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

Čj. UOOU-04015/23-19

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, společnosti [redacted] proti rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04015/23-13 ze dne 15. prosince 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) zákona č. 110/2019 Sb., o zpracování osobních údajů, vedené v souvislosti s kybernetickým útokem na servery, na nichž byly uloženy osobní údaje zaměstnanců a pacientů obviněné, společnosti [redacted] (dále „obviněná"), bylo zahájeno oznámením o zahájení řízení o přestupku čj. UOOU-04015/23-7 ze dne 5. října 2023, které bylo obviněné doručeno dne 6. října 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 společnosti [redacted], 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, a dále i spisový materiál sp. zn. UOOU-00414/23 shromážděný v rámci navazujícího řízení o přestupku vedeného se společností [redacted]. Uvedená kontrola i řízení o přestupku se týkaly zejména plnění povinností stanovených čl. 28, čl. 33 a čl. 34 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 „nařízení (EU) 2016/679“) v návaznosti na porušení zabezpečení osobních údajů v důsledku kybernetického útoku [redacted]. Jak je třeba připomenout, [redacted]. i obviněná jsou dceřinými společnostmi mateřské společnosti [redacted], přičemž jak společnost [redacted], tak i obviněná zpracovávaly osobní údaje s využitím serverů zpracovatele, společnosti [redacted], které byly postiženy týmž kybernetickým útokem [redacted]. Většinu závěrů kontroly vedené sub sp. zn. UOOU-01752/21 i řízení o přestupku vedené sub sp. zn. UOOU-00414/23 tudíž lze obdobně vztáhnout i vůči obviněné.

/3/ Ze závěrů kontroly vedené sub sp. zn. UOOU-01752/21 vyplývá, 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 (EU) 2016/679. Z druhé strany však je správce povinen plnit své další povinnosti vyplývající z nařízení (EU) 2016/679, což se týká především plnění nově vyvstalých ohlašovacích, oznamovacích a dokumentačních povinností podle čl. 33 a čl. 34 nařízení (EU) 2016/679.

/4/ Výsledkem předmětného řízení o přestupku vedeného s obviněnou pak bylo vydání rozhodnutí čj. UOOU-04015/23-13 ze dne 15. prosince 2023 (dále „rozhodnutí“). Výrokem I. rozhodnutí byla obviněná jako správce osobních údajů týkajících se [redacted] pacientů a [redacted] zaměstnanců shledána vinnou tím, že bez zbytečného odkladu po spáchání kybernetického útoku [redacted]. [redacted] cíleného na servery společnosti [redacted], na kterých měla obviněná uložené databáze s osobními údaji uvedených 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. Tím obviněná spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb., za což jí byla výrokem II. rozhodnutí uložena pokuta ve výši 26.000 Kč. a výrokem III. rozhodnutí jí byla uložena povinnost úhrady nákladů řízení.

/5/ Naproti tomu bylo výrokem IV. rozhodnutí řízení s obviněnou, které se týkalo spáchání přestupku podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. tím, že obviněná bez zbytečného odkladu neoznámila porušení zabezpečení osobních údajů subjektům údajů poté, co došlo [redacted] ke kybernetickému útoku na servery společnosti [redacted], v rozsahu posledně uvedeného skutku zastaveno, neboť bylo shledáno, že se tento skutek, jímž by byla porušena povinnost stanovená čl. 34 odst. 1 nařízení (EU) 2016/679 a o němž také bylo vedeno řízení, nestal. Obviněná totiž, jak bylo doloženo, učinila oznámení o 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 [redacted] na obvyklých místech u obviněné tak, aby se informace co nejvíce rozšířila.

/6/ Proti rozhodnutí, které bylo doručeno dne 20. prosince 2023, však obviněná podala dne 4. ledna 2024 včasný a řádný rozklad.

II. Obsah rozkladu

/7/ V rozkladu obviněná především popřela spáchání přestupku uvedeného ve výroku I. rozhodnutí, a proto navrhla, aby byly výroky I. až III. rozhodnutí změněny tak, že se řízení o přestupku popsaného ve výroku I. rozhodnutí v rozsahu tohoto skutku zastavuje.

/8/ Na podporu svého požadavku obviněná v podaném rozkladu prvně namítla, že právní věta výroku I. rozhodnutí není v rozhodnutí citována správně, neboť v ní zcela chybí podstatná část rozhraničující skutkový stav, který se odehrál (a který není porušením práva, není deliktem), od deliktu (viz úplné znění rozhodného právního předpisu).

/9/ K tomu obviněná uvedla, že data jsou uložena na externím úložišti, jehož provozovatelem je profesionální subjekt, který se stará o zabezpečení dat před kybernetickými útoky a data jsou, resp. v době kybernetického útoku byla, zašifrována, aby ani v případě, že se podaří útočníkům překonat zabezpečení, tito nezjistili skutečný obsah dat. S ohledem na šifrování znepřístupněných osobních údajů i s ohledem na znění čl. 33 odst. 1 nařízení (EU) 2016/679, podle něhož se dozorovému úřadu ohlašuje pouze takové porušení zabezpečení osobních údajů, u kterého je pravděpodobné, že mělo za následek riziko pro práva a svobody fyzických osob, se tudíž podle obviněné přestupek nestal.

/10/ Jelikož byla data pro kohokoli bez oprávnění přístupu k nim nesrozumitelná, nedošlo podle obviněné ani k žádné újmě ani pacientů, ani zaměstnanců a nebyly tedy splněny podmínky pro vznik ohlašovací povinnosti, a tudíž ani nemohl být spáchán předmětný přestupek. Na tuto skutečnost pak podle rozkladu obviněná v průběhu řízení upozorňovala, Úřad se ale touto námitkou nezabýval. Obviněná proto má zato, že rozhodnutí je nepřezkoumatelné a je založeno na nesprávném právním posouzení spočívajícím v neúplné a nesprávné aplikaci rozhodné právní normy. K tomu ještě obviněná doplnila, že, vzhledem k šifrování dat a jejich nesrozumitelnosti pro osoby bez oprávnění k přístupu, obdobné platí i pro případ oznamovací povinnosti vůči dotčeným subjektům údajů, tedy že tato povinnost odpadá s ohledem na výjimku z této povinnosti zavedenou ustanovením čl. 34 odst. 3 písm. a) nařízení (EU) 2016/679.

III. Posouzení odvolacím orgánem

/11/ Odvolací orgán na základě podaného rozkladu přezkoumal napadené rozhodnutí v celém rozsahu, včetně procesu, který předcházel jeho vydání, a nejprve se zabýval argumentací obviněné.

/12/ Odvolací orgán předně uvádí, že v důsledku předmětného kybernetického útoku nepochybně došlo k znepřístupnění a zašifrování příslušných osobních údajů, což zjevně znemožnilo či zkomplikovalo aktivity obviněné, zejména ve vztahu k pacientům, kteří měli být léčeni v době, kdy byla data nedostupná, přičemž ve vztahu k pacientům byly kybernetickým útokem postiženy i osobní údaje o zdravotním stavu, tedy zvláštní kategorie osobních údajů vyžadující vyšší úroveň ochrany. Nadto po dobu znepřístupnění obviněná nemohla spolehlivě zjistit, zda toto šifrování nebylo prolomeno. Traktované porušení zabezpečení osobních údajů tedy zjevně vyvolalo rizika pro práva a svobody dotčených subjektů údajů. Z tohoto důvodu se výjimka z ohlašovací povinnosti uvedená v čl. 33 odst.1 nařízení (EU) 2016/679 jeví jako neaplikovatelná, což ostatně koresponduje i s názorem Evropského sboru pro ochranu

osobních údajů vysloveným v rámci rozboru obdobného případu (vizte případ č. 03 popsaný sub 2.3. Pokynů 01/2021 „Příklady ohlašování případů porušení zabezpečení osobních údajů“), a tudíž nebyla uvedena v rámci výroku I. rozhodnutí.

/13/ Odvolací orgán nad rámec výše uvedeného dále připomíná, že obviněná sice opravdu v průběhu řízení v obecné rovině, tedy bez jakéhokoli doložení, uvedla, že osobní údaje napadené předmětným kybernetickým útokem byly šifrovány, nicméně zároveň se odvolávala na skutečnost, že ohlašovací povinnost vůči Úřadu byla splněna prostřednictvím mateřské společnosti [redacted]. Z tohoto ohlášení ze dne 16. března 2021 (dokument „Ohlášení porušení zabezpečení osobních údajů dle GDPR“) ovšem nijak nevyplynulo, že se mělo týkat obviněné, příp. dalších správců, a nebylo to možné odvodit ani ze skutečnosti, že ohlášení provedla mateřská společnost. Navíc, jak je také nutno připomenout, výše uvedený dokument „Ohlášení porušení zabezpečení osobních údajů dle GDPR“ neobsahuje žádnou relevantní zmínku o šifrování napadených dat ze strany správce nebo zpracovatele (na rozdíl od zašifrování dat ze strany hackera). V bodu 10.4. předmětného dokumentu „Ohlášení porušení zabezpečení osobních údajů dle GDPR“ je sice zmíněno „HW šifrování disků na diskovém poli“, nicméně takovéto šifrování chrání data před neoprávněným přístupem k nim pouze pro případ fyzického odcizení disku nebo vyjmutí disku z diskového pole. Pro posuzovaný případ kompromitace serverů společnosti zpracovatele, společnosti [redacted], útočníkem prostřednictvím zneužití zranitelnosti software [redacted] na serveru s tímto SW, následného *„prolomení přístupu do monitorovacího serveru, který měl legitimní přístup k ostatním serverům“,* navazující instalace ransomware na další servery a *„spuštění útoku vedoucího k zašifrování dat na řadě serverů včetně záloh“* (srov. bod 5 „Ohlášení porušení zabezpečení osobních údajů dle GDPR“), je takové šifrování bez významu pro zabránění přístupu k údajům uloženým na napadených serverech/discích. Jak vyplývá i z citovaného, po prolomení přístupu do monitorovacího serveru byl útočník schopen přistoupit k souborům na dalších severech a tyto zašifrovat. Předmětné HW šifrování disků na diskovém poli tak soubory na dalších serverech nijak neochránilo. HW šifrování disků na diskovém poli nemá žádný vliv na přístup k datům z již spuštěného operačního systému, pro který se data jeví jako nešifrovaná a jako k nešifrovaným k nim tedy má přístup i útočník, získá-li přístup do operačního systému. Odkaz na šifrování napadených dat ze strany obviněné, resp. zpracovatele, tedy odvolací orgán shledal jako ryze účelový.

/14/ Ohledně oznamovací povinnosti případů porušení zabezpečení osobních údajů subjektům údajů odvolací orgán připomíná, jak je nutno vyvozovat z dikce čl. 34 odst. 3 písm. a) nařízení (EU) 2016/679, že šifrování je pouze jedno z možných příkladmých opatření poskytujících liberaci z plnění předmětné povinnosti, které ovšem z logiky věci koresponduje se situací, v níž by došlo k úniku osobních údajů. Pro traktovaný případ, v němž došlo ke znepřístupnění osobních údajů, však je toto opatření zcela irelevantní, přičemž relevantním opatřením by bylo např. okamžité nasazení záložní databáze (která ovšem byla útočníkem rovněž zašifrována). Právě takovéto znepřístupnění zjevně představovalo vysoký stupeň rizika ve vztahu k subjektům údajů (zejména k pacientům). Obviněná tedy byla povinna podle čl. 34 nařízení (EU) 2016/679 traktovaný případ porušení zabezpečení subjektům údajů oznámit a této povinnosti i dostála (vizte výrok IV. rozhodnutí).

/15/ Argumentaci obviněné tedy odvolací orgán odmítl a po celkovém přezkoumání neshledal v postupu správního orgánu prvního stupně Úřadu žádná pochybení způsobující nezákonnost rozhodnutí.

/16/ 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 19. dubna 2024

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)