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-00414/23-30

ROZHODNUTÍ

Předseda Úřadu pro ochranu osobních údajů jako odvolací orgán příslušný podle § 152 odst. 2 zákona č. 500/2004 Sb., správní řád, rozhodl podle ustanovení § 152 odst. 6 písm. b) zákona č. 500/2004 Sb., správní řád, takto:

Rozklad obviněné, [redacted] proti rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-00414/23-20 ze dne 10. května 2023, **se zamítá a napadené rozhodnutí se potvrzuje.**

Odůvodnění

I. Vymezení věci

/1/ Řízení ve věci podezření ze spáchání přestupků podle § 62 odst. 1 písm. a) a b) zákona č. 110/2019 Sb., o zpracování osobních údajů, vedené 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 24. ledna 2023, které bylo obviněné, [redacted] (dále „obviněná“), doručeno dne 25. ledna 2023, přičemž v průběhu řízení došlo k dílčímu překvalifikování skutku, což bylo obviněné sděleno přípisem čj. UOOU-00414/23-17 ze dne 21. března 2023.

/2/ Podkladem pro zahájení uvedeného řízení o přestupku byl spisový materiál shromážděný v rámci kontroly provedené Úřadem pro ochranu osobních údajů (dále „Úřad“) u obviněné, která byla ukončena vydáním protokolu o kontrole čj. UOOU-01752/21-55 ze dne 8. srpna 2022 a vyřízením námitek předsedou Úřadu přípisem čj. UOOU-01752/21-61 ze dne 30. listopadu 2022. Kontrolou bylo konstatováno, že k porušení zabezpečení osobních údajů nepochybně došlo, jelikož údaje byly pro správce i zpracovatele po dobu cca 1 týdne

nedostupné. Přestože se porušení zabezpečení nepodařilo zabránit, nebylo prokázáno, že by jeho příčinou byla pozdní reakce zpracovatele na kybernetické hrozby. Skutečnost, že došlo k porušení zabezpečení osobních údajů, pak a priori neznamená, že správce porušil své povinnosti podle čl. 32 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 (dále jen „nařízení (EU) 2016/679“). Z druhé strany však je správce povinen plnit i další své povinnosti vyplývající z nařízení (EU) 2016/679, což se týká především plnění ohlašovacích, oznamovacích a dokumentačních povinností (čl. 33 a čl. 34 nařízení (EU) 2016/679).

/3/ Výsledkem uvedeného řízení o přestupku tak bylo vydání rozhodnutí Úřadu čj. UOOU-00414/23-20 ze dne 10. května 2023 (dále „rozhodnutí“). Jím byla obviněná jako správce osobních údajů týkajících se přibližně 58 zaměstnanců a 247 000 pacientů uznána vinnou především tím, že od spáchání kybernetického útoku dne 14. března 2021 do zahájení předmětného řízení o přestupku nedoložila, že by ve smyslu čl. 34 nařízení (EU) 2016/679, jež promítá zásadu transparentnosti podle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, oznámila subjektům údajů porušení zabezpečení osobních údajů následkem kybernetického útoku ze 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, 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 spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.

/4/ Dále byla rozhodnutím obviněná shledána vinnou tím, 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, čímž porušila povinnost stanovenou v čl. 33 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce ohlásit dozorovému úřadu zásadně jakékoli porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, čímž spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

/5/ Obviněná byla rozhodnutím také shledána vinnou tím, že dokumentace zaznamenávající porušení zabezpečení způsobené kybernetickým útokem dne 14. března 2021 se nezabývala účinky předmětného narušení bezpečnosti, což představuje povinný údaj podle 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 spáchala tak přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

/6/ Za spáchání uvedených přestupků byla obviněné rozhodnutím uložena pokuta ve výši 309.000 Kč.

/7/ Proti rozhodnutí, které bylo doručeno dne 10. května 2023, však obviněná podala dne

23. května 2023 včasný a řádný rozklad.

II. Obsah rozkladu

/8/ V rozkladu obviněná uvedla, že nijak nerozporuje, že formálně mohlo dojít k naplnění skutkové podstaty v rozhodnutí uvedených přestupků, nicméně uloženou pokutu považuje vzhledem k okolnostem případu za nepřiměřeně přísnou.

/9/ Na podporu svého požadavku pak obviněná uvádí skutečnosti, ke kterým měl Úřad přihlédnout jako k polehčujícím okolnostem, aniž by je však zohlednil. Těmito polehčujícími okolnostmi měla být snaha obviněné splnit své zákonné povinnosti. Pokud se tak nestalo, bylo to z důvodů formálního pochybení mateřské společnosti  . Dále bylo pominuto, že sama obviněná se stala obětí kybernetického útoku, který jí způsobil značné provozní problémy a byla tak de facto trestána dvakrát, přičemž reálné následky útoku přitom nenastaly, neboť nedošlo k odcizení údajů, ale pouze k jejich znepřístupnění. Dalšími skutečnostmi, které obviněná považuje za polehčující, jsou ty, že subjektům údajů nevznikla žádná újma. O kybernetickém útoku obviněná informovala subjekty údajů prostřednictvím webových stránek a také osobně na recepci prostřednictvím zdravotnických pracovníků, což bylo doloženo čestným prohlášením bývalé jednatelky obviněné. Pokud je obviněné vytýkáno, že v dokumentech nedostatečně popsala účinky porušení zabezpečení osobních údajů, tak tyto účinky fakticky nastaly pouze ve sféře obviněné, nikoliv u subjektů údajů, nelze tedy hovořit o jakékoli újmě subjektů údajů. Obviněná také nahlásila kybernetický útok Národnímu úřadu pro kybernetickou bezpečnost a podala trestní oznámení na Policii České republiky.

/10/ Následně obviněná připomenula § 39 a § 40 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, přičemž považuje za nesprávné použití pouze výslovně neuvedených přitěžujících okolností, když naopak výslovně neuvedené polehčující okolnosti v odůvodnění výše sankce absentují, přestože se v daném případě vyskytovaly.

/11/ Obviněná dále rozporuje i to, že ačkoli došlo k nezaviněnému porušení jednočinným souběhem, a to navíc omylem, Úřad přihlédl jako k přitěžující okolnosti k tomu, že obviněná spáchala více přestupků. Též by Úřad neměl hodnotit jako přitěžující okolnost to, že si obviněná špatně vyložila pojem „účinky porušení zabezpečení osobních údajů“.

/12/ Z výše uvedených důvodů obviněná navrhuje, aby byl výrok IV. rozhodnutí změněn tak, že uložená pokuta bude snížena na 5.000 Kč, příp. bude uvedený výrok zrušen a věc vrácena k opětovnému projednání správnímu orgánu prvního stupně.

III. Posouzení odvolacím orgánem

/13/ Odvolací orgán na základě podaného rozkladu přezkoumal napadené rozhodnutí v celém rozsahu, včetně procesu, který předcházel jeho vydání, a v této souvislosti se zabýval i argumentací obviněné.

/14/ Odvolací orgán předně uvádí, že, jak zvláště shledal a jak ostatně připouští i sama obviněná, vytýkané skutky mají charakter přestupků. Zejména konstatoval, že není

aplikovatelná žádná z výjimek uvedených v čl. 34 odst. 3 nařízení (EU) 2016/679, která zprošťuje správce (tedy obviněnou) povinnosti oznámit případ porušení zabezpečení osobních údajů subjektům údajů. K tomu je třeba připomenout, že není zřejmé, že by v době incidentu byla zavedena opatření, která by dotčené osobní údaje činila pro útočníka nesrozumitelnými (výjimka z ohlašovací povinnosti podle v čl. 34 odst. 3 písm. a) nařízení (EU) 2016/679), přičemž obviněná nad zpracovávanými osobními údaji ztratila po dobu jednoho týdne kontrolu. Zároveň nelze spolehlivě vyloučit další negativní následky pro subjekty údajů v budoucnosti, což znemožňuje přiznat výjimku z ohlašovací povinnosti podle čl. 34 odst. 3 písm. b) nařízení (EU) 2016/679. Stejně tak podle názoru odvolacího orgánu nelze akceptovat výjimku spočívající v nezbytnosti vynaložení nepřiměřeného úsilí, přičemž nelze spolehlivě doložit ani podání informace veřejným oznámením anebo jiným podobným opatřením (podrobněji vizte též komunikaci obviněné se stěžovatelem sub čj. UOOU-01752/21-1 a bod 18 níže), což vylučuje akceptaci výjimky ve smyslu čl. 34 odst. 3 písm. c) nařízení (EU) 2016/679. Spáchání přestupků spočívajících v neohlášení incidentu Úřadu (jelikož byl incident ohlášen ve vztahu ke společnosti [redacted] a nedostatcích ve vedení předepsané dokumentace, v níž absentoval popis účinků předmětného incidentu, pak je očividné. V této souvislosti je možno připomenout, že ke stejným závěrům ohledně plnění předmětných povinností došel Evropský sbor pro ochranu osobních údajů v rámci rozboru obdobného případu č. 03 popsaného sub 2.3. Pokynů 01/2021 „Příklady ohlašování případů porušení zabezpečení osobních údajů“.

/15/ Napadené rozhodnutí ohledně výměry pokuty reflektuje dokument Evropského sboru pro ochranu osobních údajů „Pokyny č. 04/2022 pro výpočet správních pokut podle obecného nařízení o ochraně osobních údajů“, ve finálním znění přijatý dne 24. května 2023 (dále „Pokyny"). Pokyny (vizte čl. 4.2.1 až 4.2.3.) jako kritéria pro určení závažnosti protiprávního jednání, a tedy i určení východiska pro vyměření sankce, stanovují povahu protiprávního jednání, jeho závažnost vymezenou ve vztahu k povaze, rozsahu a účelu zpracování, počtu dotčených subjektů údajů, výši utrpěné škody a doby trvání protiprávního jednání, přičemž tato kritéria musí být posouzena souhrnně (ve vzájemném propojení) ve vztahu ke konkrétním okolnostem případu. V této souvislosti je nutno uvést, že obviněná byla sankcionována za porušení čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 (jmenovitě zásady transparentnosti), což by odpovídalo závažnější kategorii porušení podle čl. 85 odst. 5 nařízení (EU) 2016/679, nicméně podstatou skutku je primárně porušení čl. 34 nařízení (EU) 2016/679 zásadu transparentnosti reflektující, což závažnost skutku zásadně snižuje. Nutno podotknout, že obviněná se dopustila i dalších přestupků spočívajících v porušení čl. 33 nařízení (EU) 2016/679, tyto jsou však charakteru nižší závažnosti ve smyslu čl. 85 odst. 4 nařízení (EU) 2016/679, k čemuž bylo v souladu s body 14, 29, 31 a 36 Pokynů a ustanovením § 40 písm. b) zákona č. 250/2016 Sb. přihlédnuto při stanovení výše pokuty (vizte bod 38 odůvodnění rozhodnutí). Skutek byl spáchán právnickou osobou, která nese objektivní odpovědnost, přičemž však nelze a priori detekovat úmysl osob jednajících jménem obviněné porušit předmětné povinnosti vyplývající z nařízení (EU) 2016/679 a tuto stránku věci tedy lze hodnotit spíše ve prospěch snížení závažnosti skutku. Dále je nutno přihlédnout ke značnému rozsahu zpracovávaných osobních údajů, které nadto měly charakter zvláštní kategorie a týkaly se vesměs pacientů, tedy osob ve výrazně slabším postavení vůči obviněné, což naopak závažnost skutku zvyšuje. Opačný význam, tedy jako snižující závažnost protiprávního jednání,

pak je vhodné zohlednit skutečnost, že pouze jeden stěžovatel pociťoval zvýšenou míru poškození svých práv vyplývajících z čl. 34 nařízení (EU) 2016/679, a také to, že zpracování osobních údajů není hlavní činností obviněné. Na základě tohoto hodnocení je možno souhlasit s posouzením skutku v souvislosti se stanovením východiska pro výměru sankce (vizte bod 60. Pokynů) provedeného správním orgánem prvního stupně jako středně závažného porušení.

/16/ Odvolací orgán pak shledal, že správní orgán prvního stupně uloženou pokutu vyměřil v souladu s Pokyny, přičemž nemá likvidační charakter a pohybuje se při dolní hranici možné sazby, jejíž horní hranice činí až 20 milionů EUR. Vzhledem k tomu, že obviněná je v postavení správce, a je postihována za jednání, které je jí přičítáno, považuje odvolací orgán za správné, že při výměře pokuty nebylo přihlíženo k obratu celé mateřské společnosti (vizte bod 120 Pokynů), do níž je obviněná začleněna.

/17/ Exkurs obviněné ohledně § 39 a § 40 zákona č. 250/2016 Sb. odvolací orgán považuje částečně za účelový, přičemž, jak je třeba zvláště konstatovat, tato dvě ustanovení nijak nelimitují možnosti použití jednotlivých vyjmenovaných či naopak výslovně nevyjmenovaných polehčujících či přitěžujících okolností. Zároveň však odvolací orgán připomíná, že při ukládání pokut týkajících se porušení nařízení (EU) 2016/679 je třeba primárně vzít v úvahu okolnosti uvedené v čl. 83 nařízení (EU) 2016/679, k jehož uplatnění byly přijaty výše připomenuté a aplikované Pokyny. Ohledně argumentace týkající se jednočinného souběhu odvolací orgán uvádí, že v daném případě šlo jednoznačně o vícečinný souběh přestupků, protože přestupky nebyly spáchány jedním skutkem, ale každý samostatným a odlišitelným skutkem, navíc i v různou dobu. Dále je třeba zdůraznit, že při stanovení výše pokuty správní orgán prvního stupně vycházel ze zásady, kdy pro výchozí částku pro výpočet pokuty určil nejvážnější přestupek (jím byl přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb. uvedený ve výroku I. rozhodnutí) ze všech spáchaných přestupků (vizte § 41 odst. 1 zákona č. 250/2016 Sb.) a zbylé přestupky hodnotil pouze jako přitěžující okolnosti k onomu jednomu nejzávažnějšímu. Současně je vhodné opětovně uvést, že obviněná nijak nezpochybnila v rozhodnutí popsaná porušení povinností, resp. spáchání přestupků uvedených ve výrocích I., II. a III. rozhodnutí.

/18/ Odvolací orgán také konstatuje, že obviněná není sankcionována za nedostatečné zabezpečení osobních údajů ve smyslu čl. 32 nařízení (EU) 2016/679, a tudíž obviněnou připomínané skutečnosti, podle nichž se sama stala obětí kybernetického útoku anebo že subjekty údajů neutrpěly žádnou újmu, jsou v těchto souvislostech irelevantní. Jak je také nutno připomenout, i znepřístupnění zpracovávaných osobních údajů představuje určitý negativní následek kybernetického útoku. Mělo-li pak dojít ke spáchání přestupků z důvodů formálního pochybení jiných osob, může obviněná vůči těmto subjektům uplatnit své nároky, z hlediska tohoto řízení se však opět jedná o irelevantní záležitost, která nemá žádný vliv na výsledek, jímž je neposkytnutí povinné zprávy, a tedy i spáchání příslušného přestupku. Stejně tak obviněná, jak se ostatně uvádí v odůvodnění rozhodnutí, dostatečně nedoložila podání informace o incidentu prostřednictvím webových stránek nebo ústní formou. Je totiž zjevné, že obviněná nedokázala doložit přesné znění textu údajně zveřejněného na webových stránkách, nadto se liší od informace podané klientovi obviněné dne 1. dubna 2021, a deklarovaná oznámení by rovněž nesplňovala náležitosti čl. 34 nařízení (EU) 2016/679;

podání ústní informace prostřednictvím zdravotnických pracovníků pak je zjevně nedostatečné z hlediska okruhu takto informovaných osob, přičemž není ani doložen obsah takto podané informace.

/19/ Argumentaci obviněné tedy odvolací orgán odmítl a po celkovém přezkoumání neshledal v postupu správního orgánu prvního stupně Úřadu žádná pochybení způsobující nezákonnost rozhodnutí.

/20/ Ze všech výše uvedených důvodů proto odvolací orgán rozhodl tak, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení: Proti tomuto rozhodnutí podle ustanovení § 152 odst. 5 zákona č. 500/2004 Sb., správní řád, nelze podat rozklad.

Praha 7. srpna 2023

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)