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

Čj. UOOU-01752/21-61

Praha 30. listopadu 2022

Vyřízení námitek proti kontrolním zjištěním uvedeným v protokolu o kontrole čj. UOOU-01752/21-55 ze dne 8. srpna 2022

Úřad pro ochranu osobních údajů (dále jen „Úřad“) jako kontrolní orgán podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), obdržel dne 17. srpna 2022 od [redacted] (dále jen „kontrolovaná osoba“), námitky proti kontrolním zjištěním uvedeným v protokolu o kontrole čj. UOOU-01752/21-55 ze dne 8. srpna 2022 (dále jen „protokol o kontrole“).

V souladu s § 14 odst. 1 kontrolního řádu je příslušný k vyřízení námitek předseda Úřadu.

Podané námitky podle ustanovení § 14 kontrolního řádu vyřizuji takto:

1. **Námitce** směřující proti kontrolnímu zjištění č. 2 protokolu o kontrole, v němž je konstatováno, že došlo k porušení zabezpečení ochrany osobních údajů z důvodu nedostatečného nastavení ochrany osobních údajů zpracovatelem, **se částečně vyhovuje.**

   V této souvislosti kontrolovaná osoba sdělila, že kontrolující předjímá fakt, že server byl kompromitován dne 14. března 2021, tedy v den realizace útoku, a to z toho důvodu, že nebyly instalovány opravné patche (záplaty) na zranitelnosti [redacted] vydané společností [redacted] již dne 2. března 2021, o čemž informoval i Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) dne 3. března 2021. Tyto opravné patche však zpracovatel, [redacted] (dále jen „zpracovatel“ nebo [redacted], podle kontrolované osoby instaloval již dne 5. března 2021 v souladu s interními předpisy v [redacted], tedy nejpozději [redacted]. Kontrolovaná osoba uvedla, že zpracovatel má za to, že nastavené termíny instalací opravných aktualizací jsou mnohem kratší, než je na trhu běžné, přičemž není technicky možné instalovat opravné a bezpečnostní patche ihned. Dále kontrolovaná osoba sdělila, že sám NÚKIB ve svém hlášení uvádí, že ani instalace těchto záplat nevyřeší situaci, pokud již byl server kompromitován, což tou dobou podle kontrolované osoby zjevně byl. Dále kontrolovaná osoba sdělila, že zpracovatel dále prováděl kontrolu komunikace z IP

adres, které NÚKIB uváděl jako potenciálně nebezpečné a vhodné k prověření, přičemž nebylo prokázáno, že by ze zmíněných adres probíhala jakákoli komunikace.

K tomu uvádím, že v protokolu o kontrole je konstatováno, že pokud útočník získal přístup k serveru dne 14. března 2021 díky využití zranitelností [redacted], pak zpracovatel nedostatečně reagoval na kybernetické hrozby, které bylo možné v době útoku velmi pravděpodobně eliminovat včasnou instalací dostupných záplat. V ohlášení porušení zabezpečení osobních údajů doručeném Úřadu dne 16. března 2021 (dále jen „Ohlášení porušení zabezpečení“), které učinila [redacted], je uvedeno, že došlo k hackerskému útoku na servery společnosti [redacted], přičemž je pravděpodobné, že došlo ke zneužití zranitelnosti v software [redacted], přestože servery byly aktualizovány cca 2 dny po vydání příslušné aktualizace. Dále je v Ohlášení porušení zabezpečení uvedeno, že servery [redacted] jsou pravidelně aktualizované (aktualizace v režimu [redacted], tedy den vydání aktualizace plus [redacted] na otestování vydané aktualizace a naplánování její aplikace).

Dne 3. března 2021 zveřejnil NÚKIB na svých internetových stránkách upozornění na zranitelnosti [redacted], v němž je uvedeno, že tyto zranitelnosti opravují aktualizace vydané společností [redacted] dne 2. března 2021 a že nainstalování aktualizace nevyřeší situaci, kdy už je server kompromitován. Následně dne 8. března 2021 NÚKIB zveřejnil seznam indikátorů a postupů k prověření kompromitace (např. IP adresy k prověření). Současně upozornil, že seznam indikátorů není konečný ani určující.

V protokolu o kontrole je konstatováno, že společnost [redacted] *nebyla schopna doložit dostatečnost bezpečnostních opatření před útokem, neboť v rámci reakce na útok došlo k reinstalaci části systémů, včetně výměny použitých technologií*“. Tvrzení, zda zpracovatel instaloval aktualizaci [redacted] již dne 5. března 2021, tak nelze ověřit. Nicméně [redacted] informaci o aktualizaci [redacted] Úřadu oznámila již v Ohlášení porušení zabezpečení dne 16. března 2021 a v průběhu kontroly nebyly zjištěny skutečnosti, které by tuto informaci zpochybňovaly.

Podle informací NÚKIB mohly být zranitelnosti zneužívány útočníky již od ledna 2021. K ohrožení zabezpečení osobních údajů (jejich zašifrování) došlo v případě kontrolované osoby dne 14. března 2021. Kdy přesně k pravděpodobnému zneužití zranitelnosti [redacted] došlo, se však nepodařilo zjistit. K neoprávněnému přístupu na servery kontrolované osoby, resp. jejího zpracovatele tak mohlo dojít dříve, a i kdyby zpracovatel provedl aktualizaci [redacted] okamžitě (po vydání aktualizace dne 2. března 2021), mohl již být server kompromitován a ani včasná aktualizace by na této situaci nic nezměnila. Kontrolovaná osoba v rámci podaných námitek uvedla, že zpracovatel provedl kontrolu komunikace z IP adres, které NÚKIB uvedl jako potenciálně nebezpečné, přičemž nebylo prokázáno, že by z těchto adres komunikace probíhala. Z protokolu o kontrole ani z vyjádření zpracovatele není zřejmé, zda [redacted] uvedenou kontrolu IP adres prováděla na základě doporučení NÚKIB ještě před 14. březnem 2021, nebo až poté. V rámci kontroly předložila pouze analýzu síťového provozu (za období od 1. února

[1] [redacted]

2021 do 12. března 2021) datovanou k 17. březnu 2021, ze které vyplývá, že žádné podezřelé chování na serveru nebylo odhaleno. Ani dřívější analýza by tak zřejmě nevedla k odhalení kompromitace serveru. Ačkoli kontrolovaná osoba, resp. její zpracovatel považuje za příčinu útoku na servery využití zranitelnosti [redacted], ze sdělení NÚKIB ze dne 9. prosince 2021 vyplývá, že samotná příčina útoku není známa.

Je nepochybné, že k porušení zabezpečení osobních údajů došlo, jelikož údaje byly pro správce i zpracovatele po dobu cca 1 týdne nedostupné. Kontrolovaná osoba uvedla, že včas provedla aktualizaci. Přestože se jí porušení zabezpečení nepodařilo zabránit, nebylo prokázáno, že jeho příčinou byla pozdní reakce zpracovatele na kybernetické hrozby, proto se v této části námitce vyhovuje. Současně podotýkám, že skutečnost, že došlo k porušení zabezpečení osobních údajů 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“).

S ohledem na výše uvedené konkrétní okolnosti posuzovaného případu se námitce kontrolované osoby částečně vyhovuje. Přesto je třeba připomenout, že i v případě kybernetického útoku je správce povinen plnit povinnosti vyplývající z nařízení (EU) 2016/679 a jejich plnění v souladu s čl. 5 odst. 2 uvedeného nařízení doložit.

2. **Námitka** směřující proti kontrolnímu zjištění č. 3.1 protokolu o kontrole, v němž je konstatováno, že kontrolovaná osoba porušila ustanovení čl. 33 odst. 1 nařízení (EU) 2016/679 tím, že bez zbytečného odkladu, a pokud možno do 72 hodin od okamžiku, kdy se dozvěděla o porušení zabezpečení osobních údajů, neohlásila toto porušení Úřadu, **se zamítá.**

K tomu kontrolovaná osoba uvedla, že jmenovala jako pověřence pro ochranu osobních údajů svoji [redacted] Ohlášení porušení zabezpečení bylo řešeno ve spolupráci se [redacted], přičemž kontrolovaná osoba má za to, že ohlášení porušení zabezpečení osobních údajů učinila prostřednictvím svého pověřence – [redacted]

K tomu uvádím, že Ohlášení porušení zabezpečení učinila [redacted]. (dne 16. března 2021). Jako pověřenec pro ochranu osobních údajů je v předmětném ohlášení uvedena [redacted] Kontrolovaná osoba v průběhu kontroly předložila dokument *Jmenování pověřence pro ochranu osobních údajů* z 25. května 2018 (čj. UOOU-01752/21-22, příloha č. 1), ve kterém je uvedeno, že pověřencem pro ochranu osobních údajů byla jmenována [redacted] Jmenování tohoto pověřence kontrolovaná osoba oznámila podle čl. 37 odst. 7 nařízení (EU) 2016/679 Úřadu dne 15. ledna 2019 (čj. UOOU-0006/19-172).

Podle čl. 33 odst. 1 nařízení (EU) 2016/679 oznámí správce dozorovému úřadu do 72 hodin jakékoli porušení zabezpečení osobních údajů, přičemž není vyloučeno, aby toto oznámení učinil prostřednictvím svého pověřence. Z oznámení však musí být patrné, kdo je správcem osobních údajů, jichž se ohlašované porušení zabezpečení týká. Z Ohlášení porušení zabezpečení učiněného [redacted] nijak nevyplývá, že by se porušení

zabezpečení osobních údajů (ke kterému došlo 14. března 2021) mělo týkat i kontrolované osoby či jiných správců. Pouze ze skutečnosti, že [redacted], nelze dovozovat, že se porušení zabezpečení osobních údajů týkalo i dceřiné společnosti (kontrolované osoby). Stejně tak v případě, že má více správců stejného pověřence pro ochranu osobních údajů, je nezbytné uvést, jménem kterých správců je porušení zabezpečení osobních údajů ohlašováno. Na základě výše uvedeného konstatuji, že kontrolovaná osoba ohlásila porušení zabezpečení osobních údajů až dne 23. listopadu 2021, tedy po zahájení kontroly.

3. **Kontrolovaná osoba** ve svých námitkách uvedla, že podává námitky proti kontrolnímu zjištění č. 3 – Porušení zabezpečení osobních údajů. Uvedené kontrolní zjištění je dále rozděleno na tři části: 3.1 Ohlášení porušení zabezpečení správci a Úřadu, 3.2 Oznámení porušení zabezpečení subjektům údajů a 3.3 Dokumentace všech případů porušení zabezpečení osobních údajů. Formálně kontrolovaná osoba napadá kontrolní zjištění č. 3 jako celek, fakticky se však vyjadřuje pouze ke kontrolnímu zjištění č. 3.1. **Námitky** proti kontrolním zjištěním č. 3.2 a 3.3 uvedeným v protokolu o kontrole nebyly odůvodněny (námitky obsahují pouze blíže neodůvodněné opakované tvrzení kontrolované osoby související s kontrolním zjištěním č. 3.2 protokolu o kontrole, že pacienti polikliniky byli o incidentu informováni prostřednictvím webu hned po útoku a dále ústně při návštěvě polikliniky), proto **se** v souladu s § 14 odst. 2 kontrolního řádu **zamítají jako nedůvodné.**

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)