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-00414/23-20

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 10. května 2023 takto:

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

I. je vinna, že od spáchání kybernetického útoku dne 14. března 2021 do zahájení tohoto řízení nedoložila, že by ve smyslu čl. 34 nařízení (EU) 2016/679, jež promítá zásadu transparentnosti dle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, oznámila porušení zabezpečení osobních údajů následkem kybernetického útoku na servery, 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 ze dne 14. března 2021 subjektům údajů,

   čímž porušila povinnost stanovenou v čl. 5 odst. 2 nařízení (EU) 2016/679, tedy povinnost správce doložit dodržení souladu se základními zásadami uvedenými v odst. 1 daného článku,

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

II. je vinna, že bez zbytečného odkladu po spáchání kybernetického útoku dne 14. března 2021 na servery, 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, až do dne 23. listopadu 2021 neohlásila tento útok Úřadu pro ochranu 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.,

III. je vinna, že dokumentace zaznamenávající porušení zabezpečení způsobené kybernetickým útokem dne 14. března 2021 neobsahovala účinky daného porušení, jakožto povinný údaj dle čl. 33 odst. 5 nařízení (EU) 2016/679,

čímž porušila povinnost stanovenou v čl. 33 odst. 5 nařízení (EU) 2016/679, tedy povinnost správce dokumentovat veškeré případy porušení zabezpečení osobních údajů, včetně uvedení skutečností, které se daného porušení týkají, jeho účinky a přijatá nápravná opatření,

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

IV. za což se jí podle § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 4 písm. a) a čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 309.000 Kč
(slovy tři sta devět tisíc korun českých)

V. 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.

Odůvodnění

[1] Řízení ve věci podezření ze spáchání přestupků podle § 62 odst. 1 písm. a) a b) 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-00414/23-5 ze dne 23. ledna 2023, které bylo obviněné, [redacted], doručeno dne 25. ledna 2023. Podkladem pro vydání tohoto rozhodnutí je podnět ze dne 1. dubna 2021 a spisový materiál čj. UOOU-00414/23 a též spisový materiál čj. UOOU-01752/21 shromážděný v rámci kontroly provedené Úřadem pro ochranu osobních údajů (dále jen „Úřad“) 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.

[2] Dne 1. dubna 2020 byla Úřadu doručena stížnost, ve které bylo uvedeno, že se stěžovatel z medií dozvěděl o bezpečnostním incidentu v počítačové síti [redacted] provozované obviněnou, u které je evidován jako pacient. Na základě této informace se na obviněnou obrátil s dotazem na rozsah a detaily incidentu. Jednatelka obviněné mu v odpovědi ze dne 1. dubna 2020 odmítla sdělit bližší informace s odkazem, že šetření dále probíhá.

[3] Úřad obdržel dne 16. března 2021 ohlášení porušení zabezpečení osobních údajů od [redacted] (dále jen [redacted]. V ohlášení bylo uvedeno, že dne 14. března 2021 v ranních hodinách došlo k hackerskému útoku na servery [redacted] (dále jen [redacted], která byla v roli zpracovatele vůči ohlašující [redacted]. Vzhledem k tomu, že Úřad neobdržel žádné ohlášení incidentu od obviněné, jakožto správce osobních údajů zaměstnanců a pacientů, kterých se měl útok týkat, přistoupil k zahájení kontroly.

[4] Dne 23. listopadu 2021 proběhlo u obviněné ústní jednání a místní šetření. Poté, co byla obviněná vyzvána k popisu incidentu, předložila osobám pověřeným ke kontrole *Ohlášení zabezpečení osobních údajů*, přičemž šlo o totéž ohlášení jako bylo Úřadu doručeno od [redacted]. Nicméně po dovysvětlení vzal Úřad toto ohlášení jako dodatečné ohlášení učiněné obviněnou. Následně došlo k popisu technického řešení pro zabezpečení osobních údajů a předložení [redacted] mezi obviněnou a [redacted], přičemž na základě této smlouvy [redacted] mimo jiné poskytovala obviněné službu uložení zpracovávaných osobních údajů na serverech společnosti. Dále obviněná předložila Úřadu [redacted] a vzhledem k tomu, že obviněná řešila incident i s Policií České republiky, Obvodním ředitelstvím policie [redacted], Službou kriminální policie a vyšetřování, [redacted] 3 (dále jen „Policie ČR"), též doložila Úřadu *Úřední záznam o podaném vysvětlení podle § 158 odst. 6 trestního řádu* ze dne 15. března 2021 [redacted], učiněném [redacted], jednatelem [redacted]. Na Policii ČR [redacted] vypověděl, že dne 15. března 2021 [redacted] zjistila, že došlo k hackerskému útoku na její servery, a to tak, že jednotlivé soubory byly zaheslovány a tudíž znepřístupněny. K prolomení zabezpečení mohlo dojít dvěma způsoby, a to zneužitím [redacted] nebo prolomením [redacted]. Kromě výše uvedeného ohlášení předložila obviněná *Formulář hlášení kybernetického bezpečnostního incidentu*, z nějž je patrno, že ho učinila [redacted], a to jménem [redacted], kdy se mělo jednat o závažný kybernetický bezpečnostní incident vedoucí k průniku do systému. Ani z tohoto hlášení, ani z podání vysvětlení na Policii ČR však nevyplývá, že by se kybernetický útok měl týkat i jiného správce osobních údajů, nežli [redacted]. K této skutečnosti obviněná doplnila, že ohlášení bylo učiněno [redacted], protože se jedná o mateřskou společnost a vzhledem k tomu, že se porušení zabezpečení osobních údajů týkalo více společností mateřské společnosti, veškeré dokumenty k incidentu, včetně hlášení na všechny tyto společnosti, učinila mateřská [redacted]. Obsahem daného hlášení byla i informace, že pacienti (subjekty údajů) nebudou informováni z důvodu, že by to znamenalo nepřiměřené úsilí s dodatkem, že tak bude ale učiněno prostřednictvím webových stránek. Dle vyjádření obviněné byly subjekty

údajů o incidentu informovány prostřednictvím zprávy vyvěšené na webových stránkách společnosti od 15. do 21. března 2021 s následujícím textem: „*OZNÁMENÍ O KYBERNETICKÉM ÚTOKU – Dne 14.3.2021 se stalo naše zdravotnické zařízení cílem kybernetického útoku. Momentálně probíhá intenzivní vyšetřování incidentu. Zřejmě došlo k porušení dostupnosti dat. Naše zdravotnické zařízení již pracuje ve spolupráci s IT specialisty na znovuobnovení dostupnosti dat a jejich odšifrování. Vyvineme maximální úsilí pro zajištění bezpečnosti Vašich dat. Poskytování lékařské péče zůstává z naší strany nepřerušeno. V případě Vaší potřeby získat více informací o útoku, kontaktujte našeho pověřence pro ochranu osobních údajů, jehož kontakt je uvedený na našich webových stránkách. Kybernetické napadení řešíme ve spolupráci s naším pověřencem, IT odborníky, Úřadem pro ochranu osobních údajů, Národním úřadem pro kybernetickou a informační bezpečnost a Policií ČR.“* Nicméně skutečnost, že byl daný text v danou dobu skutečně zveřejněn, obviněná nedokázala doložit, kdy toto zdůvodnila změnou svého jednatele. Pacienti měli být informováni ještě ústně při návštěvách zdravotnického zařízení, na recepci [redacted]. Obviněná nezaznamenala ke zveřejněným a poskytnutým informacím žádné reakce ze strany dotčených subjektů údajů.

[5] Z kontrolního protokolu, konkrétně ze [redacted], vyplývá, že obviněná byla v pozici správce osobních údajů a [redacted], která jí na základě této smlouvy poskytuje komplexní cloudové a související IT služby, v pozici zpracovatele osobních údajů zaměstnanců a pacientů obviněné. V související [redacted] je mj. stanovena povinnost zpracovatele zavést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, ohlásit porušení zabezpečení osobních údajů správci nebo zpracovávat osobní údaje na základě pokynů správce. Z přijatých opatření lze jmenovat zřízení [redacted]

[redacted]. Kdyz se [redacted] dozvedela o kybernetickém útoku, kontaktovala v den zjištění, tj. dne 15. března 2021, [redacted], která následně telefonicky informovala vlastní jednotlivé dotčené společnosti, včetně obviněné. Následně [redacted] zaslala dne 18. března 2021 písemně správcům všech dotčených společností spadajících pod [redacted], [redacted] oznámení o narušení bezpečnosti prostředí společnosti.

[6] [redacted] provozuje [redacted] virtuálních serverů. [redacted]

[redacted]

[7] Obviněná má vypracován dokument *Ohlášení porušení zabezpečení osobních údajů,* pro případná hlášení incidentů, ve kterém je přímo uvedeno, že povinnost ohlásit porušení zabezpečení osobních údajů má správce osobních údajů. Dále obviněná disponuje dokumentací všech případů porušení zabezpečení osobních údajů, která ke dni 23. listopadu 2021 (den místního šetření, při kterém dokument prokázala) obsahovala pouze 1 záznam (předmětného hackerského útoku). Z dokumentu nelze vyvodit, k jakému datu byla

zahájena evidence incidentů. V dokumentu je toliko uvedeno datum porušení *„14. března 2021“*, popis případu zabezpečení *„Hackerský útok Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému*“, účinky porušení zabezpečení *„Malicious Code (např. virus, červ, trojský kůň, dialer, spyware) Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, „O-Day“ útok) Intrusions (např. kompromitace aplikace nebo uživatelského účtu)“* a přijatá opatření *„Předpokládalo se, že bez ohledu na rozsah škod je celé původní prostředí kompromitované. Z tohoto důvodu proběhla zcela nová instalace celého prostředí, čistých serverů, generování nových přístupů, instalace čistých aplikací, instalace nových bezpečnostních řešení. Problém byl vyřešen a data byla dešifrována. Došlo k zcela nové instalace celého prostředí, čistých serverů, generování nových přístupů, Instalace čistých aplikací, instalace nových bezpečnostních řešení. Nedošlo k úniku dat.“*

[8] Kybernetický útok v podstatě spočíval v dočasném zablokování přístupu k datům. Odblokování systému trvalo přibližně týden. Dotčenými subjekty údajů byly zaměstnanci nebo osoby v pracovněprávním vztahu ke správci nebo zpracovateli, uživatelé a zákazníci (pacienti). Přibližný počet subjektů údajů byl [redacted] zaměstnanců a [redacted] pacientů. Mezi dotčené kategorie osobních údajů patřily identifikační, kontaktní, ekonomické a finanční údaje a data o poloze. V rámci zvláštní kategorie osobních údajů se jednalo o informace o zdravotním stavu.

[9] Dne 17. srpna 2022 byly Úřadu doručeny námitky proti kontrolnímu protokolu. Pouze jedna námitka byla směřována proti kontrolnímu zjištění týkajícího se porušení povinnosti, pro kterou bylo zahájeno řízení o přestupku, nicméně předseda Úřadu danou námitku v rámci dokumentu *Vyřízení námitek proti kontrolním zjištěním uvedeným v protokolu o kontrole* ze dne 30. listopadu 2022, čj. UOOU-01752/21-61, zamítl.

[10] Řízení o přestupku bylo zahájeno dne 25. ledna 2023 doručením *Oznámení o zahájení řízení* pro porušení povinnosti podle čl. 33 odst. 1, čl. 33 odst. 5 a čl. 34 odst. 1 nařízení (EU) 2016/679. Obviněná na něj reagovala svým vyjádřením, ve kterém uvedla, že jmenovala svým pověřencem [redacted], kdy obviněná je její dceřinou společností a sama si řeší své zákonné povinnosti prostřednictvím externího dodavatele ICT služeb, kterým je [redacted]. Tato společnost řeší i bezpečnostní opatření včetně anonymizace a šifrování osobních údajů. [redacted] informovala [redacted] o kybernetickém útoku, ta telefonicky i písemně kontaktovala jednotlivé dceřiné společnosti včetně obviněné. To, že ohlášení porušení zabezpečení osobních údajů provedla [redacted] jako pověřenec, nepovažuje obviněná za porušení čl. 33 odst. 1 nařízení (EU) 2016/679. Pacienti dle tvrzení obviněné byli informováni prostřednictvím webových stránek a zdravotnických pracovníků. Obviněná závěrem ještě doplnila, že nedošlo k žádné ztrátě dat a data se podařilo dešifrovat.

[11] Dne 2. března 2023 byla obviněné zaslána výzva ke sdělení, jakým způsobem splnila povinnost podle čl. 33 odst. 5 a čl. 34 odst. 1 nařízení (EU) 2016/679 a kolik měla v době incidentu klientů. Téhož dne zaslal Úřad výzvu i [redacted] s dotazem, jaký byl počet klientů a zaměstnanců u jednotlivých společností [redacted], které byly postiženy kybernetickým útokem.

[12] Dne 3. března 2023 byla Úřadu doručena odpověď, ve které obviněná sdělila, že se na ni vztahuje výjimka. Podle čl. 34 odst. 3 nařízení (EU) 2016/679 se totiž oznámení subjektu údajů nevyžaduje, zavede-li správce náležitá technická a organizační opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, jako je např. šifrování, které bylo v případě obviněné použito [redacted]. Obviněná též přijala následná opatření, která zajistila, že vysoké riziko pro práva a svobody subjektů údajů podle odst. 1 se již pravděpodobně neprojeví. Žádná data nebyla nikomu zpřístupněna. Pacienti a zaměstnanci přesto byli o kybernetickém incidentu v pondělí 15. března 2021 informováni osobně na recepci [redacted], na webových stránkách a v médiích. Hackerské napadení serverů [redacted] způsobilo dočasné (týdenní) porušení dostupnosti dat a velmi zkomplikovalo práci všem zdravotníkům, zaměstnancům a klientům [redacted]. Důsledkem incidentu byly finanční ztráty a poškození pověsti [redacted]. Následkem kybernetického útoku ze dne 14. března 2021 nedošlo k porušení důvěrnosti dat ani k porušení integrity dat a ani ke ztrátě dat. [redacted] se povedlo data odšifrovat a znovu zpřístupnit. [redacted]. Obviněná ke dni kybernetického útoku disponovala údaji asi [redacted] klientů, jejichž data byla šifrována, a tudíž nebyla v důsledku útoku ohrožena. Obviněná ke svému vyjádření přiložila i dokumentaci všech případů porušení zabezpečení osobních údajů. Dne 8. března 2023 byla odpověď ještě doplněna o *Dokumentaci všech případů porušení zabezpečení osobních údajů* [redacted]. Tento dokument obsahoval jeden zápis vztahující se k předmětnému incidentu a popis tohoto případu porušení zabezpečení, účinky porušení zabezpečení, přijatá opatření a datum oznámení Úřadu.

[13] Dne 9. března 2023 byla Úřadu doručena odpověď [redacted], ve které sdělila, že si nevedla žádný seznam zaměstnanců nebo zákazníků (pacientů) u jednotlivých spravovaných [redacted] a proto netuší, kolika zaměstnanců a pacientů se útok mohl týkat.

[14] Dne 23. března 2023 obdržel Úřad čestné prohlášení jednatelky obviněné týkající se informování klientů a zaměstnanců prostřednictvím webových stránek hned po útoku a dále ústně prostřednictvím zdravotnických pracovníků při návštěvě [redacted].

[15] 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, 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.

[16] 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.

[17] K výroku I. tohoto rozhodnutí správní orgán předně uvádí, že v průběhu řízení o přestupku Úřad překvalifikoval přestupek, resp. porušení povinnosti nově posoudil podle čl. 5 odst. 2 nařízení (EU) 2016/679, o čemž obviněnou písemně informoval. Podle tohoto článku má správce povinnost doložit dodržení souladu se základními zásadami uvedenými v čl. 5 odst. 1 nařízení (EU) 2016/679. Jedná se o další ze zásad uvedených v tomto článku, tentokrát tzv. zásada odpovědnosti, která se skládá ze dvou důležitých povinností správce. Prvně správce odpovídá za dodržení všech povinností, které vyplývají ze zásad uvedených v čl. 5 odst. 1 nařízení (EU) 2016/679 a současně musí být schopen doložit dodržení oněch zásad, čímž je zakotven proaktivní přístup správce v oblasti ochrany osobních údajů.

[18] Čl. 34 odst. 1 nařízení (EU) 2016/679 upravuje oznamovací povinnost správce vůči subjektům údajů v případě porušení zabezpečení osobních údajů, což musí učinit bez zbytečného odkladu. Podmínkou pro vznik této povinnosti je pravděpodobné vysoké riziko pro práva a svobody fyzických osob (subjektů údajů) plynoucí z porušení zabezpečení jejich osobních údajů. Vzhledem k tomu, že se osobní údaje v souvislosti s kybernetickým útokem na servery správce staly nedostupnými a správce nad nimi po dobu jednoho týdne ztratil kontrolu, došlo k porušení zabezpečení osobních údajů. Navíc v případě osobních údajů pacientů se jednalo o zvláštní kategorii osobních údajů (informace o zdravotním stavu). Čl. 34 odst. 1 nařízení (EU) 2016/679 promítá zásadu transparentnosti zakotvenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, podle které musí být osobní údaje ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem. Podle tohoto článku měla obviněná povinnost postupovat vůči svým pacientům a zaměstnancům transparentně v tom smyslu, že je měla informovat o porušení zabezpečení jejich osobních údajů. Obviněná sice v rámci svých vyjádření tvrdila, že subjekty údajů o bezpečnostním incidentu informovala (měla vyvěsit informaci na svých webových stránkách a ústně pacienty informovat při návštěvě v jejím zdravotnickém zařízení), ale žádným způsobem tato svá tvrzení nedoložila, čímž nedodržela zásadu odpovědnosti podle čl. 5 odst. 2 nařízení (EU) 2016/679 popsanou výše. Samotné čestné prohlášení bývalé jednatelky obviněné, které v průběhu řízení o přestupku obviněná dodala, bez dalšího není schopné prokázat, že obviněná dostála své povinnosti dle čl. 34 nařízení (EU) 2016/679.

[19] Vzhledem k tomu, že obviněná nedoložila, že by ve smyslu čl. 34 nařízení (EU) 2016/679, jež promítá zásadu transparentnosti dle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, oznámila porušení zabezpečení osobních údajů následkem kybernetického útoku na servery, na kterých měla uložené databáze s osobními údaji subjektů údajů, považuje správní orgán za prokázané,

že obviněná porušila svým jednáním čl. 5 odst. 2 nařízení (EU) 2016/679, a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.

[20] K výroku II. 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 [redacted], kterou obviněná uzavřela se [redacted] a podle které je tato společnost zpracovatelem. Dále podle této smlouvy má zpracovatel povinnost informovat správce o bezpečnostním incidentu. To učinil dne 18. března 2021, kdy odeslal dotčeným správcům, tedy i obviněné, oznámení o narušení bezpečnosti prostředí společnosti. Nařízení (EU) 2016/679 jasně říká, že ohlášení porušení zabezpečení osobních údajů dozorovému úřadu má učinit správce ohrožených osobních údajů. Úřad obdržel pouze ohlášení od [redacted], která vystupovala v postavení pověřence pro ochranu osobních údajů, a to dne 16. března 2021, ze kterého plynulo, že dne 14. března 2021 došlo ke kybernetickému útoku a k porušení zabezpečení osobních údajů správce [redacted], resp. u jejího zpracovatele [redacted]. V ohlášení nebyly uvedeni žádní další správci nebo dotčené subjekty údajů. Při místním šetření spojeném s ústním jednáním dne 23. listopadu 2021 obviněná předložila kontrolujícím ohlášení zabezpečení (totožné s ohlášením, které Úřadu zaslala [redacted] s vysvětlením, že daný bezpečnostní incident se týkal rovněž obviněné.

[21] 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. Úřad uznal splnění ohlašovací povinnosti až v den místního šetření a ústního jednání uskutečněného dne 23. listopadu 2021, kdy sice obviněná předložila totožné ohlášení porušení zabezpečení osobních údajů jako bylo dne 16. března 2021 doručeno Úřadu, ale současně poskytla dovysvětlení, že se tento incident týkal také přímo jí. Nicméně splnění povinnosti bylo učiněno opožděně, 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.

[22] K výroku III. tohoto rozhodnutí správní orgán uvádí, že dle čl. 33 odst. 5 nařízení (EU) 2016/679 má správce povinnost dokumentovat veškeré případy porušení zabezpečení osobních údajů, včetně uvedení skutečností, které se daného porušení týkají, jeho účinky a přijatá nápravná opatření.

[23] Obviněná předložila požadovaný dokument obsahující pouze jeden záznam, a to týkající se předmětného narušení zabezpečení osobních údajů ze dne 14. března 2021. Dokument obsahoval popis skutečností vztahujících se k porušení zabezpečení i opatření, která byla následně přijata. Dále zde byly vypsány účinky porušení zabezpečení (virus, červ, trojský kůň a další). K tomu správní orgán uvádí, že virus, červ, trojský kůň a další nejsou účinky porušení zabezpečení, ale jedná se o příčiny či důvody, v důsledku, kterých došlo ke kybernetickému napadení. Pokud by obviněná měla dostát své povinnosti plynoucí z daného ustanovení nařízení (EU) 2016/679, musela by v dokumentu rozepsat, jaký dopad mělo porušení zabezpečení a alespoň rozsah dotčených osobních údajů.

[24] Vzhledem k tomu, že z dokumentace případu porušení zabezpečení nevyplývají účinky daného porušení, považuje správní orgán za prokázané, že obviněná porušila svým jednáním čl. 33 odst. 5 nařízení (EU) 2016/679, když nedostatečně dokumentovala případ porušení zabezpečení osobních údajů, především jeho účinky, a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

[25] 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. b) zákona č. 110/2019 Sb. spočívajícího v porušení povinnosti stanovené v čl. 5 odst. 2 nařízení (EU) 2016/679, jednáním popsaným ve výroku II. 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 a jednáním popsaným ve výroku III. tohoto rozhodnutí přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. spočívajícího v porušení povinnosti stanovené v čl. 33 odst. 5 nařízení (EU) 2016/679.

[26] 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. Za porušení základních zásad pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9 nařízení (EU) 2016/679 lze podle čl. 83 odst. 5 nařízení (EU) 2016/679 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.

[27] 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.

[28] Podle čl. 83 odst. 3 nařízení (EU) 2016/679 platí, že pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací zpracování poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení.

[29] 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. Vzhledem k tomu, že podle čl. 83 odst. 5 nařízení (EU) 2016/679 je pro přestupek uvedený ve výroku I. stanovena vyšší horní sazba pokuty než pro přestupky uvedené ve výrocích II. a III., určil Úřad tento přestupek jako nejzávažnější.

[30] 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.

[31] 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 2021 čistý obrat ve výši 88.425.000 Kč. Vzhledem k tomu, že vyšší je hodnota 20.000.000 EUR, vzal Úřad tuto částku jako výchozí při stanovení výše pokuty.

[32] 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 středně závažný.

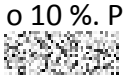
[33] Podle Pokynů se tak základ pro výpočet pokuty bude pohybovat mezi 10 až 20 % platné maximální zákonné sazby, tedy podle čl. 83 odst. 5 nařízení (EU) 2016/679 uvedené procento z 20.000.000 EUR. Z důvodu nižší střední závažnosti Úřad stanovil základ pro výpočet pokuty při dolní hranici sazby, konkrétně ve výši 2.000.000 EUR, což je přibližně dle kurzovního lístku České národní banky ke dni 10. května 2023 (23,415 Kč za 1 EUR) 46.830.000 Kč, která představuje 10 % z maximální výše pokuty podle čl. 83 odst. 5 nařízení (EU) 2016/679. Tuto částku lze dále snížit podle toho, jaký má obviněná čistý roční obrat. Dle obchodního rejstříku měla obviněná v roce 2021 čistý obrat ve výši [redacted], jedná se tedy dle Pokynů o společnost druhé kategorie, u které je možné snížení základu pro výpočet pokuty od 2 % až na 0,4 %. Vzhledem ke střední závažnosti s přihlédnutím k počtu dotčených subjektů údajů Úřad přistoupil ke snížení na [redacted] a určil základ pro výpočet pokuty ve výši [redacted].

[34] 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.

[35] Skutečnost, že podle výroku I. obviněná nepostupovala transparentně vůči velkému množství subjektů údajů  zaměstnanců a  pacientů), hodnotí Úřad jako přitěžující okolnost ve smyslu § 40 zákona č. 250/2016 Sb., což promítl do výše pokuty tak, že částku 234.150 Kč navýšil o 10 %, tedy na 257.565 Kč.

[36] Následně Úřad posoudil význam dalších dvou přestupků uvedených ve výroku II. a III. tohoto rozhodnutí ve vztahu k celkové vytýkané přestupkové činnosti obviněné. Dospěl přitom k závěru, že i jejich závažnost a charakter jsou natolik významné, že jej při stanovení výše pokuty nelze pominout (nejedná se o bagatelní přestupek), ale naopak je třeba, aby se do ní odpovídajícím způsobem promítl.

[37] U přestupku uvedeného ve výroku II. rozhodnutí šlo o jisté opomenutí povinnosti jasně a konkrétně stanovené v právním předpise. Konkrétně obviněná nesplnila ohlašovací povinnost z pozice správce osobních údajů. Považovala za dostatečné, když porušení zabezpečení osobních údajů nahlásila mateřská společnost, ale bez jediné zmínky, že skutečným správcem je obviněná. Je zde nutno doplnit, že svou povinnost dodatečně splnila, i když rozhodně již nemohla dodržet zákonem stanovou lhůtu pro ohlášení. U výroku III. tohoto rozhodnutí obviněná opět nedostála přesného znění nařízením stanovené povinnosti, protože si špatně vyložila pojem „účinky porušení zabezpečení osobních údajů“.

[38] Po vyhodnocení přestupků uvedených ve výrocích II. a III. dospěl Úřad k závěru, že každý z výše uvedených sbíhajících se přestupků s ohledem na svou individuální závažnost i na výše popsanou souvislost s přestupkem uvedeným ve výroku III. je třeba hodnotit jako přitěžující okolnosti ve smyslu § 40 písm. b) zákona č. 250/2016 Sb., které dále zvyšují závažnost přestupku uvedeného ve výroku III. tohoto rozhodnutí, a to každý o 10 %. Proto Úřad k částce  Kč připočetl za každý z výše uvedených přestupků částku  Kč.

[39] S ohledem na výše uvedené vyhodnocení závažnosti přestupků, uložil Úřad obviněné pokutu ve výši částka 309.087 Kč, zaokrouhleno na celé tisíce dolů 309.000 Kč.

[40] 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.

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 10. května 2023

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