ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.gov.cz, www.uoou.gov.cz

Čj. UOOU-04019/23-19

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 26. února 2024 takto:

[redacted] (dále jen „obviněná“), jako správce osobních údajů [redacted] 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, minimálně do dne 6. října 2023, kdy bylo zahájeno toto řízení, neučinila ohlášení porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů jako dozorovému úřadu, ač nebylo nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob - vzhledem k tomu, že se jednalo o osobní údaje [redacted] osob (zaměstnanců) a některé z těchto údajů lze bezpochyby zařadit mezi údaje zvláštní kategorie osobních údajů (údaje o zdravotním stavu zaměstnanců) a údaje zranitelných osob (rodná čísla dětí zaměstnanců),

   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 ve formě nedbalosti 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 16.000 Kč
(slovy šestnáct 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 **paušální částku nákladů 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.

Dále Úřad pro ochranu osobních údajů ve zbytku vydávává toto

usnesení:

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 podle ustanovení § 86 odst. 1 písm. a) zákona č. 250/2016 Sb. zastavuje, neboť skutek, o němž bylo řízení vedeno, 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 zdravotnického zařízení bylo zahájeno oznámením o zahájení řízení o přestupku čj. UOOU-04019/23-7 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 [redacted] (k porušení došlo [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] (pověřencem pro ochranu osobních údajů) dne 16. března 2021. 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, k porušení zabezpečení osobních údajů pacientů nemocnice nedošlo. Osobní údaje a zdravotní dokumentace pacientů byly uloženy na vlastním serveru, jenž nebyl předmětem kybernetického útoku. U zaměstnanců byly dotčeny tyto kategorie osobních údajů: identifikační (jméno, příjmení, datum narození, rodné číslo, jiný identifikátor), kontaktní (např. adresa, e-mail, telefon), ekonomické a finanční. Přibližný počet osobních údajů u jednotlivých kategorií byl [redacted] Obviněná učinila oznámení porušení zabezpečení osobních údajů subjektům údajů (zaměstnancům) tak, že o kybernetickém útoku subjekty údajů informovala prostřednictvím písemného oznámení. Obviněná dále uvedla, že porušení zabezpečení ohlásila prostřednictvím své mateřské společnosti, tj. společnosti [redacted], která je na základě smlouvy zpracovatelem osobních údajů obviněné, přičemž ke svému vyjádření připojila i dokumentaci všech případů porušení zabezpečení osobních údajů, trestní oznámení na Policii České republiky, oznámení Národnímu úřadu pro kybernetickou bezpečnost, oznámení společnosti [redacted], oznámení zaměstnancům a formulář ohlášení porušení zabezpečení osobních údajů.

[5] Následně ještě dne 1. listopadu 2023 obviněná doložila na základě výzvy Úřadu smlouvu o zpracování osobních údajů [redacted] a smlouvu o poskytování služeb ze dne [redacted], které byly uzavřeny 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 IV. 9. 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] Na další výzvu Úřadu obviněná reagovala dne 28. listopadu 2023, kdy uvedla, že její jednatelka dala vedoucím pracovníkům e-mailový pokyn ze [redacted] (kopii e-mailové zprávy připojila ke své odpovědi) k distribuci písemného oznámení podřízeným zaměstnancům o porušení zabezpečení osobních údajů. Ti pak seznámili své podřízené zaměstnance. Dále obviněná namítla, že osobní údaje, které měla uložené na cloudu, byly šifrované, což doložila komunikací mezi jejím pověřencem pro ochranu osobních údajů a společností [redacted], kde je uvedeno, že nemocniční informační systémy ukládají svá data šifrovaně, aby je nemohl rozklíčovat ani administrátor systému. Přístupy jsou po autentizaci. Vzhledem k průběhu útoku a jeho podchycení nemohlo dojít k přenosu konzistentní databáze, i kdyby došlo k částečnému přenosu, data by byla nečitelná. Současně upozornila na ustanovení čl. 34 odst. 3 písm. a) nařízení (EU) 2016/679, kdy se nevyžaduje oznámení porušení zabezpečení osobních údajů subjektům údajů v případě, že byla u osobních údajů použita taková opatření, která je činí nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, např. šifrování. Vzhledem k tomu, že po útoku zůstaly osobní údaje vzhledem k jejich zašifrování pro útočníky nedostupné, neměla obviněná podle svého názoru ani oznamovací povinnost.

[7] Obviněná dne 12. a 31. ledna 2024 odpověděla Úřadu na jeho další výzvu. Doplnila listinu, kterou byly poskytnuty informace zaměstnancům společnosti po kybernetickém útoku. Následně ještě doplnila odpovědi na dotazy Úřadu. Dodavatelem účetního programu [redacted] a mzdového programu [redacted], které používá, je společnost [redacted], [redacted], která není správcem ani provozovatelem [redacted] serverů s daty uživatelů. V obou programech bylo používáno bezpečnostní opatření [redacted], kdy data může vidět jen autorizovaný uživatel po zadání hesla, provozovatel cloud serveru nemůže tato data přečíst. Pokud se jedná o přístup do programu [redacted], tak tyto umožňují přístup pouze uživatelům, kteří se do něj přihlásí svými přihlašovacími údaji a dle přednastavených práv mají přístup například pouze k určitým agendám. Přístupové heslo je [redacted] Přístup k [redacted] je možný opět pouze [redacted]. Z uvedených důvodů má obviněná zato, že osobní údaje byly dostatečně zabezpečeny proti neoprávněnému přístupu a proti jakémukoli zneužití.

[8] 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 jedná se o údaje identifikační, kontaktní, ekonomické a finanční, jsou osobními údajů ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

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

[10] 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 ze dne [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] informovala o kybernetickém útoku obviněnou (prostřednictvím kontaktní osoby paní [redacted] i společnost [redacted] (jež je mateřskou společností obviněné), a která následně učinila i ohlášení na Úřad. Nařízení (EU) 2016/679 ale jasně říká, že ohlášení porušení zabezpečení osobních údajů dozorovému úřadu má vždy 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 [redacted] došlo ke kybernetickému útoku a k porušení zabezpečení osobních údajů správce společnosti [redacted], resp. u jejího zpracovatele společnosti [redacted] V ohlášení nebyli uvedeni žádní další správci nebo dotčené subjekty údajů.

[11] 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. Současně k ohlašovací povinnosti Úřad doplňuje, že v okamžiku, kdy se správce dozvěděl o kybernetickém útoku, měl nejprve posoudit, zda událost, o které se dozvěděl, skutečně představuje porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů, příp. jestli se obecně jedná o narušení důvěrnosti, integrity či dostupnosti zpracovávaných osobních údajů. Vzhledem k tomu, že si správce musel danou situaci vyhodnotit tak, že alespoň jedno z uvedených rizik bylo reálné, měl povinnost bezodkladně událost ohlásit Úřadu. 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 (kybernetický útok) na server obsahující osobní údaje subjektů údajů (zaměstnanců obviněné), a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

Výjimku z ohlašovací povinnosti tvoří případ, kdy je nepravděpodobné, že by porušení (bezpečnosti) mělo za následek riziko pro práva a svobody fyzických osob. Jak vyplývá ze samotného vyjádření správce, správce zcela ztratil k datům na cloud serveru přístup – a to nejméně po dobu několika dní, přičemž data na cloud serveru se vztahovala k subjektům údajů – zaměstnancům, kdy šlo zejména o jména, adresy, rodná čísla, čísla občanských

průkazů, e-maily, telefonu, příslušnost ke zdravotním pojišťovnám, informace o exekucích a insolvencích, čísla bankovních účtů, informace o výši mezd, rodná čísla dětí.

Správce tak ztratil přístup k osobním údajům, z nichž některé by se týkaly zranitelných osob (rodná čísla dětí) a některé zvláštních kategorií osobních údajů (u zaměstnavatele lze předpokládat, že shromažďuje určité údaje o zdravotním stavu svých zaměstnanců (pro potřeby personální a mzdové).

K tomuto dozorový úřad uvádí, že je důležité si uvědomit, že porušením není pouze ztráta, zničení či změna údajů nebo neautorizovaný přistup k nim, **ale může se jednat také o situace nedostupnosti osobních údajů, a to dočasně. Podle čl. 32 odst. 1 písm. b) má správce povinnost zajistit ,,neustálou důvěrnost, integritu, dostupnost a odolnost systémů", a proto ztráta dostupnosti některých systémů může být porušením bezpečnosti osobních údajů a správce by měl incident vždy zdokumentovat, případně nahlásit.**[1]

[12] 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.

[13] 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.

[14] 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 se 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;

[1] Pattynová, J., Suchánková, L., Černý, J., Růžička, M. a kolektiv: Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář. 2. vydání. Praha: Leges, 2019, 752 s.

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.

[15] 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 č. 250/2016 Sb. Zákonem chráněný zájem, tj. osobní údaje subjektů údajů, byly vzhledem k šifrování příslušného cloud serveru pro pachatele kybernetického útoku nesrozumitelné. Následek daného přestupku byl v daném případě pouze ohrožovací, nikoliv poruchový, neboť v řízení nevyšlo najevo, že by jednáním obviněné (v tomto případě ve formě opomenutím) došlo ke vzniku škody (zejména vůči subjektům údajů). Jako polehčující okolnost Úřad vyhodnotil skutečnost, že obviněná s úřadem v přestupkovém řízení spolupracovala a na výzvy úřadu včas reagovala.

[16] Dozorový úřad dospěl k závěru, že v daném případě nebyl přestupek spáchán úmyslně, ale z nedbalosti. Obviněná nesplnila ohlašovací povinnost stanovenou v čl. 34 odst. 1 nařízení (EU) 2016/679. Vzhledem k okolnostem případu dospěl Úřad k závěru, že obviněná spáchala daný přestupek minimálně ve formě nedbalosti nevědomé; tedy nevěděla, že svým jednáním (v tomto případě opomenutím) může porušit nebo ohrozit zájem chráněný zákonem, ač to vzhledem k okolnostem a svým osobním poměrům vědět měla a mohla, neboť obviněná se bez dalšího spokojila s tím, že ohlášení porušení zabezpečení osobních údajů dle GDPR učinila její mateřská společnost [redacted] a. s., ačkoliv z obecného nařízení (EU) 2016/679 vyplývá, že porušení zabezpečení má učinit každý jednotlivý správce osobních údajů.

[17] 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 [redacted] Kč. Vzhledem k tomu, že vyšší je hodnota 10.000.000 EUR, vzal Úřad tuto částku jako výchozí při stanovení výše pokuty.

[18] 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.

[19] 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, kdy se přestupek netýkal zvláštní kategorie osobních údajů podle čl. 9 nařízení (EU) 2016/679, Úřad stanovil základ pro výpočet pokuty při dolní hranici sazby, konkrétně ve výši 60.000 EUR, což je přibližně dle kurzovního lístku České národní banky ke dni 23. února 2024 (25,35 Kč za 1 EUR) 1.521.000 Kč, která představuje 0,6 % 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 105.209.000 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 15.210 Kč.

[20] 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 14.988 Kč navýšil o 10 %, tedy na 16.731 Kč.

[21] S ohledem na výše uvedené vyhodnocení závažnosti přestupku, uložil Úřad obviněné pokutu ve výši částka 16.487 Kč, zaokrouhleno na celé tisíce dolů 16.000 Kč.

[22] 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.

[23] 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.

[24] 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 kopie e-mailového pokynu pro vedoucí ve vztahu k jejich podřízeným zaměstnancům a kopie sdělené, se kterým byli tito zaměstnanci seznámeni, 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.

[25] Úřad proto řízení o tomto skutku s odkazem na ustanovení § 86 odst. 1 písm. a) správního řádu usnesením zastavil, neboť v tomto ustanovení je uvedeno, že správní orgán řízení usnesením zastaví, jestliže 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.

Proti usnesení, kterým bylo rozhodnuto ve IV. výroku, lze rovněž u Úřadu pro ochranu osobních údajů podat rozklad ve lhůtě 15 dnů ode dne doručení usnesení předsedovi Úřadu pro ochranu osobních údajů. Rozklad proti tomuto výroku nemá odkladný účinek (ustanovení § 76 odst. 5 zákona č. 500/2004 Sb.).

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 26. února 2024

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