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-01752/21-55
Praha 8. srpna 2022

Protokol o kontrole

Kontrolní orgán:
Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) 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“) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon č. 110/2019 Sb.“).

Kontrolující:
Mgr. Eva Cupáková – pověřená zaměstnankyně Úřadu, jako vedoucí kontrolní skupiny, na základě pověření ke kontrole z 11. listopadu 2021;

Mgr. Karolína Straková – pověřená zaměstnankyně Úřadu, na základě pověření ke kontrole z 11. listopadu 2021, účast na kontrole do 15. března 2022;

Bc. Linda Tamchynová – pověřená zaměstnankyně Úřadu, na základě pověření ke kontrole z 11. listopadu 2021, účast na kontrole do 31. prosince 2021;

Mgr. Marek Šnajdr – pověřený zaměstnanec Úřadu, na základě pověření ke kontrole z 11. listopadu 2021;

Bc. Jaromír Kuba – přizvaná osoba, na základě pověření ke kontrole z 11. listopadu 2021.

Kontrolovaná osoba:
[redacted]
(dále jen „kontrolovaná osoba“)

Osoba povinná:
[redacted]
(dále jen „osoba povinná“ nebo i [redacted].

Předmět kontroly:
Předmětem kontroly bylo dodržování povinností stanovených nařízením (EU) 2016/679 při zpracování osobních údajů, zejména pak čl. 28, čl. 33 a čl. 34 nařízení (EU) 2016/679 v souvislosti s ohlášením porušení zabezpečení osobních údajů Úřadu ze 14. března 2021. Předmětem kontroly bylo též prověření role správce a zpracovatele v souladu s čl. 4 odst. 7 a odst. 8 nařízení (EU) 2016/679.

První kontrolní úkon:
Místní šetření a ústní jednání v sídle kontrolované osoby 23. listopadu 2021 v 9:40 hod., z něhož byl pořízen protokol z ústního jednání a místního šetření čj. UOOU-01752/21-16.

Poslední kontrolní úkon:
Rozbor a zpracování zaslaných dokumentů kontrolovanou osobou pod čj. UOOU-01752/21-54 ze 3. srpna 2022.

I. Přehled podkladů

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Stížnost na neposkytnutí informací o bezpečnostním incidentu v síti [redacted] z 1. dubna 2021 (čj. UOOU-01752/21-1), počet listů 4;
   1.1 Vyjádření k žádosti o informace [redacted] počet listů 1;
   1.2 Žádost o poskytnutí informace, počet listů 1;
2. Ohlášení porušení zabezpečení osobních údajů [redacted], z 16. března 2021 (čj. UOOU-01504/21-1), počet listů 5;
   2.1 Záznam o odložení ohlášení ze 4. května 2021 (čj. UOOU-01504/21-2), počet listů 1;
3. Protokol z ústního jednání a místního šetření u kontrolované osoby ze dne 23. listopadu 2021 (čj. UOOU-01752/21-16), počet listů 3;
   3.1 Úřední záznam Policie České republiky, počet listů 6;
   3.2 Ohlášení porušení zabezpečení osobních údajů dle GDPR, počet listů 4;
   3.3 Formulář hlášení kybernetického bezpečnostního incidentu, počte listů 1;
   3.4 Souhlas pacienta, počet listů 1;
   3.5 Informace pro pacienty o zpracování osobních údajů, počet listů 1;
   3.6 Poučení o povinné mlčenlivosti a ochraně osobních údajů pro zaměstnance poskytovatele zdravotních služeb, počet listů 1;
   3.7 Poučení o povinné mlčenlivosti a ochraně osobních údajů pro zaměstnance poskytovatele zdravotních služeb vzor, počte listů 1;
   3.8 Informace k proškolení zaměstnanců v GDPR, počet listů 2;
   3.9 Seznámení se zásadami ochrany osobních údajů při poskytování zdravotních služeb, počet listů 1;
   3.10 Seznámení se zásadami ochrany osobních údajů při poskytování zdravotních služeb vzor, počet listů 1;
   3.11 Zásady zpracování osobních údajů zaměstnanců, počet listů 1;
   3.12 Záznamy o činnostech zpracování, počet listů 4;

3.13 Zpracování osobních údajů při distančním poskytování zdravotních služeb, počet listů 1;
3.14 Ohlášení porušení zabezpečení osobních údajů, počet listů 1;
3.15 Dokumentace všech případů porušení zabezpečení osobních údajů, počet listů 1;
3.16 Příloha č. 2 ke smlouvě č. ITS 15002, počet listů 1;
3.17 Příloha č. 1 ke smlouvě č. ITS 15002, počet listů 3;
3.18 Smlouva o poskytování cloudových a IT služeb č. ITS 15002, v počtu 5 listů;
3.19 Smlouva o zpracování osobních údajů, počet listů 5;

4. Protokol z ústního jednání a místního šetření u osoby povinné ze dne 23. listopadu 2021 (čj. UOOU-01752/21-17), počet listů 3;
5. Doplnění – přílohy k místnímu šetření (čj. UOOU-01752/21-18), počet listů 3;
   5.1 SZZC_6e21031618220, počet listů 3;
   5.2 Ohlášení_porušení_zabezpečeni dle GDPR_[redacted] počet listů 5;
   5.3 Formular_incident_report_govcert_kopie, počet listů 2;
6. Doplnění – přílohy k místnímu šetření (čj. UOOU-01752/21-19), počet listů 1;
   6.1 Ohlášení porušení zabezpečeni_dle_GDPR_[redacted] počet listů 5;
7. Sdělení – zvuková nahrávka ústní jednání a místní šetření (čj. UOOU-01752/21-21), počet listů 1;
8. Odpověď na žádost o součinnost [redacted]. z 25. listopadu 2021 (čj. UOOU-1752/21-22), počet listů 1;
   8.1 Jmenování pověřence pro ochranu osobních údajů z 25. května 2018, počet listů 1;
9. Úřední záznam, ze dne 30. listopadu 2021 (čj. UOOU-01752/21-23), počet listů 1;
   9.1 [redacted] informace o zpracování osobních úd, počet listů 4;
10. Oznámení pověřence ze dne 15. ledna 2019 (čj. UOOU-00006/19-172), počet listů 1;
11. Úřední záznam, ze dne 3. prosince 2021, (čj. UOOU-1752/21-26), počet listů 7;
12. Smlouva o poskytování služeb pověřence pro ochranu osobních údajů z 25. května 2018 (UOOU-01752/21-28), počet listů 2;
    12.1 Průvodní text – odpověď na součinnost, počet listů 1;
13. Sdělení k žádosti o součinnost ze 7. prosince 2021 (UOOU-01752/21-30, počet listů 1;
14. Odpověď na žádost o součinnost I (UOOU-1752/21-31) ze dne 7. prosince 2021, z toho:
    14.1 _smernice_kveten_2020, počet listů 9;
    14.2 GDPR_smernice_kveten_2021, počet listů 9;
    14.3 GDPR_smernice_listopad_2021, počet listů 8;
    14.4 GDPR_smernice_srpen_2019, počet listů 9;
    14.5 GDPR_smernice_zari_2020, počet listů 9;
    14.6 [redacted], počet listů 1;
    14.7 9_1_20200130_[redacted]analyza_II (Zpráva k analýze zpracování osobních údajů k GDPR z pohledu IT systému a souvisejících procesů), počet listů 8;
    14.8 8_1_Dokumentace_oprávnění_SHP, počet listů 3;
    14.9 7_1_[redacted] vyjádření (Oznámení narušení bezpečnosti prostředí společnosti), počet listů 1;
    14.10 5_5_2018_05_23_Smlouva_o_zpracování-osobních_údajů (mezi [redacted]. a [redacted], počet listů 3;
    14.11 5_4_2015_04_24_Příloha_č_3_ke_sml_č_ITS_15005_Ceník_služeb, počet listů 1;

14.12 5_3_2015_04_24_Příloha_č_2_ke_sml_č_ITS_15005_Pravidla_dostupnosti_služeb_SLA_, počet listů 1
14.13 5_2_2015_04_24_Příloha_č_1_ke_sml_č_ITS_15005_Specifikace_Služeb, počet listů 3;
14.14 5_1_2015_04_24_Smlouva_o_poskytování_Cloudových_a_IT_služeb_č_ITS_15005, počet listů 5;
14.15 4_1_Sandbox_analýza_vzorku, počet listů 1;
14.16 11_7_Úroveň zabezpečení_před_a_po, počet listů 2;
14.17 2018-05_23_Smlouva_o_zpracoávní_osobních_údajů (mezi [redacted]. a [redacted], počet listů 3;
14.18 2015_04-24_Smlouva__poskytování_Cloudových_a_IT_služeb_č_ITS_15002 (mezi [redacted] a [redacted], počet listů 5;
14.19 12_1_RESTORE_FILES_INFO, počet listů 1;
14.20 2015_04_24_Příloha_č_3_ke_sml_ITS_15002_Ceník_službe, počet listů 1;
14.21 2015_04_24_Příloha_č_2_ke_sml_ITS_15002_Pravidla _dostupnosti_služeb-SLA, počet listů 1;

15. Odpověď na žádost o součinnost II (UOOU-01752/21-32) ze dne 7. prosince 2021, z toho:
15.1 2015_04_24_Příloha_č_1_e_sml_č_ITS_15002_Specifik, počet listů 3;
15.2 11_7_Úroveň_zabezpečení_před_a_po, počet listů 2;
15.3 11_1_Úvodní_analýza_síťového_provozu, počte listů 2;
15.4 01_[redacted]_org_struktura, počet listů 1;
15.5 1_1_Průběh_řešení_incidentu, počet listů 2;
15.6 08_[redacted]_Politika_hesel, počet listů 1;
15.7 07_[redacted]_DatM, počet listů 1;
15.8 06_[redacted]_spisovy_rad, počet listů 7;
15.9 05_[redacted]_Metodika_nastup_vystup, počet listů 3
15.10 03_[redacted]_Smernice_HI, počet listů 4;
15.11 02_[redacted]_Prohlaseni_OU, počet listů 6;
16. Odpověď na žádost o součinnost III (UOOU-1752/21-33) ze dne 7. prosince 2021, počet listů 1;
17. Odpověď na žádost o spolupráci, NÚKIB (UOOU-01752/21-34), ze dne 9. prosince 2021, počet listů 1;
18. Sdělení k dotazu [redacted] (UOOU-01752/21-35), ze dne 10. prosince 2021, počet listů 1;
19. Doplnění informací [redacted] (UOOU-01752/21-37), ze dne 21. prosince 2021, počet listů 2;
19.1 Směrnice GDPR, květen 2020, počet listů 9;
19.2 Směrnice GDPR, květen 2021, počet listů 9;
19.3 Směrnice GDPR, IT komplexně, listopad 2021, počet listů 8;
19.4 Směrnice GDPR, srpen 2019, počet listů 10;
19.5 Směrnice GDPR, září 2020, počet listů 9;
25.6. Smlouva o výkonu pověřence, počet listů 3;
20. Vyjádření [redacted] (UOOU-01752/21-38), ze dne 5. ledna 2022, počet listů 1;
21. Protokol z místního šetření ze 17. března 2022 u zpracovatele [redacted] (UOOU-01752/21-47), počet listů 3;
21.1 Příloha č. 1 ke smlouvě č. IS 15002, počet listů 3;
21.2 Příloha č. 2 ke smlouvě č. IS 15002, počet listů 1;

21.3 Úřední záznam o podaném vysvětlení Policie ČR, počet listů 2;
21.4 PrtScr. obrazovky [redacted], počet listů 1;
21.5 PrtScr. obrazovky [redacted], počet listů 1;
21.6 PrtScr. obrazovky [redacted], počet listů 1;
21.7 PrtScr. obrazovky [redacted], počet listů 1;
21.8 PrtScr. obrazovky [redacted], počet listů 1;
21.9. PrtScr. obrazovky [redacted], počet listů 1;
22. Oznámení o jmenování pověřence (UOOU-01752/21-48, příloha č. 1), počet listů 1;
23. Odpověď na žádost o součinnost [redacted] ze 4. dubna 2022 (UOOU-01752/21-50), počet listů 1;
24. Odpověď na žádost o součinnost [redacted] ze 4. července 2022 (UOOU-01752/21-52), počet listů 1,
24.1. Příloha č. 1 ke smlouvě, počet listů 3,
24.2. Příloha č. 2 ke smlouvě, počet listů 1,
24.3. Smlouva o poskytování cloudových a IT služeb, počet listů 5,
24.4. Smlouva o zpracování osobních údajů, počet listů 3;
25. Odpověď na žádost o součinnost [redacted] ze 3. srpna 2022 (UOOU-01752/21-54), počet listů 1;
25.1. Oznámení o kybernetickém útoku, počet listů 1.

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly a ledaže je níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod zahájení kontroly:

Stížnost z 1. dubna 2021

Dne 1. dubna 2021 (viz bod 1. přehledu podkladů) přijal Úřad stížnost na neposkytnutí informací o bezpečnostním incidentu v síti kontrolované osoby, v souvislosti s porušením zabezpečení osobních údajů. Stěžovatel doložil (bod 1.2 přehledu podkladů), že se 19. března 2021 prostřednictvím své datové schránky [redacted] obrátil na kontrolovanou osobu se žádostí o přístup k osobním údajům dle čl. 15 nařízení (EU) 2016/679 a požadoval informace v souvislosti s kybernetickým útokem. Kontrolovaná osoba stěžovateli odpověděla (bod 1.1 přehledu podkladů), že předmětné napadení směřovalo na kompletní IT infrastrukturu dodavatele IT služeb [redacted] a cílem útoku bylo pouze zašifrování dat s následným vymáháním finanční částky, kdy po provedených úkonech byl útok vyhodnocen jako neúspěšný. V odpovědi je dále uvedeno: „*Případ je dále v intenzivním šetření příslušných správních orgánů a bylo podáno hlášení o incidentu na Úřad pro ochranu osobních údajů k prošetření míry narušení dat zákazníků“.*

Ohlášení porušení zabezpečení

Úřad obdržel 16. března 2021 *Ohlášení porušení zabezpečení osobních údajů* od [redacted] (dále jen [redacted], (bod 2. přehledu podkladů). V ohlášení je uvedeno, že 14. března 2021 ve 03:00 hodiny došlo k porušení zabezpečení osobních údajů správce

osobních údajů [redacted], respektive u jejího zpracovatele, [redacted].
Oznámen byl hackerský útok na servery [redacted], spočívající v pravděpodobném zneužití zranitelnosti v software [redacted], ve kterém je dále uvedeno: *„přesto, že byl server aktualizován a záplatován cca dva dny po vydání této aktualizace, tak byl tento server kompromitován. Následně zde došlo k prolomení přístupu do monitorovacího serveru, který měl legitimní přístup k ostatním serverům. Útočníci na další servery rozinstalovali speciálně upravený ransomware, který nebylo možné detekovat antivirovými softwary. Následně pak o víkendu v nočních hodinách spustili útok, jehož výsledkem bylo zašifrování dat na řadě serverů včetně záloh. Motivem útočníka nebylo poškodit skupinu [redacted] zcizením dat, ale vydírat provozovatele serveru o výkupné s možností následného dešifrování dat.“*
Předmětné ohlášení neobsahovalo informace o případných dalších dotčených subjektech, tedy nebyly zde uvedeni další správci osobních údajů, jejichž osobní údaje byly incidentem dotčeny.

Vzhledem k obsahu stížnosti a faktu, že od kontrolované osoby, v postavení správce osobních údajů, nebylo Úřadu doručeno žádné hlášení incidentu, dále v souvislosti s výše uvedeným nahlášením incidentu ze 16. března 2021, především z důvodu identického subjektu napadení, přistoupil Úřad ke kontrole.

Veřejně dostupné informace:
Kontrolovaná osoba je [redacted]. Předmětem podnikání kontrolované osoby je i. vnitřní lékařství, ii. neurologie, iii. dermatovenerologie, iv. radiologie a zobrazovací metody (pouze pro sonografická vyšetření), v. provozování nestátního zdravotnického zařízení: ortopedie, korektivní dermatologie, diabetologie a endokrinologie – pouze v rozsahu diabetologie, kardiologie, gynekologie a porodnictví, rehabilitační a fyzikální medicína, fyzioterapeut, oftalmologie, otorinolaryngologie, všeobecné praktické lékařství, vi. chirurgie, vii. psychiatrie, viii. endokrinologie a diabetologie a ix. výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona.

III. Kontrolní zjištění:

Kontrolní zjištění č. 1 - správce, zpracovatel

Při ústním jednání spojeném s místním šetřením předložila kontrolovaná osoba *Záznamy o činnostech zpracování* (bod 3.12 přehledu podkladů), *Smlouvu o zpracování osobních údajů* (bod 3.19 přehledu podkladů) a dále *Informace pro pacienty o zpracování osobních údajů* (bod 3.5 přehledu podkladů). Z předložených dokumentů a dále z vyjádření kontrolované osoby v rámci ústního jednání a místního šetření 23. listopadu 2021 (bod 3. přehledu podkladů), je prokázané, že kontrolovaná osoba určila účely a prostředky zpracování osobních údajů a nachází se v pozici správce ve smyslu čl. 4 bod 7 nařízení (EU) 2016/679.

[redacted] se nachází v postavení zpracovatele osobních údajů pro správce – kontrolovanou osobu, k čemuž byla předložena *Smlouva o poskytování cloudových a IT služeb č. ITS 15002* z 24. dubna 2015 a na ni navazující S*mlouva o zpracování osobních údajů* (bod 14.17., 14.16., 24.3. a 24.4. přehledu podkladů).

Rozbor smluv:

Smlouva o poskytování cloudových a IT služeb č. ITS 15002
Smlouva deklaruje spolupráci mezi kontrolovanou osobou a dodavatelem, který je ke kontrolované osobě v pozici zpracovatele. Smlouva byla uzavřena dne 24. dubna 2015 mezi kontrolovanou osobou jako objednatelem a [redacted] jako dodavatelem.

V rámci uvedené smlouvy se obě strany dohodly na poskytnutí komplexních cloudových a souvisejících IT služeb dodavatele objednateli. Podstatou uvedených cloudových služeb je umožnit osobám vybraných objednatelem připojení z počítačů a jiných zařízení k internetu k serveru objednatele prostřednictvím klientské aplikace s využitím jména a hesla a využívání SW, úložného prostoru, databází a dalších pokutovaných služeb dodavatele pro potřeby objednatele.
Smlouva též obsahuje podmínky pro migraci dat a přechod na zařízení poskytované dodavatelem.

V *čl. VI. Uživatelé* je v bodě 6.3 uvedeno, že před podpisem této smlouvy předpokládá dodavatel využití služeb celkem 30 až 40 uživateli objednatele.

V *čl. IX. Zajištění software a obsahu,* v bodě 9.1 je uvedeno, že dodavatel je povinen zajistit potřebná licenční oprávnění k SW, jehož užívání je umožňováno objednateli v rámci služeb.
V bodě 9.2. je dále uvedeno, že dodavatel je povinen zajistit, aby veškerá data nebo jakékoliv jiné informace ukládané objednatelem a uživateli v rámci služeb na zařízeních dodavatele byla:

9.2.1 řádně zabezpečena proti útoku třetích stran, a to minimálně na úrovni obvyklé pro obdobné služby (aktuální firewallové a antivirové zabezpečení)
9.2.2 průběžně zálohována kritickými zálohami v souladu se specifikacemi
9.2.3 uložena na zařízeních dodavatele umístěných fyzicky v České republice, či, je-li to předem objednateli oznámeno, v jiných zemích EU
9.2.4 přístupná pouze objednateli a oprávněným uživatelům, nestanoví-li smlouva jinak.

V *čl. XI. Další práva a povinnosti smluvních stran*, bod. 11.10 je uvedeno, že dodavatel je povinen zálohovat data na jiném zařízení tak, aby nevzniklo riziko škody způsobené ztrátou z dat nebo poškozením dat.

Příloha č. 1 ke smlouvě č. ITS 15002 – Specifikace Služeb navazuje na Smlouvu č. ITS 15002, upravuje balíčky poskytovaných služeb dodavatelem [redacted]

V části *B. POPIS SLUŽEB, čl. I. Služby poskytované v rámci balíčku, v bodě 1.2 Systémová správa (povinná část) 1.2.1* je uvedeno, že systémová správa obsahuje mj. bezpečnostní aktualizace, základní monitoring procesů, zatížení, dostupnosti, výkonu, kapacity apod. a další činnosti nutné pro spolehlivý chod systému. Dále je bodě 1.2.2 uvedeno, že zahrnuje obnovu operačního systému v případě selhání. V témže článku v *bodě 1.5 Zálohování* jsou uvedeny podmínky pro zálohování dat. V bodě 1.5.1 se stanoví období délky archivace záloh obsahujících operační systém, všechny nainstalované programy a všechna uživatelská data („kritické zálohy“), obvykle nepřesahující 14 dnů. V bodě 1.5.3 je uvedeno, že kritické zálohy

(není-li sjednáno jinak) [redacted]. Kritické zálohy jsou užívány pro automatické obnovení systému v případě kolapsu, k dispozici objednateli jsou na vyžádání.
V části *B. POPIS SLUŽEB, čl. II. Služby poskytované mimo rámec balíčků, bod 2.2.1* je uvedeno, že v případě poškození nebo ztráty dat při kritickém selhání operačního systému nebo datového úložiště jsou systémová i uživatelská data obnovována zdarma resp. v ceně balíčku.

Příloha č. 2 ke smlouvě č. ITS 15002 – Pravidla dostupnosti služeb (SLA) upravuje dostupnost objednaných služeb a poskytování uživatelské podpory.

Čl. 32 nařízení (EU) 2016/679 upravuje podmínky pro zabezpečení osobních údajů pro správce i zpracovatele. Dle odst. 1 uvedeného článku, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně: a) pseudonymizace a šifrování osobních údajů b) schopnosti zajistit neustálou důvěrnost, integritu a dostupnost a odolnost systémů a služeb zpracování c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečného zpracování.
S ohledem na uvedené ustanovení nařízení (EU) 2016/679 se zpracovatel zavázal zajistit, aby veškerá data nebo jakékoliv jiné informace ukládané správcem (objednatelem) a uživateli v rámci služeb na zařízeních zpracovatele (dodavatele) byla: řádně zabezpečena proti útoku třetích stran, a to minimálně na úrovni obvyklé pro obdobné služby; průběžně zálohována kritickými zálohami v souladu se specifikacemi.
Současně se ve smlouvě zpracovatel (dodavatel) zavazuje zálohovat data na jiném zařízení tak, aby nevzniklo riziko škody způsobené ztrátou z dat nebo poškozením dat.

Smlouva o zpracování osobních údajů z 23. května 2018:
Předmět smlouvy je specifikován v části I. jako povinnost zpracovávat pro správce osobní údaje definované článkem III. a závazek mlčenlivosti. Z dané části smlouvy tak není patrné, co je hlavním cílem zpracování a předmět smlouvy tak není zcela jasně definován. Přesnější informace lze vyčíst až z čl. III smlouvy, kde je cíl zpracování možné vyvodit z povahy zpracování, která je spjata s hlavní smlouvou, tj. *Smlouvou o poskytování cloudových a IT služeb č. ITS 15002* (dále jen „hlavní smlouva“). Cílem je tak zpracování osobních údajů v souvislosti s plněním povinností, definovaných hlavní smlouvou.
Část III. je definován účel a nepřímo i cíl zpracování, rozsah zpracování, typ zpracovávaných osobních údajů (kontaktní informace, identifikátory, informace o zdraví, genetické údaje, biometrické údaje, lokační údaje, finanční informace) a kategorie subjektů údajů (zaměstnanci, pacienti, kontaktní osoby, smluvní partneři správce). Doba zpracování je pak navázána na dobu platnosti hlavní smlouvy. Ve článku je uvedeno, že zpracovatel disponuje plnými administrátorskými přístupy k serverům a databázím správce. Zpracovatel zpracovává osobní údaje ukládáním na nosiče informací, uchováváním a předáváním v elektronické podobě.

Práva a povinnosti smluvních stran dle čl. IV. Obsahují informační povinnost stran podstatných skutečností způsobilých ovlivnit řádné a včasné plnění závazků, povinnost součinnosti při zajišťování souladu dle čl. 32 až 36 nařízení (EU) 2016/679 a povinnost součinnosti při plnění

povinností vůči subjektům údajů, definovaným čl. 16 až 21 nařízení (EU) 2016/679. K plnění povinností dle čl. 32 nařízení (EU) 2016/679 je toliko uvedeno: *„3. Zpracovatel je povinen s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně učinil opatření dle čl. 32 odst. 1 písm. a) až d) GDPR."* V dalším textu je dále uvedeno: *„5. Zpracovatel je povinen přijmout taková opatření, spolu s vnitřními postupy vedoucí k odhalování a zvládání případů porušení zabezpečení a zohlednit zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztrátu, změnu nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. 6. Mezi taková opatření může patřit mimo jiné: přesně stanovit pravidla pro práci s danými informačními systémy, zajistit, aby systémy pro automatizované zpracování osobních údajů používaly pouze oprávněné osoby, aby tyto osoby měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány a zabránit neoprávněnému přístupu k datovým nosičům, zejména prostřednictvím nastavení hesel, přístupových práv, šifrování, dokumentace k přijatým technicko-organizačním opatřením, zámků apod."* V další části jsou popsána již přijatá opatření: *„7. Zpracovatel prohlašuje, že již přijal mimo jiné opatření, a. která minimalizují riziko ztráty zpracovávaných osobních údajů před útoky z internetu. Jedná se především o zabezpečené nastavení firewallu a jiných pokročilých funkcí, které aktivně zabraňují zcizení dat útočníky; b. která omezují přístupu k osobním údajům správce na nezbytné minimum zaměstnanců a subdodavatelů zpracovatele; c. která zavádí logovací systém zaznamenávající přístupy a práci s osobními a jinými daty správce ze strany zaměstnanců a subdodavatelů zpracovatele."*
V této části je dále upraveno, že správce sám zavede logovací systémy kontrolující činnosti zaměstnanců a oprávněných osob správce.

Zpracovatel má povinnost v souladu s čl. 33 odst. 2 nařízení (EU) 2016/679 ohlásit porušení zabezpečení osobních údajů správci, a to bez zbytečného odkladu, jako kontaktní údaje je uvedena e-mailová adresa [redacted] a č. telefonu [redacted].

V rámci této smlouvy je stanovena i povinnost součinnosti při jednáních s Úřadem či jinými oprávněnými subjekty. V dalším tento článek obsahuje závazky zpracovatele: zpracovávat osobní údaje toliko na základě doložených pokynů správce vč. předávání třetím zemím či mezinárodním organizacím, povinnost závazku mlčenlivosti osob zpracovávající osobní údaje, při zapojení dalšího zpracovatele zabezpečení stejné úrovně zabezpečení osobních údajů, součinnost při výkonu práv subjektů údajů, povinnost výmazu či předání osobních údajů správci při ukončení služeb, umožnění a součinnost při auditech, inspekcích a jiných kontrolách.

Kontrolovaná osoba se k předmětu kontroly nachází v postavení správce osobních údajů ve smyslu čl. 4 bod 7 nařízení (EU) 2016/679 a [redacted] se vůči kontrolované osobě nachází v postavení zpracovatele ve smyslu čl. 4 bod 8 nařízení (EU) 2016/679.

Kontrolní zjištění č. 2 - Zabezpečení osobních údajů

Zabezpečení osobních údajů před incidentem:
V ohlášení porušení zabezpečení je uvedeno, že před porušením zabezpečení byla přijata tato organizační a technická opatření: zřízeny byly samostatné přístupové účty pro všechny

uživatele, pravidelně byly vynucovány změny hesla a jeho náročnosti, logovány byly přístupy do systému, nastaveny byly automatické aktualizace antivirového řešení, pravidelně byl aktualizován [redacted]. Kontrolovaná osoba dále uvádí, že osobní údaje byly zpracovávány těmito SW a HW prostředky: [redacted] při místním šetření 17. března 2022 (bod 21. přehledu podkladů) uvedla, že užívá servery v [redacted] (bod 21.4 přehledu podkladů). Přístup je zabezpečen prostřednictvím jediné přístupové karty (verifikace na recepci a kontrola dle občanského průkazu), 1 rack pod klíčem (všechny technologie) a fyzickým zámkem. [redacted] byla doložena screenshoty (bod 21.5 až 21.9 přehledu podkladů), užívána je verze [redacted]. V rámci svých serverů společnost provozuje desítky virtuálních serverů dle požadavků klientů. Klienti jsou izolováni v rámci svých virtualizací a v rámci virtualizace jsou provozována jednotlivá řešení klientů. Hlavní 4 servery jsou spojeny do clusteru, což je zajištěno zmíněným řešením od [redacted]. K narušení dat došlo v rámci clusteru, přičemž virtualizace nebyla dotčena, došlo k napadení hostovaných řešení zmíněných klientů. Přes napadení mail serveru [redacted] došlo ke kompromitaci monitorovacího serveru a následnému narušení systémů. Všechny napadené systémy využívaly operační systém [redacted]. Zde společnost uvádí, že nejspíše [redacted].

Zabezpečení osobních údajů po incidentu:
Původní, nevyhovující monitorovací řešení bylo nahrazeno jiným. [redacted].

Zabezpečení osobních údajů – závěr:
V době útoku byla aktivně zneužívána série zranitelností [redacted], jejichž kombinací mohl útočník, bez autentizace a uživatelské interakce, získat přístup k emailovým schránkám na serveru a následně vzdáleně spustit kód. Kontrolující upozorňují, že výrobce programu [redacted] vydal na tyto chyby opravy již 2. března 2021[1]. Na aktivní využívání těchto chyb důrazně upozorňoval i Národní úřad pro kybernetickou a informační bezpečnost v aktualitě *„Upozornění na zranitelnosti* [redacted]. Pokud útočník získal dne 14. března 2021 přístup díky

[1] [redacted]

[2] [redacted]

využití výše uvedených zranitelností a následně se mu podařilo kompromitovat a zašifrovat data správce osobních údajů, konstatují kontrolující nedostatečnou reakci zpracovatele na kybernetické hrozby, které bylo možné v době útoku velmi pravděpodobně eliminovat včasnou instalací dostupných záplat. [redacted] nebyla schopna doložit dostatečnost bezpečnostních opatření před útokem, neboť v rámci reakce na útok došlo k reinstalaci části systémů, včetně výměny použitých technologií.

Kontrolující tak mají za prokázané, že vzhledem k výše popsanému, došlo k porušení zabezpečení ochrany osobních údajů z důvodu nedostatečného nastavení ochrany osobních údajů zpracovatelem. Kontrolující upozorňují, že správce osobních údajů je povinen využívat jen takové zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky nařízení (EU) 2016/679 a aby byla zajištěna ochrana práv subjektů údajů.

Kontrolní zjištění č. 3 – Porušení zabezpečení osobních údajů

3.1. Ohlášení porušení zabezpečení správci a Úřadu

Kontrola byla zahájena 23. listopadu 2021 předložením pověření ke kontrole v sídle kontrolované osoby (bod 3 přehledu podkladů). Kontrolovaná osoba při tomto šetření předložila *Ohlášení porušení zabezpečení osobních údajů dle GDPR* (bod 3.2 přehledu podkladů). Incident, který byl předmětem tohoto ohlášení porušení zabezpečení osobních údajů, ohlásila Úřadu [redacted] (dle vyjádření kontrolované osoby její mateřská společnost), která je v ohlášení uvedena jako správce osobních údajů, avšak v textu ohlášení není uvedeno, že by se předmětné ohlášení týkalo rovněž kontrolované osoby, či, jak uvedla kontrolovaná osoba (bod 3., otázka č. 8), že by se incident týkal více společností.

Kontrolovaná osoba uvedla (bod 23. přehledu podkladů), že [redacted] (povinná osoba) zjistila porušení 15. března 2021 v 9:00 hodin, přičemž jako počátek porušení označila 14. březen 2021 mezi 0:00 a 03:00 hodinou. Povinná osoba pak v den zjištění porušení (15. března 2021) kontaktovala [redacted], která následně telefonicky (nebylo užito e-mailu z důvodu jejich nefunkčnosti způsobené incidentem) informovala vlastní jednotlivé dotčené společnosti, vč. kontrolované osoby (bod 23. otázka č. 1 přehledu podkladů). Kontrolovaná osoba byla konkrétně kontaktována 15. března 2021, telefonicky, kdy oznámení porušení bylo nahlášeno [redacted] (bod 19 přehledu podkladů). Následně [redacted] zaslala dne 18. března 2021 písemně dotčeným správcům *Oznámení o narušení bezpečnosti prostředí společnosti* (bod 14.9 přehledu podkladů).

Kromě výše uvedeného ohlášení (bod 3.2 přehledu podkladů) předložila kontrolovaná osoba také *Formulář hlášení kybernetického bezpečnostního incidentu*[3] (jako ohlašující byl uveden e-mail [redacted], tel. [redacted], z něhož je patrné, že ohlášení provedla de-facto [redacted] a to jménem [redacted]. V hlášení je uvedeno, že se jednalo o útok Kategorie III – velmi závažný kybernetický bezpečnostní

[3] V souvislosti se zákonem č. 181/2014 Sb., o kybernetické bezpečenosti, byla definována dvě pracoviště – vládní CERT a národní CERT (roli národního CERTu plní v současné době tým CSIRT.CZ). Tato dvě pracoviště jsou povinna přijímat od povinných orgánů a osob definovaných v § 3 uvedeného zákona informace o kybernetických bezpečnostních incidentech a také kontaktní informace daných subjektů.

incident, přičemž tento byl způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému. Dle standardu *ENISA/eSCIRT.net* se jednalo o *malicious code* (např. virus, červ, trojský kůň), *intrusion attemps* (např. zneužití zranitelnosti, kompromitace aktiva), *intrusions* (např. kompromitace aplikace nebo uživatelského účtu). Počet zasažených systémů: 10. Odhad počtu dotčených uživatelů: 150. Popis incidentu: Cca o půlnoci mezi sobotou a nedělí (13. – 14. 3. 2021) se nám začala šifrovat řada [redacted]. Cca ve 3 hodiny v noci na to začali reagovat naši správci, začali servery odpojovat od síťové konektivity. Výsledkem je prakticky kompletně zašifrované prostředí všech dat a dat našich zákazníků. Významná část dat je pro nás v tuto chvíli zřejmě nenávratně ztracená, šifrování zasáhlo bohužel i naše zálohovací servery a k tomu připojené zálohy. Rozsah škod: kompletně zašifrovaná data na serverech, kompletně zašifrované databáze, kompletně zašifrované zálohy. Jaká opatření byla přijata? Předpokládáme, že bez ohledu na rozsah škod je celé původní prostředí kompromitované. Z tohoto důvodu probíhá zcela nová instalace celého prostředí, čistých serverů, generování nových přístupů, instalace čistých aplikací, instalace nových bezpečnostních řešení. Systémové detaily – cíl útoku: Host nebo IP: více systémů, serverů. Funkce hosta: terminálové servery, databázové servery, file store, zálohovací servery.

Předložen byl rovněž *Úřední záznam o podaném vysvětlení podle § 158 odst. 6 trestního řádu* z 15. března 2021 8:31 hodin, ze kterého je patrné, že [redacted] ohlásil kybernetické napadení serveru společnosti Policii ČR, Obvodnímu ředitelství policie Praha III, Službě kriminální policie a vyšetřování, se sídlem Lupáčova 11, 130 00 Praha a toto ohlášení je vedeno pod č.j. KRPA-64527-1/ČJ-2021-0013SV.

Ani z jednoho z uvedených dokumentů není patrné, že by se kybernetický útok týkal také kontrolované osoby, tedy že by útokem měly být napadeny osobní údaje spravované správcem – kontrolovanou osobou.

Kontrolovaná osoba při místním šetření předložila formulář vlastního dokumentu pro případná hlášení incidentů *Ohlášení porušení zabezpečení osobních údajů* (bod 3.14 přehledu podkladů), ve kterém je uvedeno: *„pozn. Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a zpravidla ve lhůtě do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí ÚOOÚ, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.“* Z daného je jasné, že kontrolovaná osoba má pro případy porušení zabezpečení vypracován povinný dokument, pro hlášení porušení. Kontrolující tak poznamenávají, že v tomto dokumentu není uvedena alternativa, že by za správce osobních údajů – kontrolovanou osobu, mohly ohlášení porušení provádět jiné právnické osoby, respektive jiní správci osobních údajů, a to ani v případě, že jsou s kontrolovanou osobou ekonomicky či jinak propojeni.

Jak je uvedeno ve *Smlouvě o zpracování osobních údajů* (bod 3.19 a 24.4. přehledu podkladů), má [redacted] v pozici zpracovatele povinnost bez zbytečného odkladu ohlásit jakékoli porušení zabezpečení osobních údajů správci. Společnost tak vůči správci prokazatelně učinila prostřednictvím [redacted], a to telefonicky cca 27 hodin od zjištění porušení. Kontrolovaná osoba měla, dle smlouvy, následně bez zbytečného odkladu ohlásit porušení zabezpečení Úřadu, pokud možno do 72 hodin od chvíle, kdy se o porušení zabezpečení dozvěděla. Ačkoli kontrolovaná osoba uvádí, že předmětné ohlášení [redacted] je ohlášením, které sama prostřednictvím [redacted] v zákonné lhůtě udělala, kontrolující vzhledem k výše uvedeným faktům nemohou toto ohlášení považovat za

splnění povinnosti dle čl. 33 odst. 1 nařízení (EU) 2016/679 ze strany správce, kontrolované osoby. Ohlášení neobsahovalo žádnou informaci o tom, že by se ohlášení vztahovalo na jakéhokoli jiného správce osobních údajů, kromě správce – [redacted].

Kontrolující tak považují za splnění ohlašovací povinnosti ze strany kontrolované osoby toliko předání formuláře ohlášení při místním šetření 23. listopadu 2021, kdy kontrolovaná osvětlila, že se toto ohlášení týkalo rovněž jí, tedy že incidentem byli dotčeni klienti (subjekty údajů) kontrolované společnosti.

V ohlášení porušení zabezpečení je uvedeno, že pravděpodobně došlo ke zneužití zranitelnosti v [redacted] a že i přes řádné aktualizace byl server kompromitován, kdy následně došlo k prolomení přístupu do monitorovacího serveru, který měl legitimní přístup k ostatním serverům. Útočníci, dle ohlášení na další servery následně nainstalovali speciálně upravený ransomware, přičemž účinky porušení zabezpečení byly v porušení dostupnosti dat.

Dotčeny byly tyto kategorie subjektů údajů: zaměstnanci nebo osoby v pracovněprávním vztahu ke správci/zpracovateli, uživatelé, zákazníci, pacienti, zranitelné osoby (např. děti), jako přibližný počet bylo uvedeno 500 zaměstnanců a 50 000 pacientů. Mezi dotčené kategorie osobních údajů patří: identifikační údaje, kontaktní údaje, ekonomické a finanční údaje, data o poloze. V rámci osobních údajů zvláštní kategorie to byly údaje o zdravotním stavu. Jako důsledky dopadu na ohrožené subjekty jsou uvedeny ztráta nebo změna schopnosti správce /zpracovatele poskytovat služby pro dotčené subjekty údajů, finanční ztráty a poškození pověsti.

Kontrolovaná osoba při ústním jednání a místním šetření 23. listopadu 2021 (bod 3 přehledu podkladů, dotaz č. 3) uvedla, že *„po hovoru s právním oddělením kontrolovaná osoba dostala informaci, že de facto nedošlo k úniku dat, ale bezpečnostní incident spočíval v dočasném zablokování přístupu k datům. Odblokování systému trvalo přibližně jeden týden“.* Současně k odpovědi předložila *Ohlášení porušení zabezpečení osobních údajů dle GDPR (bod 3.2 přehledu podkladů)* vztahující se k předmětnému data-breach, *Formulář hlášení kybernetického bezpečnostního incidentu (bod 3.3 přehledu podkladů)* a *Úřední záznam o podaném vysvětlení podle § 158 odst. 6 tr. řádu na Policii České republiky (bod 3.1 přehledu podkladů).* K dotazu, proč bezpečnostní incident nahlásila pouze [redacted] zástupce kontrolované osoby sdělil: *„jedná se o [redacted] a vzhledem k tomu, že se porušení zabezpečení osobních údajů týkalo více [redacted], veškeré dokumenty k incidentu, včetně hlášení na všechny tyto společnosti učinila* [redacted]

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. Kontrolovaná osoba se o porušení zabezpečení prokazatelně dozvěděla 15. března 2021 (telefonicky) a 18. března 2021 (písemně), přičemž ohlášení porušení zabezpečení pak prokazatelně učinila až dne 23. listopadu 2021.

3.2. Oznámení porušení zabezpečení subjektům údajů:

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez

zbytečného odkladu subjektu údajů. Vzhledem k faktu, že porušení zabezpečení se týkalo rovněž zvláštní kategorie osobních údajů, je nutné k tomuto porušení zabezpečení přistupovat jako k vysoce rizikovému. Vzhledem k faktu, že došlo k zašifrování všech údajů včetně záloh, a tedy ke ztrátě dostupnosti osobních údajů obsahujících i údaje o zdravotním stavu, měl dle kontrolujících správce za povinnost vyrozumět fyzické osoby o možném dopadu nedostupnosti údajů a o pravděpodobných důsledcích.

Ohlášení porušení zabezpečení osobních údajů (bod 3.2. přehledu podkladů) obsahuje v části *11.3. oznámení dotčeným fyzickým osobám* informaci, že subjekty údajů (pacienti) nebudou informováni z důvodu, že by to představovalo nepřiměřené úsilí s dodatkem, že budou informováni na webových stránkách

Při místním šetření (bod 3 přehledu podkladů) kontrolovaná osoba uvedla, že *„Subjekty údajů byly o incidentu informovány prostřednictvím zprávy vyvěšené na webových stránkách společnosti, a to bezprostředně po zjištění incidentu, po dobu minimálně 1 měsíce. Pacienti byli dále informováni ústně při návštěvách zdravotnického zařízení, na recepci polikliniky."*

Upřesněno bylo datum a znění zveřejnění informace (bod 25. a příloha 25.1. přehledu podkladů), přičemž od 15. března 2021 do 21. března 2021 měla být vyvěšena informace: *„ONÁMENÍ 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 úroku kontaqktujte našeho pověřence na ochranu osobních údajů jehož kontakt je uvedený na našich webových stránkách. Kybernetické napadení řešíme ve spolupráci s naším pověřencem, IT odborníky, ÚOOÚ, NÚKIBem a Policií ČR."* K tomu, že daný text byl v danou dobu skutečně zveřejněn prostřednictvím webových stránek však kontrolovaná nedoložila (bod 25. přehledu podkladů), kdy nemožnost dodání důkazu o zveřejnění informace zdůvodnila změnou jednatele (k čemuž je nutné pouze poznamenat, že změna jednatele nic nemění na povinnosti správce doložit soulad s nařízením (EU) 2016/679 dle čl. 5 odst. 2 tohoto nařízení).

Kontrolovaná osoba při místním šetření (bod 3 přehledu podkladů) rovněž uvedla, že *„Ke zveřejněným a poskytnutým informacím nezaznamenala kontrolovaná osoba žádné reakce ze strany dotčených subjektů údajů."*

Toto tvrzení je však v rozporu se stížností stěžovatele (bod 1. přehledu podkladů), který doložil komunikaci s kontrolovanou osobou (bod 1.2. přehledu podkladů). Stěžovatel v ní uvádí, že se o kybernetickém útoku dozvěděl z médií a nikoli od správce, jako poskytovatele zdravotní péče, jehož služby stěžovatel aktivně využíval. Doložil, že se 19. března 2021 dotázal správce na podrobnosti útoku, a to mimo jiné popis, datum a čas porušení, datum a čas zjištění porušení a popis přijatých opatření k zabránění dalšího neoprávněného přístupu. Kontrolovaná osoba ve své odpovědi (bod 1.1. přehledu podkladů) sice uvádí: *„1. Jak již bylo uvedeno na našich webových stránkách napadení směřovalo na kompletní IT infrastrukturu našeho dodavatele IT služeb. 2. Cílem útoku nebylo poškodit, zneužít naše data, ale znemožnit jejich užití zašifrováním s následným vymáháním finanční částky výměnou za jejich opětovné zpřístupnění. 3. Po provedených kontrolách můžeme uvést, že útok nebyl úspěšný. Všechna naše data máme k dispozici, a to i přes krátkodobý výpadek jsme zpět v plném provozu."* V dalším kontrolující uvádí: *„Povinnost informovat vychází z nařízení GDPR v případě, kdy daný*

případ bude mít za následek vysoké riziko pro práva a svobody dotčených osob. Zároveň uvádí, že oznámení se nevyžaduje jestliže: a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování; b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví; c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření. Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek uvedených v odstavci 3.“

Kontrolující k tomu uvádějí, že ve smyslu čl. 34 odst. 2 nařízení (EU) 2016/679 musí oznámení určené subjektu údajů obsahovat povahu porušení zabezpečení osobních údajů a přinejmenším informace: jméno a příjmení pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace, popis pravděpodobných důsledků porušení zabezpečení osobních údajů a popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jak je popsáno výše, kontrolovaná osoba tvrdí, že k ohlášení došlo prostřednictvím webových stránek a dále ústně, při osobních návštěvách subjektů údajů na recepci polikliniky. K tomuto je třeba předně uvést, že v daném případě by k naplnění podmínek čl. 34 nepostačovalo sdělení subjektům na recepci polikliniky, neboť dosah takovéhoto učinění oznámení není v žádném případě srovnatelný s oznámením učiněným na internetových stránkách správce.

K samotnému zveřejnění oznámení na webu správce, k čemuž mělo dle tvrzení kontrolované osoby dojít, je nutné uvést, že toto nelze mít na základě doložených dokumentů za prokázané. Sama kontrolovaná osoba ostatně uvedla ve svém přípisu (bod 25 přehledu podkladů), že *„Screenshot obrazovky bohužel nemáme,* (…) *ale vzhledem ke změně jednatele Společnosti v minulém roce nejsme schopni tento dodat.“* Samotný text, který údajně měl být na webu uveřejněn, toto uveřejněný neprokazuje.

Též je nutné v této souvislosti upozornit na fakt, že informace, které byly sděleny stěžovateli, neodpovídají textu údajného oznámení, neboť stěžovateli bylo sděleno, že *„Jak již bylo uvedeno na našich webových stránkách napadení směřovalo na kompletní IT infrastrukturu našeho dodavatele IT služeb.* “ Takováto informace však v údajném oznámení zcela absentuje. Tato skutečnost by mohla nasvědčovat tomu, že byl text oznámení koncipován ex post či pro účely kontroly. Nicméně i bez této skutečností platí závěr, že kontrolovaná nedoložila publikování oznámení na webu.

Kontrolovaná osoba nedoložila splnění povinnosti stanovené v ustanovení čl. 34 odst. 1 nařízení (EU) 2016/679, tj. nedoložila, že by vhodným způsobem oznámila porušení zabezpečení osobních údajů subjektům údajů.

Pro úplnost lze dodat, že i kdyby zaslané oznámení bylo skutečně vyvěšeno na webu kontrolované osoby (což nicméně nebylo doloženo), zcela v tomto *Oznámení o kybernetickém útoku* absentuje jasná informace o tom, že se útok dotýkal zpracovávaných osobních údajů a subjekt údajů by nemusel dojít k tomu, že se mělo jednat o oznámení ve smyslu čl. 34 odst. 1

nařízení (EU) 2016/679. I v případě doložení publikování oznámení na webu by pak muselo být konstatováno minimálně porušení čl. 34 odst. 2 nařízení (EU) 2016/679.

3.3. Dokumentace všech případů porušení zabezpečení osobních údajů (bod 3.15 přehledu podkladů)

Jedná se o dokument vydaný kontrolovanou osobou a předložený v rámci ústního jednání a místního šetření. V uvedeném dokumentu se nachází pouze 1 záznam, z čeho lže dovodit, že předmětný hackerský útok byl jediným zaznamenaným útokem u kontrolované osoby. Z dokumentu není zřejmé, k jakému datu byla zahájena evidence těchto incidentů. V dokumentu je 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: [redacted], Instrusions (např. kompromitace aplikace nebo uživatelského účtu), přijatá opatření: Předpokládalo se, že bez ohledu na rozsah škod je celé původní prostředí kompromitované. Z toho důvodu proběhla zcela nová instalace celého prostředí, čistých serverů, generování nových přístupů, instalace čistých aplikací, instalace nových bezpečnostních řešení. Problém byl vyřešen a data dešifrována. Došlo k zcela nové instalaci celého prostředí, čistých serverů, generování nových přístupů, instalace čistých aplikací, instalace nových bezpečnostních řešení. Nedošlo k úniku dat.

Dle čl. 33 odst. 5 nařízení (EU) 2016/679 správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

Z uvedeného vyplývá, že správce je povinen vést dokumentaci veškerých případů porušení zabezpečení osobních údajů a tuto na požádání dozorovému úřadu předložit. Kontrolovaná osoba předložila jí vedenou dokumentaci, ze které však není zřejmé, za jaké období porušení zabezpečení eviduje. Jako zásadní nedostatek je, že dokumentace neobsahuje účinky porušení zabezpečení (tj. jaký dopad porušení zabezpečení mělo a alespoň rozsah dotřených osobních údajů), neboť tato část toliko heslovitě a příkladmo vyjmenovává možné důvody porušení zabezpečení, nikoliv však jeho účinky. Stejně tak v záznamu není uvedeno, z jakých podkladů správce vycházel, když uvedl, že nedošlo k úniku dat / osobních údajů.

Kontrolou bylo prokázáno, že kontrolovaná osoba porušila ustanovení čl. 33 odst. 5 nařízení (EU) 2016/679, z důvodu, že jí vedená dokumentace porušení zabezpečení osobních údajů neobsahuje účinky daného porušení.

IV. Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

Kontrolující:

Mgr. Eva Cupáková	vedoucí kontrolní skupiny	*(podepsáno elektronicky)* podpis
Mgr. Marek Šnajdr	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Bc. Jaromír Kuba	pověřený zaměstnanec Úřadu	_____ Podpis