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-04015/23-13

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „zákon č. 110/2019 Sb.“) 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, dále jen „nařízení (EU) 2016/679“], v řízení o přestupku vedeném podle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (dále jen „zákon č. 250/2016 Sb.“), a zákona č. 500/2004 Sb., správní řád, ve znění dalších předpisů (dále jen „zákon č. 500/2004 Sb.“) rozhodl dne 15. prosince 2023 takto:

[redacted] (dále jen „obviněná“), jako správce osobních údajů [redacted] pacientů a zaměstnanců podle čl. 4 bodu 7 nařízení (EU) 2016/679 (dále jen „subjekty údajů“),

I. je vinna, že bez zbytečného odkladu po spáchání kybernetického útoku [redacted] na servery společnosti [redacted], na kterých měla uložené databáze s osobními údaji subjektů údajů v rozsahu identifikační, kontaktní, ekonomické a finanční údaje, data o poloze a údaje o zdravotním stavu, minimálně do dne 6. října 2023, kdy bylo zahájeno toto řízení, neučinila ohlášení porušení zabezpečení osobních údajů,

   čímž porušila povinnost stanovenou v čl. 33 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce ohlásit dozorovému úřadu jakékoli porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl,

   a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.,

II. za což se jí podle § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 4 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 26.000 Kč
(slovy dvacet šest tisíc korun českých)

III. a dále podle § 95 odst. 1 zákona č. 250/2016 Sb. a vyhlášky 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, ve znění vyhlášky č. 112/2017 Sb., 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 obviněné, konstantní symbol 1148.

IV. Řízení s obviněnou, které se týkalo spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., tím, že bez zbytečného odkladu neoznámila porušení zabezpečení osobních údajů subjektům údajů poté, co došlo [redacted] ke kybernetickému útoku na servery společnosti [redacted], čímž měla porušit povinnost stanovenou v čl. 34 odst. 1 nařízení (EU) 2016/679,

se v rozsahu tohoto skutku podle § 86 odst. 1 písm. a) zákona č. 250/2016 Sb. zastavuje, neboť skutek, o němž se vede řízení se nestal.

Odůvodnění

[1] Řízení ve věci podezření ze spáchání přestupků podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. v souvislosti s kybernetickým útokem na servery obsahující osobní údaje zaměstnanců a pacientů zdravotnického zařízení bylo zahájeno oznámením o zahájení řízení o přestupku čj. UOOU-04015/23-7 ze dne 5. října 2023, které bylo obviněné, společnosti [redacted], doručeno dne 6. října 2023. Podkladem pro vydání tohoto rozhodnutí je spisový materiál čj. UOOU-01752/21 shromážděný v rámci kontroly provedené Úřadem pro ochranu osobních údajů (dále jen „Úřad“) u společnosti [redacted] ve dnech 23. listopadu 2021 až 1. prosince 2022, a to včetně vyřízení námitek předsedou Úřadu čj. UOOU-01752/21-61 ze dne 30. listopadu 2022, a spisový materiál čj. UOOU-00414/23-20 shromážděný v rámci navazujícího řízení o přestupku s danou společností. Z uvedených spisových materiálů vyplynulo podezření z porušení nařízení (EU) 2016/679 i s obviněnou, proto Úřad přistoupil k zahájení řízení.

[2] Součástí Oznámení o zahájení řízení byla výzva ke sdělení kategorií dotčených subjektů údajů a osobních údajů a jejich přibližného počtu a k doložení splnění povinnosti podle čl. 34 odst. 1, čl. 33 odst. 1 a čl. 33 odst. 5 nařízení (EU) 2016/679.

[3] Na uvedenou výzvu obviněná reagovala dne 20. října 2023, kdy uvedla, že nespáchala žádný přestupek. Kybernetickým útokem byly postiženy servery společnosti [redacted] (dále jen „společnost [redacted] Obviněná jako správce osobních údajů jmenovala pověřencem na ochranu osobních údajů společnost [redacted] (dále jen „společnost [redacted], jejíž je obviněná dceřinou společností. Obviněná plní své zákonné povinnosti prostřednictvím externího dodavatele ICT služeb, společnosti [redacted]. Jedním z prvků zabezpečení byla i anonymizace a šifrování prostřednictvím uvedené externí společnosti. Obviněná se rozhodla pro spolupráci s externím dodavatelem cloudových služeb právě z důvodu nutnosti zajištění kvalitního zabezpečení ochrany dat. Obviněná prostřednictvím pověřence neprodleně ohlásila Úřadu porušení zabezpečení osobních údajů

a rovněž tuto skutečnost oznámila dotčeným subjektům údajů. Společnost [redacted] zjistila jako zpracovatel osobních údajů porušení v [redacted] hodin dne [redacted] (k porušení došlo dne [redacted] mezi [redacted] a [redacted] hodin) a téhož dne informovala mateřskou společnost, která telefonicky a e-mailem kontaktovala jednotlivé dceřiné společnosti, včetně obviněné. Ohlášení porušení zabezpečení bylo mateřskou společností odesláno Úřadu datovou schránkou [redacted] dne 16. března 2021. Pacienti a zaměstnanci byli o incidentu informováni prostřednictvím webových stránek obviněné a zaměstnanci navíc i e-mailovou zprávou. Obviněná prostřednictvím své mateřské společnosti nahlásila kybernetický útok rovněž Národnímu úřadu pro kybernetickou bezpečnost a současně bylo podáno trestní oznámení na Policii České republiky vedené pod čj. [redacted]. Obviněná dále uvedla, že nedošlo k žádné ztrátě, poškození nebo úniku osobních údajů, ale pouze k jejich znepřístupnění po určitou dobu. Společnosti [redacted] se podařilo data odšifrovat a subjektům údajů žádná újma nevznikla.

[4] K jednotlivým bodům z Výzvy obviněná sdělila, že porušení zabezpečení osobních údajů se týkalo [redacted] zaměstnanců a [redacted] pacientů. Dotčeny byly tyto kategorie osobních údajů: identifikační (jméno, příjmení, datum narození, rodné číslo, jiný identifikátor), kontaktní (např. adresa, e-mail, telefon), ekonomické a finanční, data o poloze (lokační údaje), a údaje o zdravotním stavu. Přibližný počet osobních údajů u jednotlivých kategorií byl [redacted] Obviněná učinila oznámení porušení zabezpečení osobních údajů subjektům údajů tak, že o kybernetickém útoku subjekty údajů informovala prostřednictvím webových stránek, což doložila screenshotem. Zaměstnance dále informovala e-mailovou zprávou [redacted] a zároveň došlo k vyvěšení dokumentu ze dne [redacted] na obvyklých místech u obviněné tak, aby se informace co nejvíce rozšířila. Obviněná dále uvedla, že porušení zabezpečení ohlásila prostřednictvím své mateřské společnosti, tj. společnosti [redacted], vystupující jako pověřenec pro ochranu osobních údajů, přičemž formulář ohlášení též připojila ke své odpovědi.

[5] Následně ještě dne 1. listopadu 2023 obviněná doložila na základě Výzvy Úřadu Smlouvu o zpracování osobních údajů a Smlouvu o poskytování cloudových služeb, oboje uzavřené se společností [redacted] Z těchto smluv mj. vyplývá, že obviněná vystupuje v pozici správce a společnost [redacted] v pozici zpracovatele osobních údajů. A dále např. v první uvedené smlouvě v části [redacted] je stanovena povinnost zpracovatele v souladu s čl. 33 odst. 2 nařízení (EU) 2016/679 bez zbytečného odkladu, jakmile zjistí porušení zabezpečení osobních údajů, ohlásit toto porušení správci a konkrétní kontaktní údaje.

[6] 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 obviněná o svých zaměstnancích a pacientech a jedná se o údaje identifikační, kontaktní, ekonomické a finanční a data o poloze jsou osobními údajů ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách. Údaje o zdravotním stavu pacientů jsou zvláštní kategorií osobních údajů podle čl. 9 odst. 1 nařízení (EU) 2016/679.

[7] 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 činnosti uchovává osobní údaje svých zaměstnanců a pacientů, které má uložené na serverech, aby byly interně přístupné zaměstnancům pro výkon jejich pracovní činnosti, čímž nepochybně zpracovává osobní údaje zaměstnanců a pacientů, neboť je shromažďuje, uchovává a v případě potřeby dále používá. Je tedy i správcem údajů svých zaměstnanců a pacientů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své podnikatelské činnosti určila účel a prostředky zpracování.

[8] K výroku I. tohoto rozhodnutí správní orgán uvádí, že podle čl. 33 odst. 1 nařízení (EU) 2016/679 má správce povinnost ohlásit dozorovému úřadu jakékoli porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Správcem v daném případě je obviněná. To je stanoveno mj. i ve Smlouvě o zpracování osobních údajů [redacted], kterou obviněná uzavřela se společností [redacted] a podle které je tato společnost zpracovatelem. Dále podle této smlouvy má zpracovatel povinnost informovat správce o bezpečnostním incidentu. Společnost [redacted] dne 15. března 2021 informovala o kybernetickém útoku mateřskou společnost [redacted], která následně učinila i ohlášení na Úřad. Nařízení (EU) 2016/679 ale jasně říká, že ohlášení porušení zabezpečení osobních údajů dozorovému úřadu má učinit správce ohrožených osobních údajů. Úřad obdržel pouze ohlášení od společnosti [redacted], která vystupovala v postavení pověřence pro ochranu osobních údajů, a to dne 16. března 2021, ze kterého plynulo, že dne [redacted] došlo ke kybernetickému útoku a k porušení zabezpečení osobních údajů správce společnosti [redacted], resp. u jejího zpracovatele společnosti [redacted] V ohlášení nebyly uvedeni žádní další správci nebo dotčené subjekty údajů.

[9] Z prvotního ohlášení porušení zabezpečení osobních údajů ze dne 16. března 2021 nijak nevyplynulo, že se mělo týkat obviněné, příp. dalších správců, a nebylo to možné odvodit ani ze skutečnosti, že ohlášení provedla mateřská společnost. Do zahájení tohoto řízení o přestupku Úřad neobdržel žádné ohlášení porušení zabezpečení osobních údajů od správce dotčených údajů, tedy obviněné. Proto považuje správní orgán za prokázané, že obviněná porušila svým jednáním čl. 33 odst. 1 nařízení (EU) 2016/679, když bez zbytečného odkladu a pokud možno do 72 hodin od bezpečnostního incidentu, neohlásila Úřadu porušení zabezpečení osobních údajů svých zaměstnanců a pacientů, a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

[10] Jak vyplývá z výše uvedeného, Úřad má za prokázané, že se obviněná dopustila jednáním popsaným ve výroku I. tohoto rozhodnutí přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. spočívajícího v porušení povinnosti stanovené v čl. 33 odst. 1 nařízení (EU) 2016/679.

[11] Za porušení povinnosti správce podle článků 8, 11, 25 až 39, 42 a 43 nařízení (EU) 2016/679 lze podle čl. 83 odst. 4 nařízení (EU) 2016/679 uložit správní pokutu až do výše 10.000.000 EUR, jedná-li se o podnik, až do výše 2 % z celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

[12] Podle čl. 83 odst. 1 nařízení (EU) 2016/679 dozorový úřad zajistí, aby ukládání správních pokut v souladu s tímto článkem ohledně porušení tohoto nařízení podle odstavců 4, 5 a 6 bylo v každém jednotlivém případě účinné, přiměřené a odrazující; podle čl. 83 odst. 1 nařízení (EU) 2016/679 při rozhodování o výši správní pokuty v jednotlivých případech řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakákoliv jiná přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

[13] Při stanovení druhu správního trestu Úřad přihlédl předně k povaze a závažnosti přestupku dané významem zákonem chráněného zájmu, který byl přestupkem porušen či ohrožen, podle § 38 písm. a) zákona 250/2016 Sb. Zákonem chráněný zájem v této souvislosti je v širším smyslu právo na informace zaručené v čl. 17 odst. 1 Listiny základních práv a svobod. S ohledem na to nebylo možné uvažovat o jiném druhu správního trestu nežli o pokutě.

[14] Při výpočtu pokuty vycházel Úřad z dokumentu Pokyny o výpočtu správních pokut podle obecného nařízení o ochraně osobních údajů vydaného Evropským sborem pro ochranu údajů (dále jen „Pokyny“). Nejprve musel Úřad určit základ pro výpočet pokuty, tedy zjistit, jaká hodnota horní hranice pokuty je vyšší. Dle obchodního rejstříku měla obviněná v roce 2022 čistý obrat ve výši  Kč. Vzhledem k tomu, že vyšší je hodnota 10.000.000 EUR, vzal Úřad tuto částku jako výchozí při stanovení výše pokuty.

[15] Pokud jde o zhodnocení závažnosti přestupku uvedeného ve výroku I. tohoto rozhodnutí, pro účely stanovení základu pro výpočet pokuty, tento přestupek při zohlednění jeho povahy a individuální závažnosti včetně konkrétních okolností, za nichž byl spáchán, Úřad hodnotí jako méně závažný.

[16] Podle Pokynů se tak základ pro výpočet pokuty bude pohybovat mezi 0 až 10 % platné maximální zákonné sazby, tedy podle čl. 83 odst. 4 nařízení (EU) 2016/679 uvedené procento z 10.000.000 EUR. Z důvodu nízké závažnosti Úřad stanovil základ pro výpočet pokuty při dolní hranici sazby, konkrétně ve výši 100.000 EUR, což je přibližně dle kurzovního lístku České národní banky ke dni 13. prosince 2023 (24,48 Kč za 1 EUR) 2.448.000 Kč, která představuje 1 % z maximální výše pokuty podle čl. 83 odst. 4 nařízení (EU) 2016/679. Tuto částku lze dále snížit podle toho, jaký má obviněná čistý roční obrat. Dle obchodního rejstříku měla obviněná v roce 2022 čistý obrat ve výši 181.326.000 Kč, jedná se tedy dle Pokynů o společnost druhé kategorie, u které je možné snížení základu pro výpočet pokuty od 2 % až na 0,3 %. Vzhledem k nízké závažnosti povahy spáchaného přestupku Úřad přistoupil ke snížení na 1 % a určil základ pro výpočet pokuty ve výši 24.480 Kč.

[17] Úřad v souvislosti s rozhodováním o výši pokuty vztahující se k výroku I. neshledal žádnou polehčující okolnost ve smyslu § 39 zákona č. 250/2016 Sb.

[18] Skutečnost, že podle výroku I. obviněná minimálně do zahájení tohoto řízení neučinila nápravu, hodnotí Úřad jako přitěžující okolnost ve smyslu § 40 zákona č. 250/2016 Sb., což promítl do výše pokuty tak, že částku 24.480 Kč navýšil o 10 %, tedy na 26.928 Kč.

[19] S ohledem na výše uvedené vyhodnocení závažnosti přestupku, uložil Úřad obviněné pokutu ve výši částka 26.928 Kč, zaokrouhleno na celé tisíce dolů 26.000 Kč.

[20] Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z § 95 odst. 1 zákona č. 250/2016 Sb., který správnímu orgánu ukládá uložit obviněné, která byla uznána vinnou, 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 obviněná vyvolala porušením své právní povinnosti, činí 1.000 Kč.

[21] K výroku IV. tohoto rozhodnutí Úřad uvádí, že správní řízení bylo zahájeno též pro podezření z porušení povinnosti stanovené v čl. 34 odst. 1 nařízení (EU) 2016/679, podle něhož má správce povinnost oznámit bez zbytečného odkladu porušení zabezpečení osobních údajů subjektu údajů, pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

[22] Úřad při zahájení řízení vycházel zejména ze spisového materiálu shromážděného v rámci řízení týkajícího se stejného kybernetického útoku. Nicméně během tohoto řízení se ukázalo, jak dokládají Úřadu doručené dokumenty ze strany obviněné, konkrétně screenshoty webových stránek obviněné a kopie e-mailové zprávy, obojí obsahující oznámení porušení zabezpečení osobních údajů subjektům údajů, že povinnost stanovenou v čl. 34 odst. 1 nařízení (EU) 2016/679 obviněná dostatečně splnila. Proto Úřad konstatoval, že nedošlo ke spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

[23] Úřad proto řízení dle § 86 odst. 1 písm. a) zákona č. 250/2016 Sb. v rozsahu výroku IV. tohoto rozhodnutí zastavil, neboť skutek, o němž se vede řízení, se nestal.

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 předsedovi 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 15. prosince 2023

Mgr. Eva Cupáková
vedoucí oddělení kontroly soukromého sektoru
(podepsáno elektronicky)