvedených případech bez dalšího opodstatnění uchovávala jejich osobní údaje po dobu 2 let.

K výroku I. bodu 3. tohoto příkazu správní orgán uvádí, že ze spisového materiálu vyplývá, že obviněná jako správce osobních údajů využívání při zpracování osobních údajů svých klientů služeb externího zpracovatele, společnosti [redacted] S tímto zpracovatelem však obviněná neměla dříve než dne 10. března 2020 řádně uzavřenou smlouvu ve smyslu čl. 28 odst. 3 nařízení (EU) 2016/679, dle kterého se zpracování zpracovatelem řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektu údajů, povinnosti a práva správce.

K výroku I. bodu 4. tohoto příkazu správní orgán konstatuje, že z výsledků kontroly je zřejmé, že obviněná je společností, v rámci jejíž podnikatelské činnosti dochází k takovému zpracování, jež nelze označit za příležitostné. Obviněná zpracovává osobní údaje pravidelně, a to jak u svých zaměstnanců, tak u klientů, a proto je povinna vést písemné záznamy o činnostech zpracování ve smyslu čl. 30 nařízení (EU) 2016/679. Obviněná však minimálně v období do 12. března 2020 tyto nevedla, a tedy porušila svou povinnost správce.

K výroku I. bodu 5. tohoto příkazu správní orgán uvádí, že obviněná využívá na svých webových stránkách dostupných na adrese [redacted] tzv. cookies za účelem analýzy návštěvnosti a bezpečného provozování stránek. V rámci kontroly však bylo zjištěno, že obviněná nesplnila povinnost sdělit návštěvníkům stránek dobu uložení jednotlivých cookies a další případné příjemce osobních údajů, které vyplývají z použití cookies. Obviněná tak porušila informační povinnost vyplývající jí z čl. 13 odst. 1 písm. e) a čl. 13 odst. 2 písm. a) nařízení (EU) 2016/679.

Podle § 5 zákona č. 250/2016 Sb. je přestupkem škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

Podle § 41 odst. 1 zákona č. 250/2016 Sb. se za dva nebo více přestupků téhož pachatele projednaných ve společném řízení uloží správní trest podle ustanovení vztahujícího se na přestupek nejpřísněji trestný. Jsou-li horní hranice sazeb pokut stejné, uloží se správní trest podle ustanovení vztahujícího se na přestupek nejzávažnější. Správní orgán tak musel v rámci aplikace tzv. absorpční zásady posoudit, který přestupek spáchaný obviněným je nejzávažnější. Dospěl přitom k závěru, že se jedná o přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť se jednalo o porušení základní zásady, od níž se odvíjejí všechny procesy zpracování, a jejím porušením byl dotčen nejvyšší počet subjektů údajů.

Za porušení 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.

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.

Při stanovení sankce tak správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, zejména k tomu, že protiprávním jednáním byl dotčen vyšší počet subjektů údajů. Přitěžující okolností je též skutečnost, že jednáním účastníka řízení bylo porušeno více povinností stanovených mu nařízením (EU) 2016/679. Dále však správní orgán při rozhodování o uložení sankce a její výši, jako k okolnosti snižující závažnost jednání, přihlédl k tomu, že účastník řízení během kontroly spolupracoval a učinil kroky k nápravě protiprávního stavu. 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 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), v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679, (tedy zásadu, že osobní údaje musí být uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány), v čl. 28 odst. 3 nařízení (EU) 2016/679 (tedy povinnost správce mít se zpracovatelem uzavřenou smlouvu, která jej zavazuje), v čl. 30 nařízení (EU) 2016/679 (tedy povinnost správce vést písemné záznamy o činnostech zpracování) a v čl. 13 odst. 1 nařízení (EU) 2016/679 (tedy povinnost poskytnout subjektu údajů v okamžiku získání osobních údajů zde uvedené informace), 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 7. září 2020

otisk
úředního
razítka

JUDr. Jiří Žůrek
ředitel odboru dozoru
(podepsáno elektronicky)