ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

čj. UOOU-11412/17-17
Praha 19. března 2018

Protokol o kontrole

Kontrolní orgán:
Úřad pro ochranu osobních údajů, se sídlem 170 00 Praha 7 – Holešovice, Pplk. Sochora 727/27, IČ: 70837627 (dále jen „Úřad“).
Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z § 2 odst. 2 a 3, § 29 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon č. 101/2000 Sb.“).

Kontrolující:
– inspektorka Úřadu pro ochranu osobních údajů, PaedDr. Jana Rybínová, číslo průkazu [redacted];
– pověřený zaměstnanec Úřadu pro ochranu osobních údajů, JUDr. Michal Jelínek, číslo průkazu [redacted];
– pověřený zaměstnanec Úřadu pro ochranu osobních údajů, Ing. Max Gůt, číslo průkazu [redacted].

Kontrolovaná osoba:
[redacted]. se sídlem [redacted], [redacted] (dále jen „Kontrolovaná osoba“ nebo „Klinika“).
Zastoupená:
[redacted], [redacted] na základě Substituční plné moci [redacted].

Předmět kontroly:

Předmětem kontroly je plnění povinností správce osobních resp. citlivých údajů klientů při jejich zabezpečení ve smyslu § 13 zákona č. 101/2000 Sb.

Zahájení kontroly:
Přípis Oznámení o zahájení kontroly čj. UOOU-11412/17-8 ze dne 10. ledna 2018, které Kontrolovaná osoba obdržela téhož dne.

Poslední kontrolní úkon předcházející vyhotovení protokolu o kontrole – Úřední záznam k ústnímu jednání a místnímu šetření ze dne 15. března 2018, č.j. UOOU-011412/17-16.

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady (údaje, dokumenty a věci vztahující se k předmětu kontroly nebo k činnosti Kontrolované osoby a dokumenty, které byly pořízeny v průběhu kontroly), popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti.

1. Podnět, který Úřad obdržel [redacted], čj. UOOU-11412/17-1 elektronickou cestou;
2. Žádost Úřadu, o doplnění podnětu, č.j. UOOU-11412/17-2 [redacted];
3. Doplnění podnětu od stěžovatelky [redacted], č.j. UOOU-11412/17-3 + přílohy – kopie e-mailové komunikace s Klinikou (4 listy);
4. Interní sdělení č.j. UOOU-11412/17-4 ze dne 18. prosince 2017 – předání podnětu odboru kontrolnímu;
5. Sdělení Úřadu stěžovatelce ze dne 19. prosince 2017, č.j. UOOU-11412/17-5;
6. Interní sdělení – předání podnětu ke kontrole, ze dne 19. prosince 2017, č.j. UOOU-11412/17-6;
7. Analýza podnětu ze dne 4. ledna 2018; , č.j. UOOU-11412/17-7 + příloha kopie formuláře Request and call back;
8. Oznámení o zahájení kontroly ze dne 10. ledna 2018, č.j. UOOU-11412/17-8;
9. Sdělení Kontrolované osoby ze dne 24. ledna 2018, č.j. UOOU-11412/17-9 + přílohy:
    - písemná informace
    - vnitřní předpis [redacted] Pracovní postup na oddělení [redacted]
    - Záznam o interním školení [redacted]
    - Souhlas se zpracováním osobních údajů
    - vnitřní předpis [redacted] Řízení informačních systémů [redacted]
    - vnitřní předpis [redacted] Pravidla pro uživatele [redacted]
    - e-mail ze dne [redacted] – aktualizované směrnice
    - Organizační řád
    - Zápis z porady ze dne [redacted];
10. Úřední záznam o pořízení výtisku webových stránek Kontrolované osoby ze dne 14. února 2018, č.j. UOOU-11412/17-10 + přílohy:
    - Formulář „Kontaktujte nás“ - [redacted]
    - Formulář „Request and call back“ - [redacted]
    - Formulář „Kontaktujte nás“ - [redacted]
    - Souhlas se zpracováním osobních údajů
    - Consent to processing of personal data

11. Žádost o součinnost ze dne 20. února 2018, č. j. UOOU-11412/17-11;
12. Protokol z ústního jednání a místního šetření [redacted], č.j. UOOU-11412/17-12 + přílohy:
    - dokument písemná informace o souhlasu se zpracováním osobních údajů [redacted]
    - kopie vyplněného formuláře [redacted]
    - kopie interního předpisu [redacted] Pracovní postup na oddělení [redacted]
    - kopie vyplněného formuláře [redacted] - Záznam o interním školení (Školení [redacted] Pracovní postup na oddělení [redacted]
    - kopie vnitřního předpisu [redacted] Identifikace pacientů a dárců reprodukčních buněk
    - printscreen Outlook „Pošta, kalendář, lidé úkoly – Inbox“
    - printscreen Outlook „Pošta, kalendář, lidé úkoly“ – nepřečtená pošta
    - kopie vzorové e-mailové odpovědi „Dear xxx“
    - Plná moc - [redacted]
    - Substituční plná moc - [redacted];
13. Úřední záznam (kopie a výtisk souhlasu) ze dne 7. března 2018, č.j. UOOU-11412/17-14;
14. Vyjádření k Protokolu z ústního jednání a místního šetření – oprava a upřesnění ze dne 14. března 2018, č.j. UOOU-11412/17-15;
15. Úřední záznam k Protokolu z ústního jednání a místního šetření ze dne 15. března 2018, č.j. UOOU-011412/17-16.

II. Kontrolní zjištění kontrolujících:

Kontrolní zjištění obsahují:

A. Zjištěný stav věci

[redacted], [redacted]. se sídlem [redacted] je nestátní zdravotnické zařízení poskytující zdravotní péči, výrobu, obchod a služby neuvedené v příloze 1 a 3 živnostenského zákona, zapsaná v obchodním rejstříku vedeným Městským soudem v Praze, v oddílu [redacted], vložka [redacted].

1. Z analýzy podnětu vyplývá:

Stěžovatelka [redacted] ve svém podnětu, který Úřad obdržel [redacted], doplněném [redacted], uvedla (Úřad obdržel podnět v angličtině a v angličtině je vedena veškerá korespondence mezi stěžovatelkou [redacted], Kontrolovanou osobou a osobou, která se označuje [redacted] – překlad dokumentů byl proveden zaměstnanci Úřadu):
„Moje právo na soukromí bylo [redacted] porušeno klinikou [redacted], kdy tato zaslala mé osobní zdravotní údaje mně zcela neznámé [redacted] se žádným způsobem

nezúčastnila tohoto porušení kromě toho, že byla nedobrovolnou příjemkyní emailu, který na konci obsahoval moje zdravotní údaje. Chyba spočívá naprosto na . Měla jsem email a kontaktní informace na . Před pěti dny napsala stížnost do , ale nedostala od nich odpověď. mne také žádným způsobem nekontaktoval, aby mne informoval o tom, že moje soukromé zdravotní údaje byly sdíleny. Velmi mne znepokojuje, že moje údaje mohly být sdíleny dalšími lidmi kromě . Prosím prošetřete a dejte mi vědět, pokud zjistíte, že mé údaje byly sdíleny také dalšími lidmi".

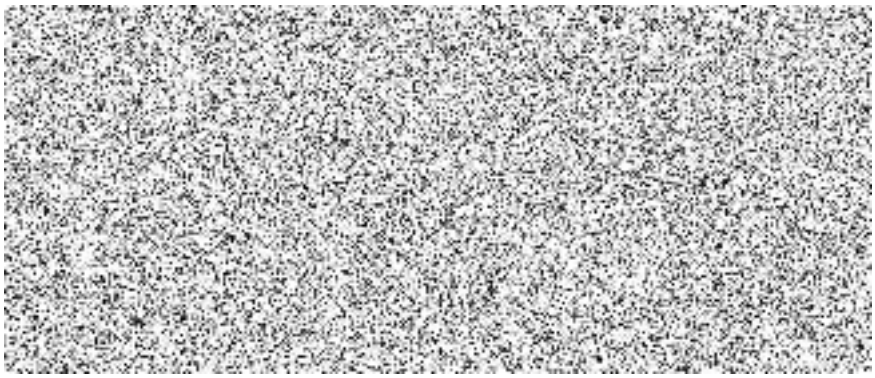
Tato tvrzení stěžovatelka doložila kopiemi e-mailů:

A.
Od:
Komu:

V tomto emailu informuje o tom, že od obdržela zprávu, která obsahuje údaje o . Dále je ve zprávě vložen další email:

B.
Od:
Komu:
Předmět: Záznam požadavku na zpětné volání

Email obsahuje následující údaje:



C.
Od:
Komu:

Ve zprávě jsou vloženy 3 emaily - korespondence mezi a ohledně , přičemž je vložen i email , který obsahuje osobní údaje - viz bod 1. výše.

D.
Od:
Komu:

Ve zprávě jsou vloženy následující 2 emaily:

a) Stížnost

Od: [redacted]
Komu: [redacted]

Velmi mne znepokojuje, že jste mi poslali dotaz jiného pacienta! (Viz na konci tohoto emailu). Určitě nevyužiji vaši kliniku, když vidím, jak jste nedbalí na údaje o pacientech. Kontaktovala jsem [redacted] abych jí informovala o tom, že jste mi poslali její osobní údaje. Jak absolutně nedbalé! Prosím, vymažte všechnu mou korespondenci z vašich emailů, protože nechci být další obětí takových nedbalých praktik.

b) Odpověď [redacted]

[redacted]
Od: [redacted]
Komu: [redacted]

Velmi se omlouvám za chybu. Kontaktní formulář jiného pacienta se bohužel nějak dostal do systému. Tato chyba již byla opravena a nic podobného se již nestane.
Chápeme, jaké zklamání to pro vás musí být a velmi se za to omlouváme.
Jak si přejete, nebudeme vás více kontaktovat.
[redacted]

Kontrolujícími bylo zjištěno, že rozsah osobních údajů v e-mailu [redacted] odpovídá struktuře formuláře „Request and call back" (viz příloha) zveřejněného na stránce [redacted].
Z dotazu [redacted] u společnosti [redacted] na podmínky [redacted] vyplývá, že se jedná o občanku [redacted].
Z vyjádření [redacted] (zaměstnankyně Kliniky, e-mail [redacted] nevyplývá, zda se jednalo o lidskou nebo technickou chybu.

2.

Z informací poskytnutých Klinikou vyplývá:

A.

V rámci kontroly byla vyžádána součinnost podle § 10 odst. 2 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a to v rozsahu § 7, § 8 a § 11 tohoto zákona, Klinika byla požádána o předložení a dokumentování přijatých a provedených technicko-organizačních opatření k zajištění ochrany osobních údajů ve smyslu ustanovení § 13 zákona č. 101/2000 Sb.; dále o předložení organizačního řádu a interních předpisů (pracovní řád, metodické pokyny, pracovní postupy apod.), kterými se řídí komunikace Kontrolované osoby s klienty, resp. zájemci o poskytované služby, dále o popis informační a komunikační infrastruktury sloužící ke zpracování osobních údajů klientů a ke zpracování žádostí o kontakt aplikovaných prostřednictvím webových formulářů Kontaktujte nás / Request and call back. Dále bylo od Kliniky vyžádáno podání vysvětlení, jak a čím bylo [redacted] způsobeno zpřístupnění (odeslání e-mailem) osobních údajů [redacted] neoprávněné osobě [redacted] na e-mailovou adresu [redacted], a to formou připojení přílohy kontaktního formuláře [redacted].

B.

Klinika v rámci kontroly sdělila:

Systém ochrany osobních údajů, které Klinika jakožto poskytovatel zdravotních služeb zpracovává je tvořen souhrnem organizačních, personálních a technických opatření. Mezi tato opatření patří např. pracovní postupy, směrnice, školení zaměstnanců, přístupová hesla do zdravotnických systémů, sledování pohybu osob do určených prostor, zabezpečení listinné i elektronické formy karet pacientů, stanovení postupů o předávání zdravotnické dokumentace nebo poskytování informací pacientům, stanovení kompetencí, skartační řízení, atd. V současné době dle sdělení probíhá na Klinice audit zpracování osobních údajů pro účely splnění požadavků GDPR. Klinika hodlá zavést bezpečnostní [redacted], který bude sledovat, jak se s osobními údaji pacientů nakládá, aby nedošlo k jejich neoprávněnému zpřístupnění nebo pozměnění či zničení. Dále Klinika uvedla, že bohužel ani zavedení nejlepších organizačních nebo technických opatření nedovede zabránit selhání jednotlivce.

Dále Klinika uvedla, že osoby, které mají zájem o její služby, kontaktují Kliniku prostřednictvím webového formuláře nebo prostřednictvím [redacted], postupy při kontaktování klientů a organizační a technická opatření jsou následující:

Potencionální zahraniční klient hovořící anglicky, německy nebo italsky má možnost kontaktovat Kliniku prostřednictvím webového formuláře „Request and Call back“. Údaje z formuláře se následně zobrazují v e-mailové schránce [redacted], ke které mají přístup pouze zaměstnanci na zahraničním oddělení [redacted] zaměstnanců. U českých klientů jsou kontaktní údaje odlišné a pracují s nimi jiní zaměstnanci.

Před odesláním formuláře klienti vyslovují souhlas se zpracováním osobních údajů, který Klinika zasílá v příloze. V některých ojedinělých případech klienti píší přímo na e-mail [redacted], který patrně obdrželi od dalších zahraničních pacientů Kliniky. Jednotlivé příchozí e-maily si rozdělí asistentky na oddělení [redacted] dle jazykových požadavků a odpovídají na ně ze své „podschránky“ [redacted]. S jedním klientem následně komunikuje z této e-mailové schránky asistentka oddělení [redacted]. Na dotaz zobrazený v e-mailové schránce [redacted] podaný prostřednictvím formuláře se bohužel nedá odpovědět přímo, jelikož jako odesílatel není uveden klient, který formulář vyplnil, ale e-mailová schránka [redacted]. Proto je nutné obsah e-mailu zkopírovat do jiného e-mailu („podschránky“), aby mohly být zodpovězeny dotazy uvedené ve formuláři. Klient totiž odesláním formuláře nedostává potvrzení o obsahu položeného dotazu na svůj e-mail nebo jinou formou, a tak nemusí přesně vědět, co do formuláře uvedl.

Klinika dále uvedla, že vedle Pracovního postupu oddělení [redacted] upravuje nakládání s údaji klientů také směrnice „Řízení informačních systémů“ (příloha č.j. UOOU-11412/17-9 ze dne 24. ledna 2018, dále viz str. 10 tohoto protokolu o kontrole), která stanovuje postupy pro řízení výpočetní techniky, včetně požadavků na ochranu dat a údajů. S touto směrnicí byli všichni zaměstnanci rovněž seznámeni [redacted] (viz e-mail s předmětem „aktualizovaná směrnice“, příloha č.j. UOOU-11412/17-9 ze dne 24. ledna 2018, dále viz str. 10 tohoto protokolu o kontrole). Dle této směrnice nesmí zaměstnanec zpřístupnit důvěrné informace zaměstnavatele, klientů nebo jiných osob třetím osobám bez zvláštního svolení (viz odst. 5 směrnice).

Kontrolou na místě byl ověřen postup zaměstnanců zahraničního oddělení [redacted] při vyřizování cizojazyčné elektronické korespondence s potencionálními klientkami [redacted].

- Z údajů vložených zájemcem do webového registračního formuláře je sestavena e-mailová zpráva, která je odeslána na e-mailovou adresu [redacted] (zahraniční oddělení).
- V aplikaci Microsoft Outlook je každá zpráva vložena jednak do sdílené složky doručené pošty, do které mají přístup všechny asistentky [redacted], dále jsou kopie zprávy uloženy v osobních složkách všech asistentek [redacted].
- Příchozí požadavky si asistentky rozdělí (obvykle ráno), a to podle jazyku (angličtina, italština, němčina), v dané skupině pak podle vzájemné dohody, a to tak, že každá asistentka si ve své osobní složce ponechá jen ty zprávy, které bude zpracovávat, ostatní pak smaže, odstraněné položky jsou automaticky přesunuty do složky Odstraněná pošta.
- Při vlastním vyřizování požadavku otevře asistentka v apliakci Outlook novou (prázdnou) zprávu, do které vloží dle druhu požadavku příslušný standardizovaný vzor odpovědi - jsou používány 4 různé vzory (šablony) uložené na Intranetu [redacted]. Tento vzor dle potřeby doplní (personifikuje), např. oslovení, apod. Dále pak do nové zprávy zkopíruje celý obsah přijatého požadavku a z něj zkopíruje e-mailovou adresu adresáta do záhlaví zprávy (pole „Komu“). Takto vytvořená zpráva je pak odeslána žadateli o informace a uložena do složky Odeslaná pošta.
- V současné době neexistuje technické opatření, které by asistentce zabránilo otevřít dva nebo více e-mailů najednou.
- Odpovědi, které jsou uloženy v části odeslaná pošta Outlooku, se mažou automaticky po jednom roce.
- Při odeslání standardizované odpovědi jsou formou přílohy přikládány i obecné informace týkající se činnosti společnosti [redacted]. Tyto přílohy neobsahují nikdy osobní údaje klientů.
- S nově registrovanou klientkou následně komunikuje pouze ta asistentka [redacted], která vyřizovala první kontakt. Po té, co je ukončena činnost v zahraničním oddělení [redacted], je veškerá složka, týkající se jedné klientky předána elektronicky koordinátorce [redacted]. V rámci této složky nejsou zpracovávány informace o zdravotním stavu pacientky.
- Zahraniční oddělení [redacted] zpracovává cca [redacted] požadavků nových (dosud neregistrovaných) zájemců o služby [redacted] měsíčně.

Kontrolou bylo dále zjištěno:

Kontrolovaná osoba na základě Oznámení o zahájení kontroly ÚOOÚ o nesprávném odeslání e-mailu provedla [redacted] vlastní interní šetření, z něhož byl vypracován interní dokument [redacted]. Tento dokument obsahuje rovněž nápravná opatření.
Na základě zjištění z interního šetření byl upraven vnitřní řídící předpis [redacted] Pracovní postup na oddělení [redacted], který nově v části 4.2.1. upravuje povinnost asistentkám [redacted] pracovat jen s jednou konverzací (e-mailem/klientkou).
Kontrolovaná osoba v oblasti ochrany osobních údajů, provádí v rámci celé společnosti včetně zahraničního oddělení [redacted] pravidelně 1x ročně interní audity.

Kontrolovaná osoba po vypracování vlastního zjištění incidentu uskutečnila k nově upraveným pravidlům interní školení, kterého se zúčastnily všechny zaměstnankyně [redacted].

B. Porovnání zjištěného stavu věci s relevantním ustanovením právního předpisu

Kontrolní zjištění č. 1

Dle ustanovení § 4 písm. a) a b) zákona č. 101/2000 Sb. je
a) „*osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*
b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Z podkladů, zaslaných klientkou [redacted] vyplývá, že Kliniku kontaktovala prostřednictvím webového formuláře „Request and Call back“, umístěného na stránkách Kliniky [redacted], Formulář (URL formuláře [redacted] obsahuje následující pole: *Female first name, Female surname, E-mail, Country, Phone, I am interested in, Question.* Následují zaškrtávací políčka *Contact me by e-mail, Contact me by phone, I agree with terms of use.* V zápatí stránky s registračním formulářem je dále uveden copyright [redacted]. Na frázi „*terms of use“* je navázán odkaz na dokument „*Consent to processing of personal data“* (příloha č.j. UOOU-11412/17-10 ze dne 14. února 2018).
Údaje uvedené na webovém formuláři v rozsahu jméno, příjmení, e-mail, země, telefon, jsou identifikačními údaji klienta, které Klinika dále zpracovává, jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť na základě těchto údajů lze identifikovat konkrétní fyzickou osobu.

Kontrolou bylo zjištěno, že v rámci komunikace Kliniky, resp. asistenty [redacted] s klientkou [redacted] došlo [redacted] k neoprávněnému zpřístupnění osobních údajů stěžovatelky [redacted]. prostřednictvím e-mailu zaslaného [redacted], který obsahoval požadavek na doplnění informací, jehož součástí byl e-mail [redacted], který zaslala Klinice a který obsahoval údaje v rozsahu jméno, příjmení [redacted], e-mailovou adresu a telefon, a dále sdělení [redacted] „*Zajímám se o:* [redacted].
Údaje vypovídající o požadované zdravotní péči uvedené na webovém formuláři „Request and Call back“, které Klinika dále zpracovává minimálně za účelem vyřízení požadavku na poskytnutí služeb klientů, jsou údaje vypovídající o zdravotním stavu („*Zajímám se o:* [redacted] – vložený e-mail [redacted], tedy jedná se o citlivé údaje ve smyslu § 4 písm. b) zákona č. 101/2000 Sb., protože jsou osobním údajem vypovídajícím o zdravotním stavu tazatelky.

Kontrolní zjištění č. 2

Dle ustanovení § 4 písm. e) zákona č. 101/2000 Sb. je „*zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“.*

Klinika zpracovává osobní a citlivé údaje klientů shromážděné prostřednictvím webového formuláře „Request and Call back“, zaslané prostřednictvím e-mailu. E-maily, obsahující osobní údaje jsou tříděny do osobní schránky konkrétní zaměstnankyně, která bude dotaz vyřizovat, současně jsou uchovávány v poštovní schránce zahraničního oddělení [redacted], tyto e-maily obsahující osobní a citlivé údaje jsou dále tříděny, ukládány, předávány a dále využívány. Klinika provádí s osobními a citlivými údaji operace, které jsou zpracováním osobních údajů dle § 4 písm. e) zákona č. 101/2000 Sb.,

Kontrolní zjištění č. 3

Dle ustanovení § 4 písm. j) zákona č. 101/2000 Sb. je „*správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak*“.

Klinika je poskytovatelem zdravotní péče ve smyslu zákona č. 372/2011 Sb., účel a prostředky zpracování osobních, resp. citlivých údajů klientů má určeny výše uvedeným zákonem. Ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. je správcem osobních a citlivých údajů klientů, kteří prostřednictvím webového formuláře kontaktují Kliniku za účelem poskytnutí zdravotní služby.

Kontrolní zjištění č. 4

Dle ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. „*Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů“*.

Kontrolou bylo zjištěno, že v rámci komunikace Kliniky, resp. asistenty [redacted] s klientkou [redacted] došlo [redacted] k neoprávněnému zpřístupnění osobních údajů [redacted] prostřednictvím e-mailu zaslaného [redacted], který obsahoval požadavek na doplnění informací, jehož součástí byl e-mail [redacted]. [redacted], který obsahoval údaje v rozsahu jméno, příjmení [redacted], e-mailovou adresu a telefon, a dále sdělení [redacted] „*Zajímám se o:* [redacted]. Neoprávněně byly zpřístupněny osobní a citlivé údaje [redacted]. (potvrzeno Klinikou – [redacted]. [redacted]. [redacted] – příloha č.j. UOOU-11412/17-12 ze dne 5. března 2018).

Systém komunikace s 1. kontaktem, resp. s potenciálním klientem, je dle Kliniky podrobně popsán v dokumentu „Pracovní postup oddělení [redacted] (příloha č.j. UOOU-11412/17-9 ze dne 24. ledna 2018 , dále viz str. 10 tohoto protokolu o kontrole), a to zejména čl. 4.2.1. Asistent [redacted] je dle Pracovního postupu oddělení [redacted] povinen odpovědět adekvátně na otázky klienta. To znamená, že není přípustné, aby se v e-mailu objevily, tj. do e-mailu byly překopírovány z formuláře, údaje jiného klienta, jak se stalo v posuzovaném případě. Je odpovědností příslušné asistentky [redacted], aby před odesláním e-mailu vše zkontrolovala. S Pracovním postupem oddělení [redacted] se tedy zaměstnanci seznamují i několikrát v průběhu pracovního poměru. Seznámení se děje buď formou školení vedoucího zaměstnance, nebo formou obeznámení prostřednictvím e-mailu.

Klinika zaslala přílohou (příloha č.j. UOOU-11412/17-9 ze dne 24. ledna 2018, dále viz str. 10 tohoto protokolu o kontrole) záznam o interním školení ze dne [redacted] v rámci kterého byli zaměstnanci seznámeni s aktuální verzí předmětného pracovního postupu.

V daném případě dle Kliniky asistentka [redacted] patrně pracovala se dvěma e-maily, a tak došlo ke zkopírování údajů z formuláře jedné klientky do odpovědi pro druhou klientku. Jednalo se o pochybení jednotlivce, kterému se nedalo zabránit ani v případě přijetí těch nejpřísnějších opatření. Po zjištění této nežádoucí události Klinika i přes tuto skutečnost instruovala asistentky a koordinátorky oddělení [redacted] v tom směru, že mohou pracovat pouze s jedním kontaktem a před odesláním jsou povinny znovu vložené údaje zkontrolovat.
Kontrolou bylo zjištěno, že byly neoprávněně zpřístupněny osobní a citlivé údaje stěžovatelky, odpovědnost za vzniklý incident má zaměstnankyně Kliniky, která neoprávněně zpřístupnila údaje z webového formuláře jiné osobě, v důsledku čehož došlo k poškození práv stěžovatelky. I přes přijatá technicko-organizační opatření, Klinika nemohla individuálnímu selhání její zaměstnankyně zabránit, asistentka [redacted] nezpracovala osobní, resp. citlivé údaje stěžovatelky za podmínek a v rozsahu stanoveném Klinikou, tedy v rozporu s ustanovením § 14 zákona č. 101/2000 Sb.

Klinika v rámci ústního jednání a místního šetření předložila Zápis z porady ze [redacted] (příloha č.j. UOOU- UOOU-11412/17-12 ze dne 5. března 2018) - zaměstnanci [redacted] byli kromě jiného seznámeni s postupem práce [redacted] – *vždy pracovat jen s jedním otevřeným e-mailovým kontaktem, který je zpracován tak, aby nedošlo k záměně; vždy se ujistit, že adresát je správný a nedojde k úniku dat nebo jeho zaměnění*; postup při odesílání a zaheslování souborů – *důležitá je směrnice o poskytování informací a vydávání zdravotnické dokumentace* [redacted] *Jak dohodnuto je potřeba poslat* [redacted] *jako první dokument, který míří k pacientce a ponechán jen ID pacienta. Následně se všechny soubory, které obsahují osobní data, zaheslovávají v souboru zip a jsou s krátkou instruktáží odeslány pacientovi* – odkaz na intranet Kliniky.

V rámci ústního jednání a místního šetření v provozovně společnosti [redacted], na adrese [redacted], které se konalo dne [redacted], zástupkyně Kliniky popsaly a následně prezentovaly práci asistentek zahraničního oddělení [redacted] při vyřizování příchozích požadavků dosud neregistrovaných zájemců o služby [redacted]:

- z údajů vložených zájemcem do webového registračního formuláře je sestavena e-mailová zpráva, která je odeslána na e-mailovou adresu [redacted] (zahraniční oddělení) – viz printscreen - příloha č.j. UOOU- UOOU-11412/17-12 ze dne 5. března 2018.

- v aplikaci Microsoft Outlook je každá zpráva vložena jednak do sdílené složky doručené pošty, do které mají přístup všechny asistentky [redacted], dále jsou kopie zprávy uloženy v osobních složkách všech asistentek [redacted].
- příchozí požadavky si asistentky rozdělí (obvykle ráno), a to podle jazyku (angličtina, italština, němčina), v dané skupině pak podle vzájemné dohody, a to tak, že každá asistentka si ve své osobní složce ponechá jen ty zprávy, které bude zpracovávat, ostatní pak smaže, odstraněné položky jsou automaticky přesunuty do složky Odstraněná pošta.
- při vlastním vyřizování požadavku otevře asistentka v aplikaci Outlook novou (prázdnou) zprávu, do které vloží dle druhu požadavku příslušný standardizovaný vzor odpovědi - jsou používány 4 různé vzory (šablony) uložené na Intranetu [redacted]. Tento vzor dle potřeby doplní (personifikuje), např. oslovení, apod. Dále pak do nové zprávy zkopíruje celý obsah přijatého požadavku a z něj zkopíruje e-mailovou adresu adresáta do záhlaví zprávy (pole „Komu“). Takto vytvořená zpráva je pak odeslána žadateli o informace a uložena do složky Odeslaná pošta.
- V současné době neexistuje technické opatření, které by asistentce zabránilo otevřít dva nebo více e-mailů najednou.
- Odpovědi, které jsou uloženy v části odeslaná pošta Outlooku, se mažou automaticky po jednom roce.
- Při odeslání standardizované odpovědi jsou formou přílohy přikládány i obecné informace týkající se činnosti společnosti [redacted]. Tyto přílohy neobsahují nikdy osobní údaje klientů.
- S nově registrovanou klientkou následně komunikuje pouze ta asistentka [redacted], která vyřizovala první kontakt. Po té, co je ukončena činnosti v zahraničním oddělení [redacted], je veškerá složka, týkající se jedné klientky předána elektronicky koordinátorce [redacted]. V rámci této složky nejsou zpracovávány informace o zdravotním stavu pacientky.
- Zahraniční oddělení [redacted] zpracovává cca [redacted] požadavků nových (dosud neregistrovaných) zájemců o služby [redacted] měsíčně.

Dále bylo zjištěno, že Klinika na základě Oznámení o zahájení kontroly ÚOOÚ o nesprávném odeslání e-mailu provedla [redacted] vlastní interní šetření, z něhož byl vypracován interní dokument [redacted]. Tento dokument obsahuje rovněž nápravná opatření.
Na základě zjištění z interního šetření byl upraven vnitřní řídící předpis [redacted] Pracovní postup na oddělení [redacted] (příloha č.j. UOOU-11412/17-12 ze dne 5. března 2018), který nově v části 4.2.1. upravuje povinnost asistentkám [redacted] pracovat jen s jednou konverzací (e-mailem) pacienta, tak, že pro odpověď pacientce se nemohou zobrazovat i další rozepsané e-maily. Dále, zástupkyně Kliniky sdělily, že po vypracování vlastního zjištění bylo uskutečněno interní školení k tomuto předpisu – [redacted] Záznam o interním školení, příloha č.j. UOOU-11412/17-12 ze dne 5. března 2018.
Dále, bylo zástupkyněmi Kliniky sděleno, že v oblasti ochrany osobních údajů, a to včetně kontroly zahraničního oddělení [redacted] jsou prováděny pravidelně 1x ročně interní audity.

Na základě výše uvedeného kontrolující konstatují, že Klinikou byly neoprávněně zpřístupněny osobní a citlivé údaje stěžovatelky [redacted], ke zpřístupnění došlo chybou asistentky [redacted], která jako zaměstnankyně Kliniky tímto porušila ustanovení § 14 zákona č. 101/2000 Sb., *kdy zaměstnanec může zpracovávat osobní údaje pouze za podmínek*

a v rozsahu správcem nebo zpracovatelem stanoveném, nikoli na základě Klinikou chybně nastavených opatření ve smyslu § 13 odst. 1 zákona č. 101/2000 Sb.

V uvedeném případě se nejednalo o úmyslné porušení vnitřních pravidel ze strany asistentky [redacted], ale nahodilou lidskou chybu. V daném případě je na Klinice, jako správci osobních, resp. citlivých údajů klientů, aby vyhodnotila možnost doplnění dalšího technicko-organizačního zabezpečení osobních údajů tak, aby minimalizovala možnost lidského pochybení při zpracování osobních, resp. citlivých údajů klientů.

Kontrolní zjištění č. 5

Dle ustanovení § 13 odst. 2 zákona č. 101/2000 Sb.“*Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy“.*

Klinika předložila v rámci kontroly níže uvedené dokumenty:

- **vnitřní předpis** [redacted] **Pracovní postup na oddělení** [redacted] – účelem je upravit a sjednotit činnosti na oddělení [redacted], tento pracovní postup platí pro společnost [redacted]. – konkrétně pro oddělení [redacted] na pobočce [redacted], [redacted]. Čl. 4.2.1 Zpracování 1. kontaktu – stanoveny přesné postupy pro komunikaci s pacientem, založení karty pacientky [redacted] – identifikace pacienta – jméno a příjmení; rodné číslo či číslo pojištěnce, jedná-li se o cizince nepojištěného v ČR, pak datum narození, dle kterého program vygeneruje fiktivní číslo pojištěnce; osobní číslo (vygeneruje program); číslo dokladu totožnosti; rodné příjmení u žen; rodinný stav; adresa trvalého pobytu; telefonní kontakt; e-mail; číslo zdravotní pojišťovny; občanství; důvod proč přichází; odesílající lékař; a další údaje.

  Čl. 4.2.3. Další administrativní činnosti asistentky – vytvoření objednávkového pole [redacted]; vytvoření objednávkového pole [redacted]; …

  Školení zaměstnanců je doloženo dokumentem [redacted] Záznam o interním školení [redacted]. V Záznamu je podpis [redacted], která vyřizovala dotaz [redacted], [redacted].

  Aktualizace směrnic Kliniky zaslána na vědomí všem zaměstnancům Kliniky -e-mail ze [redacted].

- **vnitřní předpis** [redacted] **Řízení informačních systémů** - směrnice stanovuje odpovědnosti, pravomoci a postupy pro řízení výpočetní techniky (SW, HW), včetně požadavků na ochranu dat a údajů tak, aby byl zabezpečen bezpečný provoz kanceláří a laboratoří společnosti [redacted]; směrnice je závazná pro všechny zaměstnance a uživatele souboru výpočetní techniky a počítačové sítě.

- **Organizační řád –** stanoví základní zásady vnitřní organizace společnosti, její organizační strukturu, úkoly a působnost jednotlivých oddělení, zaměstnanců společnosti a jejich vzájemné vztahy. Účelem organizační směrnice, je stanovení působnosti, odpovědností a pravomocí ve společnosti, stanovení povinností

zaměstnanců společnosti ….; směrnice platí pro všechny oddělení společnosti. Čl. 5.4.3.2 [redacted] a [redacted] – činnost tohoto oddělení vede a za jeho činnost odpovídá - vedoucí [redacted] oddělení, přímo podléhající řediteli pobočky. Jeho kompetence jsou specifikovány v Příloze č. 2. Zaměstnanci oddělení jsou asistentky a koordinátorky [redacted]. Povinnosti těchto zaměstnanců jsou specifikovány v Příloze č. 2.

Příloha [redacted] Náplň práce – účelem je obeznámení zaměstnanců s pracovními náplněmi jednotlivých pracovních pozic – asistentka [redacted] – e-mailová a telefonická komunikace s pacienty (první kontakty); zakládání karet; asistence pacientům po klinice [redacted]; práce v systému [redacted] a sledování splatnosti faktur v SW [redacted] …….

- **vnitřní předpis [redacted] Pravidla pro uživatele-[redacted]**

  Dle čl. 5 Důvěrné informace (ať už zaměstnavatele, jeho klientů, nebo jiných osob), nesmějí být zpřístupněny třetím osobám bez zvláštního svolení.

Kontrolou nebylo zjištěno porušení ustanovení § 13 odst. 2 zákona č. 101/2000 Sb.

Kontrolní zjištění č. 6

Dle zjištění kontrolujících, lze kontaktovat Kliniku a provést registraci prostřednictvím registračního formuláře taktéž prostřednictvím vyhledavače seznam.cz [redacted].
Formulář obsahuje pole: *Jméno, Příjmení, Telefon, E-mail, Dotaz* a zaškrtávací políčka *Kontaktovat telefonicky, Kontaktovat e-mailem.* Pod vlastním formulářem „Kontaktujte nás“, je uvedeno pod proklikem „ODESLAT“: „*odesláním formuláře souhlasíte s podmínkami*“, otevřením odkazu „podmínky“dojde k zobrazení dokumentu s informací, že se jedná o internetové stránky společnosti [redacted], zapsané v obchodním rejstříku vedeném Městským soudem v Praze, oddíl [redacted], vložka [redacted]. Společnost [redacted] je členem koncernu [redacted], [redacted], zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl [redacted], vložka [redacted].

Níže v dokumentu uvedeno:

„Souhlas se zpracováním osobních údajů

Zájemce souhlasí se zpracováním svých osobních údajů v rozsahu poskytnutých osobních údajů (dále jen „údaje“) a s jejich zařazením do databáze společnosti [redacted] se sídlem [redacted], zapsané v obchodním rejstříku vedeném Městským soudem v Praze, oddíl [redacted], vložka [redacted], ….., jakožto správce, a s jejich případným zpracováním prostřednictvím zpracovatele, tj. nabízení produktů

a služeb, informování o marketingových akcích, jakož i pro zasílání obchodních sdělení prostřednictvím elektronických prostředků dle zákona č. 480/20004 Sb., o některých službách

informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů, a to do odvolání souhlasu.

Zájemce bere na vědomí, že má práva zaručena zákonem č. 101/2000 Sb. zejména ustanoveními § 9 písm. a), § 11, § 12 a § 21, tj. zejména, že poskytnutí údajů je dobrovolné, že svůj souhlas může bezplatně kdykoli na adrese správce odvolat, že má právo přístupu k osobním údajům a právo na opravu těchto údajů….atd. V případě pochybností o dodržování práv se může obrátit na správce nebo i přímo na Úřad pro ochranu osobních údajů.

Zpracovávané osobní údaje: jméno, příjmení, věk, e-mail. Osobní údaje jsou od zájemce získávány na základě aplikace/webového formuláře, prostřednictvím kterého je subjekt udělí správci. Osobní údaje zájemce budou zpracovávány ve výše uvedeném rozsahu v elektronické databázi správce, popř. zpracovatelem, se kterým správce uzavře příslušnou smlouvu. Veškerá data jsou ukládána v digitální formě.

Požádá-li zájemce o informaci o zpracování osobních údajů, je mu správce a případně i zpracovatel povinen tuto informaci bez zbytečného odkladu předat. Správce……

Tento souhlas může zájemce kdykoli písemně odvolat.

S odesláním dotazníku zájemce souhlasí se zveřejněním otázky a odpovědi".

V zápatí stránky s formulářem je uveden copyright [redacted].

V rámci přípisu Žádost o součinnost ze dne 20. února 2017, č.j. UOOU-11412/17-11 byla od Kliniky vyžádána písemná informace, z jakého důvodu je souhlas se zpracováním osobních údajů klientů Kliniky udělován společnosti [redacted], [redacted] (viz [redacted] a [redacted]. Písemná informace byla předána kontrolujícím při ústním jednání a místním šetření [redacted] (viz příloha č.j. UOOU-11412/17-12 ze dne 5. března 2018).

Klinika předložila písemnou informaci, podepsanou generální ředitelkou Kliniky [redacted], [redacted], [redacted] (viz příloha č.j. UOOU-11412/17-12 ze dne 5. března 2018), z níž vyplývá, že společnost [redacted], se sídlem [redacted], [redacted], je jediným společníkem [redacted], [redacted]. Společnost [redacted], [redacted]. vyvíjela v roce [redacted] master web, na který byl umístěn souhlas se zpracováním osobních údajů s jejími identifikačními údaji. Tento master web společnost [redacted]. převzala a dále si jej upravila na míru. Společnost [redacted]. měla dle Kliniky patrně zajišťovat marketingové aktivity a nabízení služeb v rámci skupiny [redacted], přičemž od tohoto záměru se při spuštění webu upustilo. Na webu Kliniky však došlo k administrativní chybě,

kdy Klinika při převzetí a spuštění webu nevyměnila u souhlasu se zpracováním osobních údajů informace týkající se identifikace správce osobních údajů. Dále uvedeno, že k marketingovým, ani jiným účelům uvedeným v souhlasu, nebyly údaje klientů zpracovávány (kromě nabízení již klientem poptaných zdravotních služeb) a údaje nebyly ani zpřístupňovány společnosti [redacted], na základě souhlasů tedy údaje zpracovány nebyly.

Kontrolující dne [redacted] ověřili na webových stránkách [redacted] společnosti [redacted]. aktuální znění dokumentů „Souhlas se zpracováním osobních údajů" v českém, anglickém, italském a německém jazyce. Bylo zjištěno, že v aktuální verzi je souhlas poskytován společnosti [redacted]. [redacted]: [redacted] – viz ÚZ ze dne 7. března 2018, č.j. UOOU-11412/17-14 a příloha – soubory [redacted].

Kontrolující konstatují, že Klinika v průběhu kontroly zajistila úpravu souhlasu k zpracování osobních údajů za účelem nabízení produktů a služeb ve smyslu § 5 odst. 5 a násl. zákona č. 101/2000 Sb., předkládaného klientům prostřednictvím webových stránek tak, že případný souhlas je poskytován skutečně Klinice, nikoli společnosti [redacted]. Současně bylo zjištěno, že Klinika nezasílá nabízení produktů a služeb a tudíž souhlas se zpracováním osobních údajů za účelem nabízení produktů a služeb nikdy nevyužila.

C. Uvedení podkladů, ze kterých kontrolní zjištění vycházejí:
Spisová dokumentace č.j. UOOU-11412/17.

Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může Kontrolovaná osoba podat kontrolnímu orgánu 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.

Pokud kontrolující inspektorka nevyhoví námitkám ve lhůtě 7 dnů ode dne jejich doručení, vyřídí je předsedkyně Úřadu ve lhůtě 30 dnů ode dne jejich doručení.

Protokol o kontrole je vypracován ve dvou vyhotoveních. Jedno vyhotovení bude doručeno, společnosti [redacted], [redacted]. se sídlem [redacted], [redacted], formou stejnopisu, druhé vyhotovení bude založeno jako originál s podpisem kontrolujících v kontrolním spisu čj. UOOU-11412/17. V tomto spisu jsou rovněž založeny všechny podklady (dokumenty, úřední záznamy apod.) uvedené ve sběrném archu kontrolního spisu pod pořadovým číslem 1-17.
V rámci této kontroly bylo kontrolujícími kontrolováno a prověřováno výhradně zpracování osobních údajů v čase provedení kontroly uvedeném v tomto protokolu o kontrole a v rozsahu stanoveném předmětem kontroly.

Podpisová doložka:

Kontrolující:

otisk
úředního
razítka

PaedDr. Jana Rybínová	inspektorka	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis
JUDr. Michal Jelínek	pověřený zaměstnanec Úřadu	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis
Ing. Max Gůt	pověřený zaměstnanec Úřadu	*(dokument podepsán elektronicky)*
…….		……..
jméno		podpis