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-01824/20-9
Praha 23. září 2020

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.

Kontrolující:

Mgr. et Mgr. Božena Čajková – inspektorka Úřadu, č. průkazu: [redacted] jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze dne 23. června 2020;

Bc. Hana Imiolková – pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze dne 23. června 2020;

Josef Polák – pověřený zaměstnanec Úřadu pro ochranu osobních údajů, č. průkazu: [redacted],

Ing. David Mrňák, DiS, – pověřený zaměstnanec Úřadu pro ochranu osobních údajů, č. průkazu: [redacted]

Kontrolovaná osoba:

[redacted] zastoupená [redacted] pověřencem pro ochranu osobních údajů, jmenovaného dne 13. března 2018

(dále také „[redacted]“ nebo „společnost“)

Předmět kontroly:

Předmětem kontroly je zpracování osobních údajů při provozování aplikace [redacted] se zaměřením na postavení kontrolované osoby a plnění na něj navazujících povinností stanovených nařízením (EU) 2016/679, zejména pak v čl. 5, 6, čl. 12 až 23, čl. 25 a čl. 28 až 32 tohoto nařízení.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-01824/20-2, které bylo doručeno kontrolované osobě dne 3. června 2020.

Poslední kontrolní úkon:

Podklady doručené Úřadu dne 21. srpna 2020 dle požadavku kontrolujících z ústního jednání a místního šetření konaného dne 28. července 2020, čj. UOOU-01824/20-8).

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. oznámení o zahájení kontroly čj. UOOU-01824/20-2, doručené kontrolované osobě dne 3. června 2020, počet listů 2;
2. poskytnutí součinnosti nezbytné pro posouzení plnění povinností, které jsou předmětem kontroly ze dne 16. června 2020, čj. UOOU-01824/20-5, počet listů 7, přílohy:
   2.1. příloha – 001.001.200.600.000.000.000 Zásady ochrany osobních údajů.pdf, počet listů 10,
   2.2. příloha – 002.000.000.600.001.000.000 Zacházení s daty zákazníků.pdf, počet listů 6,
   2.3. příloha – 002.000.000.600.001.000.005 Pověřenec pro ochranu osobních údajů a Koordinátor pro ochranu osobních údajů (en).pdf, počet listů 4,
   2.4. příloha – 002.000.000.600.001.000.010 Naplnění práv subjektu údajů.pdf, počet listů 6,
   2.5. příloha – 002.000.000.600.001.000.011 Posouzení vlivu na ochranu osobních údajů.pdf, počet listů 6,
   2.6. příloha – 002.000.000.600.001.000.020 Pověřené zpracování a TOM (en).pdf, počet listů 8,
   2.7. příloha – 002.000.000.600.001.000.024 Záznamy o činnostech zpracování (en).pdf, počet listů 2,

2.8. příloha – 002.000.000.600.001.000.030 Porušení zabezpečení osobních údajů.pdf, počet listů 5,
2.9. příloha – 002.000.000.600.001.000.040 Pravidla ochrany osobních údajů v produktech [redacted] (en).pdf, počet listů 4,
2.10. příloha – 002.000.000.600.001.000.042 Export dat (přenositelnost dat) (en).pdf, počet listů 2,
2.11. příloha – 002.000.000.600.001.000.045 Autorizační koncept (en).pdf, počet listů 6,
2.12. příloha – 002.000.000.600.001.000.050 Audit ochrany osobních údajů (en).pdf, počet listů 5,
2.13. příloha – 002.000.000.600.001.000.104 Hromadná korespondence mimo skupinu [redacted] pdf, počet listů 4,
2.14. příloha – [redacted].pdf, počet listů 1,
2.15. příloha – [redacted] pdf, počet listů 3,
2.16. příloha – Implementace GDPR v systému [redacted] pdf, počet listů 5,
2.17. příloha – INTERNÍ AUDIT GDPR 2019.11.pdf, počet listů 12,
2.18. příloha – INTERNÍ AUDIT ČSN EN 82304 [redacted] pdf, počet listů 15,
2.19. příloha – ISO 9001_2015 CZ_[redacted] CR.pdf, počet listů 1,
2.20. příloha – ISO_IEC 20000-1_2011 CZ_[redacted] CR.PDF, počet listů 1,
2.21. příloha – Jmenování pověřence pro ochranu osobních údajů.pdf, počet listů 1,
2.22. příloha – Koncept vymazání pro produkty [redacted] (en).pdf, počet listů 12,
2.23. příloha – Licenční podmínky [redacted] pdf, počet listů 1,
2.24. příloha – Obchodní podmínky [redacted] pdf, počet listů 2,
2.25. příloha – Politika bezpečnosti informací.pdf, počet listů 7,
2.26. příloha – Prohlášení o ochraně osobních údajů v produktu [redacted] pdf, počet listů 2,
2.27. příloha – Prohlášení o závazku zachování důvěrnosti a dodržování ochrany osobních údajů.pdf, počet listů 2,
2.28. příloha – Seznam operací zpracování (ne)podléhajících požadavku na DPIA.pdf, počet listů 8,
2.29. příloha – Skartace zdravotnické dokumentace – [redacted] pdf, počet listů 4,
2.30. příloha – Smlouva o zpracování osobních údajů (převod dat) v2.0 VZOR.pdf, počet listů 4,
2.31. příloha – Smlouva o zpracování osobních údajů v1.0 VZOR.pdf, počet listů 4,
2.32. příloha – Smlouva o zpracování osobních údajů v2.0 VZOR.pdf, počet listů 4,
2.33. příloha – Technická a organizační opatření.pdf, počet listů 9,
2.34. příloha – Uplatnění práv subjektů údajů podle čl. 15 EU-2016-679 (proces) (en).pdf, počet listů 3,
2.35. příloha – Uplatnění práv subjektů údajů podle čl. 17 EU-2016-679 (proces) (en).pdf, počet listů 3,
2.36. příloha – Uživatelská příručka [redacted] pdf, počet listů 867, uloženo elektronicky,
2.37. příloha – Základní informace o systému [redacted] pdf, počet listů 3,
2.38. příloha – Zásady zpracování a ochrany osobních údajů v [redacted] pdf, počet listů 5,

3. protokol z ústního jednání a místního šetření konaného dne 28. července 2020, čj. UOOU-01824/20-7, počet listů 4;
4. Doložení požadovaných dokumentů dle protokolu z ústního jednání a místního šetření konaného dne 28. července 2020, ze dne 21. srpna 2020, čj. UOOU-01824/20-8, počet listů 1, přílohy:

4.1. příloha – Přehled realizovaných školení GDPR.png; počet listů 1;
4.2. příloha – 2019-04-29 Školení ochrany osobních údajů.pdf; počet listů 3;
4.3. příloha – 2020-07-27 Školení ochrany osobních údajů-v9-20200813_141028.pdf; počet listů 1;
4.4. příloha – 2020-08-18 Školení ochrany osobních údajů-v14-20200821_164839.pdf; počet listů 1;
4.5. příloha – [redacted]základní GDPR školení[redacted] CZ 2020.xlsx; počet listů 2;
4.6. příloha – 002.000.000.600.001.000.024 Záznamy o činnostech zpracování.pdf; počet listů 2;
4.7. příloha – 002.000.000.600.001.000.028 Záznamy o činnostech zpracování - adresář zpracování.xlsx; počet listů 9;
4.8. příloha – VVT_[redacted] xlsx., počet listů 5.

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 kontroly:

Kontrola byla zahájena na základě kontrolního plánu Úřadu pro rok 2020, zaměřila se na postavení kontrolované osoby jako dodavatele ambulantního informačního systému [redacted] (dále jen „systém [redacted] poskytovatelům zdravotních služeb a dodržování povinností stanovených v nařízení (EU) 2016/679 v souvislosti s poskytováním služeb při provozování tohoto systému.

III. Kontrolní zjištění:

Kontrolní zjištění č. 1:

Kontrolující předně posuzovali, zda informace, které kontrolovaná osoba v souvislosti s poskytováním služeb při provozování systému [redacted] klienty (poskytovateli zdravotních služeb) zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, podle kterého se osobním údajem rozumí *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*. A dále, zda dochází i ke zpracování zvláštních kategorií osobních údajů, kterými jsou dle čl. 9 odst. 1 nařízení (EU) 2016/679 osobní údaje *„vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání*

či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby".

Současně kontrolující hodnotili, zda jsou tyto údaje zpracovávány ve smyslu čl. 4 bod 2) nařízení (EU) 2016/679, podle kterého *„je zpracováním osobních údajů jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení".*

Kontrolou bylo zjištěno, že systém [redacted] je komplexní informační software určený pro všechny typy poskytovatelů ambulantní péče a menší poskytovatele zdravotních služeb (pro vedení kompletní pacientské dokumentace a související administrativy). Obsahuje veškeré manažerské přehledy související s chodem ordinace, včetně správy financí. Zajišťuje elektronickou komunikaci. Systém [redacted] obsahuje databázový server (databáze [redacted] a klientskou aplikaci pro uživatele poskytovatele zdravotních služeb. Lze ho provozovat jak lokálně (na jednom PC), tak v síťové verzi v rámci lokální počítačové sítě (LAN). Data jsou uchovávána vždy pouze v databázovém serveru (hlavní PC), který spravuje poskytovatel zdravotních služeb. Systém umožňuje nastavení různých uživatelských oprávnění (rolí) na jejichž základě mají jednotliví pracovníci (lékař, sestra, administrativní pracovník atd.) přístup k daným částem systému. Systém disponuje nadstavbovými moduly, jež nejsou součástí základní licence systému a musí být zákazníkem objednány dodatečně. (podklad č. 2.)

Kmenová data poskytovatele zdravotních služeb a jeho zaměstnanců jsou v systému [redacted] ukládána z důvodu souladu s právními požadavky na činnosti prováděné v tomto systému a jeho modulech (vedení zdravotnické dokumentace, řízení přístupu k ní, vyúčtování zdravotní péče, vykazování statistik, vytváření elektronické preskripce a podobně), jsou odpovídajícím způsobem označena a zahrnují následující informace:

Název a adresu ordinace

- Typ ordinace
- IČO, DIČ a IČZ subjektu (ordinace)
- Údaje o pracovištích poskytovatele zdravotních služeb, zejména odbornosti, IČP, lokality, ordinační doby
- Poskytované služby
- Data související s lékařem/Provozovatelem lékařské praxe
    - Oslovení/Titul
    - Křestní jméno/Příjmení
- Informace o pracovnících poskytovatele zdravotních služeb (zaměstnanci, popřípadě majitel ordinace):
    - Příjmení, křestní jméno,
    - Uživatelské jméno/bezpečný hash hesla
    - Kontaktní údaje (telefon, e-mail adresa, jiné adresy a identifikátory pro elektronickou komunikaci)
    - U lékařů pak odbornost lékaře, evidenční číslo lékaře v ČLK

- Osobní přístupové údaje do systémů třetích stran. Tyto jsou v systému ukládány v šifrované podobě. Jde například o přístupové údaje do Centrálního úložiště elektronické preskripce (SÚKL) nebo přístupy pro předávání dávek do zdravotních pojišťoven.
- Otisk osobního kvalifikovaného certifikátu (podklad č. 2.)

Poskytovatelé zdravotních služeb v systému [redacted] vedou zdravotnickou dokumentaci pacienta v elektronické podobě, zpracovávají jeho osobní údaje, včetně zvláštních kategorií osobních údajů v souladu s § 54 zákona č. 372/2011 Sb., zákona o zdravotních službách. Dle uvedeného ustanovení lze vést zdravotnickou dokumentaci v listinné nebo elektronické podobě nebo v kombinaci obou těchto podob.

V systému [redacted] jsou k danému účelu vedeny následující kategorie osobních údajů:

- Osobní údaje a údaje o zdravotním stavu (včetně rodinné a sociální anamnézy, v případě potřeby etnický původ a genetické údaje) za účelem řádného vedení zdravotnické dokumentace k poskytované zdravotní péči, plnění povinností při poskytování zdravotních služeb
- Osobní údaje a informace o pojištění pacienta u zdravotní pojišťovny za účelem vyúčtování zdravotní péče
- Osobní údaje pacientů a kontaktní údaje (e-mail, telefon), termín a důvod objednávky za účelem zefektivnění přijímání pacientů v ordinaci a využití pracovní doby ordinace
- Daňové doklady a na nich uvedené osobní údaje pacientů z důvodu řádného vedení daňových dokladů

V systému mohou být nad rámec těchto základních účelů zpracovávány i jiné údaje pacientů. Zákonnost těchto zpracování, popřípadě nutnost souhlasu pacientů s konkrétním účelem zpracování je odpovědností správce osobních údajů, tedy poskytovatele zdravotních služeb. Údaje o pacientech jsou shromažďovány a vkládány do informačního systému v rámci dokumentace péče o pacienta personálem poskytovatele zdravotních služeb.

Evidovanými osobními údaji jsou:

- Osobní údaje (křestní jméno, příjmení, titul před nebo za jménem, rodné příjmení, datum a místo narození, věk, pohlaví, rodné číslo, státní občanství, číslo občanského průkazu, stav)
- Adresa trvalá a kontaktní (Ulice, číslo domu, poštovní směrovací číslo, město, země)
- Telefonní číslo, e-mailová adresa
- Informace o plátci zdravotní péče a typu pojištění (zdravotní pojišťovna, číslo pojištěnce)
- Soukromé zdravotní pojištění
- Praktický lékař, ošetřující lékař, v případě předání pacienta do péče dalším lékařem i doporučující lékař
- Údaje o zaměstnání (povolání, zaměstnavatel, adresa)
- Informace o osobě blízké (jméno, adresa, telefonní kontakt)
- Doplňující informace (krevní skupina, kuřák, příbuzní, zbrojní průkaz, řidičský průkaz, ZTP, v evidenci od-do, historie osobních údajů) (podklad č. 2. a 2.36.)

Údaje o zdravotní péči pacienta jsou zvláštní kategorií osobních údajů a jsou předmětem vyšší ochrany v rámci obecného nařízení o ochraně osobních údajů.

Integrace dat do lékařských záznamů pacienta je dána zákonem stanovenou povinností ošetřujícího lékaře zaznamenávat a dokumentovat veškerá vyšetření a postupy léčby a jednotlivé výsledky podstatné pro současnou a budoucí léčbu pacienta.

Tato data zahrnují:

- Anamnézy
- Alergie
- Výška, hmotnost, krevní skupina
- Diagnózy
- Vyšetření
- Výsledky vyšetření
- Nálezy
- Terapeutická ošetření a jejich výsledky
- Operační zákroky a jejich výsledky
- Medikace pacienta
- Lékařské a ošetřovatelské zprávy, další zdravotnická dokumentace

Dle výše citované definice je pro posouzení povahy informace jako osobního údaje základním kritériem možnost přiřazení této informace ke konkrétní fyzické osobě. S ohledem na výše popsaný rozsah informací, které uživatelé poskytovatele zdravotních služeb do systému [redacted] k jednotlivým pacientům a výše uvedeným kmenovým datům poskytovatele zdravotních služeb vkládají a obecně s ohledem na účel tohoto systému, kterým je vedení evidence pacientů a informací o poskytovaných zdravotních službách, je pak zřejmé, že prostřednictvím systému [redacted] dochází ke zpracování **osobních údajů** a **zvláštních kategorií osobních údajů** (informací o zdravotním stavu ve smyslu čl. 4 bod 1) a čl. 9 odst. 1 nařízení (EU) 2016/679.

Kontrolovaná osoba uzavírá se zákazníkem (poskytovatelem zdravotních služeb) systému [redacted] smlouvy o zpracování osobních údajů za účelem poskytování uživatelské podpory formou vzdáleného přístupu (podklad č. 2.32.) a o převodu dat (podklad č. 2.30.), případně uzavírá servisní smlouvy (podklad č. 2.31., 2.32. a 3.).
Společnost [redacted] je tak na základě smluv zmocněna k tomu, aby pro poskytovatele zdravotních služeb (správce) zpracovávala osobní údaje, které jí správce za účelem poskytování služby zpřístupní, a to pouze na základě pokynů daného správce upravených v rámci zpracovatelských smluv (popř. jejích písemných dodatků).
Kontrolovaná osoba na základě výše uvedeného **zpracovává osobní údaje, včetně údajů zvláštní kategorie** ve smyslu definice uvedené v čl. 4 bod 1), čl. 9 odst. 1 a bod 2) nařízení (EU) 2016/679.

Kontrolní zjištění č. 2:

Kontrolující se dále zabývali postavením kontrolované osoby ve vztahu k čl. 4 bod 8) nařízení (EU) 2016/679, v nichž je uvedena definice správce a zpracovatele osobních údajů. Správcem se přitom rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“.* Zpracovatelem je pak *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“.*

Jak bylo již uvedeno výše, kontrolovaná osoba dodává svým zákazníkům – poskytovatelům zdravotních služeb (správcům) systém [redacted] jakožto nástroj pro plnění jejich zákonné povinnosti vést zdravotnickou dokumentaci, popř. k zajištění dalších činností souvisejících s provozem poskytovatele zdravotních služeb. Povinnosti spojené se zpracováním osobních údajů, ke kterému prostřednictvím tohoto systému dochází, tak vyplývají ze zvláštních právních předpisů, zejména zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování.

Kontrolovaná osoba v souvislosti s dodávkou systému [redacted] poskytovatele zdravotních služeb uzavírá smlouvu o zpracování osobních údajů (podklad č. 2.32.), za účelem poskytování uživatelské podpory formou vzdáleného přístupu nebo osobní návštěvy ve vztahu k ambulantnímu informačnímu systému poskytovatele zdravotních služeb, dále uzavírá smlouvu o převodu dat (podklad č. 2.30.), která upravuje převod dat z původního lékařského software správce do ambulantního informačního sytému nově poskytnutého správci společností [redacted] S velkými poskytovateli zdravotních služeb pak může být uzavřena i tzv. servisní smlouva, která obsahuje ze strany [redacted] i pravidelné kontroly serverů nebo přístup jiným způsobem než prostřednictvím nástroje [redacted] ([redacted]). (podklad č. 2.30., 2.31., 2.32. a 3.)

Konkrétně poskytuje kontrolovaná osoba poskytovatelům zdravotních služeb na základě uzavřených smluv (podklad č. 2.30. a 2. 32.) službu spočívající v zajištění technické podpory. Činnost kontrolované osoby pak fakticky spočívá především v poskytování vzdálené technické podpory. Povaha činnosti kontrolované osoby není tedy přímo založena na zpracování osobních údajů pacientů při jejich shromažďování či dalším využívání, nicméně poskytované služby jsou pro zajištění předmětného zpracování údajů nezbytné. Při poskytování vzdálené technické podpory může nicméně v některých případech a v návaznosti na pokyn příslušného správce kontrolovaná osoba na osobní údaje nahlížet, případně provádět s daty další úkony (převod dat či jiné úpravy).

Kontrolující proto dle výše uvedeného konstatují, že kontrolovaná osoba je v postavení **zpracovatele** osobních údajů podle čl. 4 bod 8) nařízení (EU) 2016/679, neboť na základě smluvních ujednání zpracovává osobní údaje pro správce – poskytovatele zdravotních služeb.

Kontrolní zjištění č. 3:

V návaznosti na závěry předchozích kontrolních zjištění se kontrolující dále zabývali tím, zda jsou pro účast zpracovatelů na předmětném zpracování splněny podmínky čl. 28 odst. 1 nařízení (EU) 2016/679, dle kterého lze využít pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření směřujících k zajištění souladu s požadavky citovaného nařízení. Zapojení dalších zpracovatelů na straně zpracovatele je pak dle čl. 28. odst. 2 nařízení (EU) 2016/679 možné pouze s předchozím svolením správce. Činnost zpracovatelů se dále musí řídit smlouvou, jejíž parametry jsou definovány v čl. 28 odst. 3 nařízení (EU) 2016/679.

Úvodem je třeba konstatovat, že plnění těchto povinností primárně dopadá na správce osobních údajů, zde tedy na jednotlivé poskytovatele zdravotních služeb. V daném případě však tito správci svoji základní odpovědnost za zpracování osobních údajů realizují fakticky pouze rozhodnutím o tom, že budou při své činnosti využívat produkt poskytovaný kontrolovanou osobou – systémem [redacted]

Kontrolovaná osoba z pozice zpracovatele osobních údajů uzavírá s jednotlivými správci (zákazníky ambulantního systému [redacted] standardně následující typy smluv:

- Licenční podmínky (podklad č. 2.23.)
- Obchodní podmínky (podklad č. 2.24.)
- Smlouva o zpracování osobních údajů za účelem poskytování uživatelské podpory formou vzdáleného přístupu pomocí aplikace [redacted] nebo formou osobní návštěvy za účelem efektivního řešení dotazů a reportovaných problémů ve vztahu k ambulantnímu informačnímu systému Klienta (poskytovatele zdravotních služeb) (dále také „smlouva vzor 1“) (podklad č. 2.31.), tj. poskytování uživatelské podpory formou vzdáleného přístupu nebo osobní návštěvy ve vztahu k ambulantnímu informačnímu systému poskytovatele zdravotních služeb.
- Smlouva o zpracování osobních údajů za účelem poskytování uživatelské podpory formou vzdáleného přístupu pomocí aplikace [redacted] nebo formou osobní návštěvy za účelem efektivního řešení dotazů a reportovaných problémů ve vztahu k ambulantnímu informačnímu systému Klienta (poskytovatele zdravotních služeb) (dále také „smlouva vzor 2“) (podklad č. 2.32.), tj. poskytování služeb provozní a uživatelské podpory aplikačního programového vybavení.
- Smlouva o zpracování osobních údajů za účelem převodu dat, opravy databáze, analýzy databáze apod. (dále jen „smlouva o převodu dat“) (podklad č. 2.30.)

Správce a zpracovatel uzavírají smlouvy vzor 1 a vzor 2 a smlouvu o převodu dat (dále jen „zpracovatelské smlouvy“), jejichž předmětem je úprava vztahů mezi správcem a zpracovatelem a určení jejich práv a povinností při zpracování osobních údajů zpracovatelem a v souvislosti s ním, zejména pak vymezuje jednotlivé kategorie osobních údajů a kategorie subjektu údajů, které bude zpracovatel zpracovávat, prostředky a účel, pro který bude osobní údaje zpracovávat, dobu zpracování osobních údajů, jakož i podmínky a záruky zpracovatele z hlediska technického a organizačního zabezpečení ochrany osobních údajů tak, aby zpracování probíhalo v souladu s právními předpisy v oblasti ochrany osobních údajů.

Kontrolou bylo zjištěno, že kontrolovaná osoba zpracovatelskými smlouvami naplňuje povinnosti uvedené v čl. 28 odst. 2 a 3 nařízení (EU) 2016/679.

Ve zpracovatelských smlouvách jsou zejména upraveny tyto náležitosti:

- Rozsah osobních údajů a kategorie subjektů údajů
- Popis přijatých technických a organizačních opatření
- Podmínky pro přístup zaměstnanců [redacted] (kontrolovaná osoba jako zpracovatel nesmí předchozího prokazatelného výslovného souhlasu anebo pokynu správce, na základě dokumentovaných instrukcí správce, zpracovávané osobní údaje upravit nebo pozměnit, třídit nebo kombinovat, zpřístupnit ani předat třetí osobě, šířit ani zveřejňovat, ani jakýmkoli způsobem použít pro vlastní potřebu, ledaže takové zpracování vyžadují závazné právní předpisy. Pokud subjekt údajů kontaktuje přímo [redacted] za účelem opravy, vymazání nebo omezení zpracování, předá zpracovatel neprodleně požadavek správci. V rozsahu, v jakém je to zahrnuto v rozsahu služeb, budou postup vymazávání, „právo na zapomenutí“, oprava, přenos údajů a přístup zajišťovány [redacted] a to bez zbytečného odkladu na základě dokumentovaných instrukcí správce).
- Záznamy o činnostech zpracování v rozsahu čl. 30 citovaného nařízení
- Podmínky pro využití subdodavatele kontrolovanou osobou (další smluvní zpracovatele)
- Dozorová oprávnění klienta (poskytovatele zdravotních služeb)
- Postupy po ukončení platnosti zpracovatelských smluv
- Pravidla vymazání a vrácení osobních údajů poskytovateli zdravotních služeb– správci.

Po zhodnocení obsahu předložených smluv proto kontrolující konstatují, že spolupráce správců (poskytovatelů zdravotních služeb) a zpracovatele (kontrolované osoby) je nastavena způsobem, který odpovídá požadavkům čl. 28 odst. 2 a 3 nařízení (EU) 2016/679, čímž je dán i předpoklad k závěru, že **nedochází k porušení** základní povinnosti vyjádřené v odst. 1 citovaného nařízení.

Kontrolní zjištění č. 4:

Kontrolující dále hodnotili, zda je pro zpracování osobních údajů, které je předmětem této kontroly, dán právní titul, jak je požadováno v čl. 6 odst. 1 a ve vztahu ke zvláštním kategoriím osobních údajů současně i v čl. 9 odst. 2 nařízení (EU) 2016/679 (při zpracování zvláštních kategorií osobních údajů je nutné, aby správce disponoval jak některým z obecných právních titulů pro zpracování osobních údajů dle čl. 6 odst. 1, tak i právním titulem pro zpracování zvláštních kategorií údajů dle čl. 9 odst. 2 citovaného nařízení).

Jak bylo již uvedeno, správci osobních údajů zpracovávaných pomocí systému [redacted] jsou jednotliví poskytovatelé zdravotních služeb. Těmto subjektům je příslušnými právními předpisy (zejména zákonem č. 372/2011 Sb.) uložena povinnost vést zdravotnickou dokumentaci pacientů, a to ve stanoveném rozsahu. Správci osobních údajů tak při vedení zdravotnické dokumentace postupují v souladu s čl. 6 odst. 1 písm. c) a čl. 9 odst. 2 písm. h) nařízení (EU) 2016/679, neboť předmětné zpracování osobních údajů, včetně zvláštních kategorií, realizují z důvodu své právní povinnosti.

Kontrolovaná osoba pak, jakožto zpracovatel, vlastním právním titulem disponovat nemusí, resp. jeho oprávnění zpracovávat předmětné osobní údaje se odvozuje od právního titulu správce. Samostatný právní titul by byl nezbytný pouze za předpokladu, kdy by kontrolovaná osoba překročila rámec smluvního vztahu se správcem (tj. zpracovával by zpřístupněné osobní údaje za jiným účelem, než jaký definoval správce, čímž by se stal ve vztahu k této činnosti sám správcem).

Kontrolující tedy konstatují, že **nebylo zjištěno** porušení povinností uvedených v čl. 6 a čl. 9 nařízení (EU) 2016/679, jelikož osobní údaje a zvláštní kategorie osobních údajů pacientů, které jsou zpracovávány pomocí systému [redacted] jsou zpracovávány na základě zákonem předpokládaných právních titulů.

Kontrolní zjištění č. 5:

Kontrolující rovněž hodnotili roli kontrolované osoby jako zpracovatele při vyřizování žádostí subjektů údajů spojených se zpracováním osobních údajů prostřednictvím systému [redacted] a to zejména s ohledem na splnění povinností uvedených v čl. 12, 15 a 17 nařízení (EU) 2016/679. Podle těchto ustanovení má subjekt údajů právo požádat správce o přístup k jeho osobním údajům (tj. poskytnutí informace o tom zda a jaké osobní údaje o něm zpracovává), právo na to, aby správce za definovaných okolností jeho osobní údaje bez zbytečného odkladu vymazal, a právo obdržet informace o opatřeních, která správce přijal v návaznosti na žádost subjektu údajů (uplatněnou podle čl. 15 až 22 citovaného nařízení), a to bez zbytečného odkladu a v každém případě do jednoho měsíce po obdržení žádosti.

Pověřenec pro ochranu osobních údajů ke dni 28. července 2020 obdržel celkem tři žádosti ze strany subjektu údajů v souvislosti s uplatněním práv subjektů údajů podle nařízení (EU) 2016/679, pouze dvě žádosti (ze dne 3. a 11. června 2020) se týkaly předmětného zpracování (podklad č. 2.).

V souvislosti s uplatněním práv subjektů údajů podle nařízení (EU) 2016/679 má kontrolovaná osoba vypracovaný postup při vyřizování těchto žádostí na základě podmínek stanovených ve zpracovatelských smlouvách (spolupráce s poskytovateli zdravotních služeb), a dle standardních procesů [redacted]

Kontrolovaná osoba vždy žadatele informuje o přijetí žádosti (požadavku). V případě, že je [redacted] v postavení:

- zpracovatele, informuje žadatele o zamítnutí žádosti z důvodu tohoto postavení a připojí kontakt na příslušného správce. Zároveň je žádost subjektu údajů postoupena danému správci.
- správce, informuje žadatele o přijetí žádosti a žádost začne podle interních postupů zpracovávat. (podklad č. 2.)

Kontrolovaná osoba postupovala při vyřizování uvedených stížností podle výše uvedených postupů a procesů.

S ohledem na uvedené kontrolující konstatují, že při vyřizování žádostí subjektu údajů (pacientů) kontrolovaná osoba **plní** povinnosti stanovené v citovaných ustanovení nařízení (EU) 2016/679, které jí vyplývají z jejího postavení zpracovatele v rámci předmětného zpracování.

Kontrolní zjištění č. 6:

Kontrolující dále ověřili, zda kontrolovaná osoba vede záznamy o činnostech zpracování dle čl. 30 odst. 2 nařízení (EU) 2016/679.

Kontrolovaná osoba uvádí, že všechny její obchodní jednotky jsou povinny vést záznamy o činnostech zpracování a evidovat je v tzv. adresáři zpracování, který je přílohou směrnice Záznamy o činnostech zpracování (podklad č. 4.6. a 4.7.).

Tyto záznamy jsou vedeny podle čl. 30 odst. 2 nařízení (EU) 2016/679, a to písemně i v elektronické formě (ve formátu Excel). Směrnice obsahuje postupy při vedení záznamů o činnostech, stanovuje odpovědnost například general managera a manažerů centrálních služeb za udržování záznamů o činnostech zpracování v souladu s touto směrnicí a za její aktuálnost a věcnou správnost a pověřenci pro ochranu osobních údajů odpovědnost za kvalitu pořízených záznamů.

Kontrolovaná osoba v pozici zpracovatele **vede** záznamy o činnostech zpracování, které obsahují veškeré informace uvedené **v čl. 30 odst. odst. 2 písm. a) – d) nařízení (EU) 2016/679** (podklad č. 4.6., 4.7. a 4.8.).

Kontrolní zjištění č. 7:

Kontrolující dále posuzovali, zda kontrolovaná osoba přijala vhodná technická a organizační opatření k zabezpečení osobních údajů zpracovávaných v rámci systému [redacted] jak je jeho povinností dle čl. 32 nařízení (EU) 2016/679. Z citovaného ustanovení vyplývá komplex povinností ve vztahu k zajištění bezpečnosti zpracovávaných osobních údajů, a to jak po organizační, tak po technické stránce, včetně příslušné dokumentace provedených opatření, přičemž tyto povinnosti se vztahují jak na poskytovatele zdravotních služeb v pozici správce, tak i na společnost [redacted] jako zpracovatele.

Kontrolou bylo zjištěno, že technická a organizační opatření, přijatá za účelem zajištění bezpečnosti zpracovávaných osobních údajů, kontrolovaná osoba zdokumentovala ve vnitropodnikových předpisech společnosti [redacted] (viz podklad dokumenty označené 2.1.-2.38)

Kompletní znění technických a organizačních opatření je upraveno v dokumentu Technická a organizační opatření.pdf. (podklad č. 2.33.) Společnost [redacted] je součástí skupiny

[redacted] na jejíž infrastruktuře mohou být provozovány některé vnitropodnikové systémy. Za součást svých technických a organizačních opatření považuje [redacted] i technická a organizační opatření celé skupiny. (podklad č. 2.)

Uvedeným dokumentem kontrolovaná osoba dokládá naplňování povinností stanovených dle čl. 32 odst. 1, písm. b) nařízení (EU) 2016/679, jsou v něm upravena technická a organizační opatření zaměřující se na řízení ochranu dat společnosti [redacted]

V jednotlivých částech dokumentu jsou upraveny následující oblasti řízení ochrany dat:
v části 1. Důvěrnost informací

- řízení fyzického přístupu – bezpečnostní opatření budovy, jejich prostor a nájemních prostor
- systém řízení přístupu k zařízením zpracovávající osobní údaje
  - Zařízení používané k zpracování osobních údajů jsou zabezpečeny pomocí řízeného přístupu. Za prvé to se týká ochrany lokálního přístupu, jako je například přístup chráněný heslem na úrovni operačního systému, nebo přístup chráněný na úrovni čipové karty. Přístup zaměstnanců přes čipovou kartu není využíván, zaměstnanci se přihlašují pouze přes uživatelské jméno a heslo. V síťovém prostředí je ošetřen bezpečný přístup i prostřednictvím sítě. Jsou zajištěny požadavky na zvýšenou ochranu zejména při připojení k internetu. Zajištění bezpečnosti je obvykle prováděno prostřednictvím brány firewall, antivirů atd. Zařízení používané k zpracování osobních údajů a jiné prostředky ochrany dat jsou udržovány pravidelně aktualizované.
  - uspořádání pracoviště
  - identifikace a ověřování uživatelů
    Identifikace a ověřování uživatelů na klientských zařízeních a v aplikacích je zajištěno unikátním uživatelským ID a heslem. Po 15 minutách nečinnosti uživatele, je vynuceno automatické uzamčení obrazovky pracovní stanice. Zamčená obrazovka je odemčena pouze při zadání odpovídajícího uživatelského
  - jednotné přihlášení / předávání uživatelského hesla
  - zásady hesel
    Zásady hesel v rámci [redacted]
    Jsou přijaty vnitřní směrnice definující minimální požadavky na délku a složitost uživatelských hesel – Zásady informační bezpečnosti [redacted] Bezpečnost uživatelských hesel je zajišťována pomocí odpovídající délky, platnosti a počtu generací hesel. Dodržování konvencí hesel je vynucováno přímo systémovými nastaveními.
  - vzdálený přístup zaměstnanců
    [redacted]
  - opravy a údržby

Opravy a údržby prováděné externími dodavateli služeb jsou realizovány pouze za dohledu odborného personálu společnosti. Pro opakující se činnosti údržby je stanoven plán údržby.

Jestliže jsou IT zařízení obsahující osobní údaje předány mimo společnost [redacted] jsou všechna osobní data uložena na samostatném médiu a před vlastním předáním jsou tato osobní data vymazána nebo jinak odstraněna z předávaného zařízení.

- systém řízení přístupu k datům
  Předmětem systému řízení přístupu k datům je především kontrola oprávnění pro přístup k osobním datům. K osobním datům je udělen přístup pouze oprávněným osobám (zaměstnancům [redacted] jež z příkazu zaměstnavatele provádí zpracování osobních údajů. Pouze oprávněný uživatel (zaměstnanec [redacted] může přistupovat k osobním údajům subjektů, nedochází k neoprávněnému čtení, kopírování, pozměňování nebo odstranění zpracovávaných osobních údajů.
  - správa systému
- oddělení kontroly
  Shromážděné osobní údaje jsou pro různé účely zpracovány odděleně, a to pomocí logického a fyzického oddělení.

v části 2 Integrita:

- prohlášení o řízení (přenosu / uchování / vymazání)
  [redacted]
- řízení vstupů
  V závislosti na proporcionalitě je realizováno automatické protokolování vstupů. Protokolování probíhá na úrovni auditních souborů nebo databázových tabulek.
  Součástí protokolování jsou:
  - Dotčené záznamy osobních údajů
  - Druh činnosti (vytvoření, změna, smazání záznamu osobních údajů)
  - Datum a čas činnosti nebo události
  - Uživatelské ID osoby, která data zpracovávala

v části 3 Dostupnost a odolnost

- připravenost provozu
  IT systémy jsou nepřetržitě monitorovány prostřednictvím příslušných prostředků. Je zaveden systém včasného varování.
  - [redacted]

[redacted]

v části 4 Postupy pro periodické přezkoumání, posuzování a hodnocení jsou zejména upraveny:

- postupy a odpovědnost pověřených osob v oblasti řízení ochrany dat (členové rady, všichni generální manažeři a v dozorové roli i pověřenci pro ochranu osobních údajů),
- sankce za nedodržení postupů dle vnitřních pokynů společnosti [redacted]
- monitorovací procesy
- správa objednávek včetně objednávek importu dat
- správa objednávek – služba vzdálené správy

[redacted]

- [redacted]

- správa objednávek – import dat
  Import zákaznických dat je obecně zakázán a podléhá schválení zákazníkem (poskytovatelem zdravotních služeb). Import zákaznických dat je proto povolen pouze ve výjimečných případech, pouze jménem zákazníka a pouze za určitých podmínek stanovených v interním dokumentu Technická a organizační opatření
  Jiné formy dohody nejsou povoleny. Zákaznická data jsou přenášena pouze v zašifrované podobě a pouze na chráněné serverové uložiště. Ukládání neanonymních zákaznických dat na pracovní stanice, notebooky nebo externí přenosné paměťové médium je přísně zakázáno. Během procesu analýzy je původní datový nosič zákazníka (poskytovatele zdravotních služeb) uložen na bezpečném místě. Všechny datové nosiče obsahující zákaznická data jsou explicitně označeny tak, aby je bylo možné identifikovat. Každý zaměstnanec [redacted] účastnící se procesu analýzy je povinen v podobě Ticketu neprodleně dokumentovat svou činnost a uskutečněné zpracování zákaznických dat v [redacted] systému, a to bez uvedení jakýchkoliv osobních údajů. Ticket v systému [redacted] je v „otevřeném“ stavu do doby, dokud nejsou všechny data bezpečně zničena nebo vrácena zpět zákazníkovi (poskytovateli zdravotních služeb). Na konci procesu, jsou všechna data odstraněna. Nadřízený zaměstnance [redacted] provádějícího zpracování je zodpovědný za dodržení se zákazníkem (poskytovatele zdravotních služeb) předem dohodnutých lhůt pro vymazání. Po dohodě se zákazníkem je původní datový nosič bezpečně zničen nebo vrácen zpět zákazníkovi (poskytovateli zdravotních služeb).
- bezpečnostní kniha importu dat
  Kromě řádného dokumentování provedených činností v podobě Ticketů v [redacted] systému, byla zřízená za účelem vedení podrobnější dokumentace importů dat a jejich zpracování bezpečnostní kniha. Jedná se o vázanou knihu uchovávanou v tištěné podobě.
- správa incidentů
  Opatření popisované v pokynech zajišťují:
  - Včasné rozpoznání bezpečnostního incidentu tak, aby jeho dopad byl minimální nebo v omezené možné míře
  - Bezpečnostní incidenty jsou hlášeny jednotným a centralizovaným způsobem
  - Je zaveden strukturovaný a časově nenáročný proces svázaný s jasně definovanými
  - zodpovědnostmi v případě vzniku incidentu. Jsou popsány první kroky a postupy pro mimořádné události a výpadky, pořadí informování odpovědných osob, postupy pro restart, hierarchie eskalací v organizační struktuře.
  - Incidenty jsou srozumitelně dokumentovány, ohodnoceny a analyzovány
  - Zamezení opakování incidentů je dosaženo přijmutím odpovídajících opatření
- Privacy by Default
- Certifikace.

Kontrolovaná osoba má vypracovány taktéž dokumenty týkající se zásad ochrany osobních údajů, konkrétně Zásady ochrany osobních údajů ze dne 20. září 2019 (směrnice) (podklad č. 2.1.) a Zásady ochrany osobních údajů v [redacted] ze dne 27. července 2019 (podklad č. 2.38.)

Směrnice Zásady ochrany osobních údajů (podklad č. 2.1.) upravuje způsob, jakým [redacted] zachází s osobními údaji jejich zákazníků. Účelem je zajistit konzistentní a vysokou úroveň ochrany osobních údajů v rámci [redacted] SE a v rámci všech obchodních jednotek [redacted] v Evropě a zajistit dodržování příslušných zákonů o ochraně osobních údajů. Dále pak stanovit základní pravidla pro zacházení s osobními údaji a stanovit organizaci ochrany osobních údajů. Vztahuje se na všechna zpracování osobních údajů zákazníků (poskytovatelů zdravotních služeb), partnerů, dodavatelů, zaměstnanců, akcionářů a dalších zúčastněných stran, jakož i na údaje zákazníků a klientů zákazníků [redacted] (např. zákazníků, pacientů, klientů, zaměstnanců, rodinných příslušníků pacientů, obchodních partnerů apod.). Směrnice je rozdělena do několika částí, přičemž v části F této směrnice je uveden postup k dodržování zásad zpracování osobních údajů:

F.1 zásady zpracování osobních údajů
- transparentnost (čl. 5 odst. 1, písm. a) nařízení (EU) 2016/679 – zásada zákonnosti, korektnosti a transparentnosti)
- vyčlenění (čl. 5 odst. 1, písm. b) nařízení (EU) 2016/679 – zásada účelového omezení)
- minimalizace údajů (čl. 5 odst. 1, písm. c) nařízení (EU) 2016/679)
- kvalita dat (čl. 5 odst. 1, písm. d) nařízení (EU) 2016/679 – zásada přesnosti)
- důvěrnost
- automatizované rozhodování

F.2 přípustnost zpracování údajů
- zpracování osobních údajů
- zpracování citlivých osobních údajů
- zpracování osobních údajů pro reklamní účely

F.3 předávání osobních údajů
F.4 zpracování dat v zastoupení
F.5 práva subjektu údajů
F.6 důvěrnost zpracování
F.7 bezpečnost zpracování
F.8 pořízení hardwaru a softwaru
F.9 odpovědnosti a sankce
F.10 řízení ochrany dat (organizace ochrany dat)
- pověřenec pro ochranu osobních údajů a koordinátoři pro ochranu osobních údajů
- povinnosti zaměstnanců a školení
- informační povinnost při porušení
- kontrolní procesy
- spolupráce s dozorovým úřadem

F.11 změny zásad ochrany osobních údajů.

Dokument Zásady ochrany osobních údajů v [redacted] (podklad č. 2.38.) je prohlášením společnosti o ochraně a zpracování osobních údajů, slouží k naplnění zákonem stanovené informační povinnosti poskytování informací o nakládání s osobními údaji v rámci [redacted]

Dokument Politika bezpečnostních informací ze dne 3. dubna 2020 (podklad č. 2.25.) je směrnice, která vymezuje pravidla a požadavky ve vztahu k bezpečnému a spolehlivému provozu firemní IT infrastruktury. Smyslem směrnice a jejího soustavného uplatňování je chránit [redacted] před škálou nežádoucích událostí včetně podvodu, zpronevěry, průmyslové

špionáže, sabotáže, výpadku a nedostupnosti interních IT systémů včetně systémů poskytovaných zákazníkům. Směrnice rovněž vymezuje minimální kontrolní mechanismy nezbytné k prevenci právních problémů, například obvinění z nedbalostního jednání, porušení fiduciární povinnosti nebo ochrany osobních údajů, a základní pravidla, s nimiž musí být seznámeni a jimiž se musí soustavně řídit jak zaměstnanci společnosti [redacted] tak její dodavatelé i další obchodní partneři.

Směrnice s názvem Naplnění práv subjektů ze dne 28. března 2018 (podklad č. 2.4.) upravuje v části F postup při uplatňování práv subjektu údajů dle čl. 15 – 23 nařízení (EU) 2016/679:

F.1 právo být informován o zpracování osobních údajů
F.2 ostatní práva (všeobecné informace)
F.3 právo na přístup k osobním údajům
F.4 právo na opravu
F.5 právo na výmaz (právo být "zapomenut")
F.6 právo na přenositelnost údajů
F.7 právo vznést námitku proti zpracování
F.8 právo na omezení zpracování
F.9 právo nebýt předmětem automatizovaného individuálního rozhodování
F.10 právo odvolat souhlas
F.11 právo podat stížnost u dozorového úřadu.

[redacted] se v dokumentu Prohlášení o ochraně osobních údajů v produktu [redacted] (podklad č. 2.26.) zavazuje k přísnému dodržování všech příslušných právních předpisů a norem týkajících se ukládání a zpracování osobních údajů. [redacted] tímto implementovala centrální systém řízení ochrany dat, který zajišťuje trvalou a vysokou úroveň ochrany osobních údajů ve všech společnostech [redacted] v souladu s příslušnými právními předpisy. Toto prohlášení o ochraně dat slouží k naplnění zákonem stanovené informační povinnosti poskytování informací o nakládání s daty v rámci [redacted] Toto prohlášení o ochraně dat se týká výslovně [redacted]
V bodě 7. tohoto prohlášení se zaměřuje na bezpečnostní opatření / zabránění riziku, [redacted] přijímá veškerá technická a organizační bezpečnostní opatření za účelem zajištění ochrany osobních údajů před neoprávněným přístupem, úpravami, zveřejněním, ztrátou, zničením nebo jinými způsoby zneužití. Tato opatření zahrnují interní testování a kontroly našich procesů shromažďování dat, ukládání a zpracování. Dále zahrnují bezpečnostní opatření na ochranu informačních systémů, na kterých kontrolovaná osoba ukládá smluvní údaje a data z technických operací, před neoprávněnými přístupy.
V bodě 8. Technická a organizační opatření je uvedeno, že k zajištění ochrany údajů provádí [redacted] pravidelný průzkum stavu vývoje v oblasti bezpečnostních technologií.
Včetně specializovaného penetračního testování, které je prováděno formou pravidelných testů, posuzování a vyhodnocování účinnosti těchto technických a organizačních bezpečnostních opatření, která zajišťují bezpečnost zpracování dat.
Následující pokyny upravují implementaci vhodných technických a organizačních opatření:

- Zálohování dat (ordinace)
  Za účelem zamezení ztrátám dat jsou data pravidelně zálohována.
- Ochrana soukromí
  [redacted] zajišťuje, aby byly ochrana údajů/soukromí a zásady ochrany údajů zohledněny v návrhu a vývoji procesů informačních systémů.

- Ochrana soukromí
  [redacted] systém [redacted] dodává s továrním nastavením, které je optimalizováno na ochranu dat (jsou zpracovávány pouze osobní údaje nezbytné k danému účelu).
- Komunikace prostřednictvím e-mailu (lékařská praxe/[redacted]
  [redacted] upozorňuje, že komunikace prostřednictvím e-mailu nesplňuje požadované zásady ochrany předávaných informací (obsah e-mailových zpráv může být viděn třetími stranami).
- Vzdálená správa
  Zaměstnanci a subdodavatelé [redacted] mohou mít přístup k údajům o pacientovi nebo zákazníkovi a v určitých případech také k údajům o lékařské praxi. Tento přístup se řídí obecnými pravidly [redacted]
  - Vzdálený přístup k administraci je ve výchozím nastavení uzamčen a je udělován pouze poskytovatelům zdravotních služeb.
  - Hesla k přístupu do informačního systému poskytovatele zdravotních služeb jsou vydávána pouze za účelem vzdálené správy systému.
  - Kritické zásahy jsou zabezpečeny principem 4 očí s další kvalifikovanou osobou.
  - Používané nástroje vzdálené správy, které vyžadují aktivní potvrzení přístupu poskytovatele zdravotních služeb, což umožňuje poskytovateli zdravotních služeb sledovat prováděné zásahy.
  - Přístup formou vzdálené správy je zaznamenáván do systému. Zaznamenávána jsou následující data: odpovědné osoby, datum a čas, délka trvání, cílový systém, nástroj vzdálené správy, stručný popis úkonů a v případě kritických zásahů také jméno (jména) další kvalifikované osoby v případě použití principu 4 očí.
  - Zaznamenávání relací vzdálené správy je zakázáno.

Technickou podporu poskytuje kontrolovaná osoba svým klientům (poskytovatelům zdravotních služeb**)** dálkově, a to za použití aplikace [redacted] Poskytování vzdálené podpory je možné pouze ze služebního vybavení (pracovní stanice, notebook).
V rámci práce z domova lze využít i tablet a mobilní telefon splňující následující technické požadavky:

- Zařízení musí používat následující operační systémy: Android nebo IOS
- Minimální podporovaná verze se nachází na webové stránce [redacted] website (Our People > [redacted] > Our services > Mobile / Naši lidé > IT skupina > Naše služby > Mobilní).
- Zařízení musí ukládat všechna hesla uložená uživatelem v šifrovaném úložišti hesel.
- Zařízení musí být konfigurováno s bezpečným heslem, nejméně PIN kódem se 4 znaky, které se musí měnit každých 90 dnů. Historie hesel bude ukládat posledních pět hesel.
- Zařízení musí být konfigurováno tak, aby se po uplynutí 15 minut zamkla obrazovka vašeho mobilního zařízení.
- Zařízení musí být konfigurováno tak, aby se ztracené nebo ukradené zařízení vymazalo.
- Zařízení musí být konfigurováno tak, aby se resetoval PIN.
- Zařízení musí být konfigurováno tak, aby se zamykalo.
- S výjimkou zařízení řízených IT není u těchto zařízení dovoleno, aby se připojovala přímo do interní podnikové sítě.
- Zařízení musí mít možnost šifrování interní paměti.

Požadavky na uživatele (zaměstnance [redacted]

- Uživatelé smí do svých mobilních zařízení stahovat pouze data nutná pro jejich funkci.
- Pokud má uživatel podezření, že dochází k neoprávněnému přístupu k datům společnosti prostřednictvím mobilního zařízení, musí takový incident nahlásit v souladu s procesem řešení incidentů [redacted]
- Zařízení nesmí být „jailbreakována“, „rootována“, ani nesmí být instalován žádný software/firmware, který je navržen tak, aby získal přístup k funkcím, jež nejsou určeny pro uživatele.
- Uživatelé nesmí na svá zařízení nahrávat pirátský software ani nezákonný obsah.
- Aplikace musí být instalovány pouze z oficiálních zdrojů schválených majitelem platformy. Instalace kódu z nedůvěryhodného zdroje je zakázána. Pokud si nejste jistí, jestli aplikace pochází ze schváleného zdroje, kontaktujte IT odbor Skupiny [redacted]
- Zařízení musí být aktualizována opravami dodávanými výrobcem nebo sítí. Opravy by měly být kontrolovány minimálně jednou týdně a aplikovány alespoň jednou za měsíc.
- Zařízení nesmí být připojena do počítače, který nemá aktuální a aktivní ochranu proti malwaru a který není v souladu s podnikovou politikou.
- Zařízení musí být šifrována v souladu se standardy dodržování předpisů ze strany [redacted]
- Uživatelé musí být opatrní při slučování osobních a pracovních e-mailových účtů na svých zařízeních. Velkou pozornost musí věnovat zejména zajištění, aby byla data společnosti zasílána pouze podnikovým e-mailovým systémem. Pokud má uživatel podezření, že jsou data společnosti odeslána z osobního e-mailového účtu, buď jako text nebo jako příloha, musí neprodleně informovat IT odbor [redacted]
- Uživatelé nesmí používat a ukládat dokumenty [redacted] u externích poskytovatelů cloudových úložišť (např. Dropbox, Google Drive, OneDrive, atd.).

Obsah mobilních zařízení (zaměstnanců [redacted] je šifrovaný a chráněný přístupovým PINem nebo biometrickou identifikací (otisk prstu). Obsah mobilních telefonů lze v případě ztráty pomocí vzdálené správy vymazat.

Požadavky na hesla zaměstnanců kontrolované osoby:

- platnost: 90 dnů
- minimální délka: 8 znaků
- složitost struktury: velké písmeno, malé písmeno, číslice a nejméně jeden speciální znak
- historie hesel: posledních 24 hesel
- zablokování účtu: po pěti neúspěšných pokusech o přihlášení po sobě
- možnost nového přihlášení: po 30 minutách nečinnosti nebo po zásahu správce systému
- uzamknutí relace: po 15 minutách nečinnosti, chráněno heslem (podklad č. 3.)

Opatření ze strany uživatelů (zaměstnanců kontrolované osoby):

- Uživatel nesmí své heslo nikomu sdělovat (ani nadřízenému či spolupracovníkům).
- Uživatel nesmí ukládat hesla v jakýchkoliv počítačových souborech, přihlašovacích skriptech a jiných programech, pokud není heslo uloženo v šifrované podobě ve schváleném šifrovacím nástroji (např. KeePass).

- Správci systému ani ostatní pracovníci úseku IT nesmí nikdy po uživateli vyžadovat jeho heslo. Sdělení hesla jiné osobě je uživateli povoleno pouze v jediné situaci, a to při vydání prvotního hesla. Uživatel je povinen si dočasně přidělené heslo neprodleně při následujícím přihlášení změnit.
- Má-li uživatel za to, že jeho uživatelské jméno a heslo používá jiná osoba, je povinen své podezření okamžitě oznámit oddělení [redacted]
- Původní, dodavatelem technického nebo aplikačního vybavení nastavené heslo se musí změnit dle požadavků [redacted] na bezpečnost hesel ještě před tím, než se systém začne využívat v produkci.
- Uživatel je povinen uzamknout pracovní stanici před jejím opuštěním. (podklad č. 3.)

V rámci technických a organizačních opatření jsou pořádána pravidelná školení zaměstnanců pověřených zpracováním osobních údajů. Kontrolovaná osoba pořádá pravidelně dvakrát ročně pro stávající zaměstnance školení o ochraně osobních údajů. Jedním z nich je prezenční školení, prováděné pověřencem pro ochranu osobních údajů a druhé je e-learningového školení. Nově přijatí zaměstnanci jsou proškoleni ihned po svém nástupu do zaměstnání, včetně e-learningové školení a také se seznamují se všemi vnitropodnikovými směrnicemi. (podklady č. 2., 3. a 4.-4.5.)

[redacted] provádí kontrolu dodržování zásad ochrany osobních údajů ve formě interních a externích auditů jehož předmětem je mimo jiné audit ochrany osobních údajů. (podklad č. 2.17., 2.18. a 3) Tyto kontroly provádí [redacted] v podobě pravidelných a nepravidelných auditů. Pravidelné audity se uskutečňují jednou ročně a zaměřují se na kontrolu plnění všech zásad ochrany osobních údajů, oproti nepravidelným auditům zaměřeným na konkrétní zásady ochrany osobních údajů (podklad č. 3.)

V roce 2020 byl systém [redacted] auditován na soulad s požadavky normy ČSN EN 82304-1 – Zdravotnický software – Část 1: Obecné požadavky na bezpečnost produktů. (podklad č. 2.18.) [redacted] je držitelem certifikátů ISO 9001:2015 v oblasti vývoje, prodeje, implementace, servisu a provozování informačních systémů pro zdravotnictví (podklad č. 2.19.) a ISO 20000-1:2011 v oblasti systému řízení IT služeb v oblasti podpory a provozování informačních systémů pro zdravotnictví (podklad č. 2.20).

Povinnost mlčenlivosti
Všichni zaměstnanci [redacted] zapojení do činnosti zpracování osobních údajů klienta (poskytovatele zdravotních služeb) jsou povinni mít uzavřen dodatek pracovních smluv (Prohlášení o závazku zachování důvěrnosti a dodržování ochrany osobních údajů.pdf.) (podklad č. 2.27.)

[redacted] jako jedno z organizačních opatření jmenovala pověřence pro ochranu osobních údajů. (podklad č. 2.21.)
Pověřenec pro ochranu osobních údajů zajišťuje pravidelná školení zaměstnanců zpracovávající osobní údaje.

Zacházení s daty zákazníků (poskytovatelů zdravotních služeb) – vzdálený přístup:
Ke vzdálené správě počítače pomocí aplikace [redacted] je nutná součinnost daného poskytovatele zdravotních služeb. Poskytnutí vzdálené podpory tak vždy předchází

komunikace kontrolované osoby s daným poskytovatelem zdravotních služeb, jehož pracovník musí spustit aplikaci [redacted] na svém PC a následně sdělit zástupci kontrolované osoby připojovací kód a heslo pro spuštění vzdálené správy. Nezbytné úpravy tak kontrolovaná osoba provádí fakticky na PC klienta (uživatele poskytovatele zdravotních služeb), v rámci jeho uživatelského účtu. Využití aplikace [redacted] je na straně kontrolované osoby částečně logováno, uchovávány jsou logy vypovídající o tom, kdy byla podpora provedena, jak dlouho trvala a z kterého zařízení byla provedena (podklad č. 2.33., 3.)
V rámci vzdáleného přístupu má technik přístup jen dle rozsahu uživatelských práv toho, kdo mu umožňuje přihlášení ze strany správce přes vzdálenou podporu. (podklad č. 3.)

Každé připojení je zaznamenáno v informačním systému [redacted] Zaznamenávanými údaji jsou:

- identifikace správce (generováno automaticky)
- identifikace zaměstnance, který hovor přijal (generováno automaticky)
- datum a čas přijetí (generováno automaticky)
- trvání připojení
- médium, které se připojilo na vzdálenou podporu (generováno automaticky)
- popis úkonu, který technik provedl. (podklad č.3.)

Pokud by docházelo k velkému zásahu do databáze zákazníků je třeba splnit tzv. princip čtyř očí. Zásahy do databáze klienta (uživatelů poskytovatele zdravotních služeb) (správce) se neuskutečňují, výjimkou je například oprava poškozené databáze. (podklad č. 3)
Vždy je snahou [redacted] aby veškeré činnosti prováděl samotný správce na základě slovního pokynu zaměstnance [redacted] s výjimkou výjimečných případů, jako např. zásah do databáze, které vyžadují zvláštní odbornost. (podklad č. 3.)

S velkými poskytovateli zdravotních služeb může být uzavřena i tzv. servisní smlouva, která může obsahovat ze strany [redacted] i pravidelné kontroly serverů nebo přístup jiným způsobem než prostřednictvím nástroje [redacted] ([redacted]). (podklad č. 3.)

Jak bylo uvedeno v kontrolním zjištění č. 1, systém [redacted] lze provozovat jak lokálně (na jednom PC), tak v síťové verzi v rámci lokální počítačové sítě (LAN). Data jsou uchovávána vždy pouze v databázovém serveru (hlavní PC). Přístup do systému aplikace je možný na základě přihlašovacího jména a hesla.

Ochrana osobních údajů je v systému [redacted] řešena v těchto specifických oblastech:

- šifrování hesel
- protokolizace použití systému
- informace o osobních údajích pacienta zpracovávaných ordinací
- ověření pacienta při telefonickém rozhovoru
- zabezpečení přístupu k zdravotní dokumentaci pacienta
- doporučení k šifrování dat a práci s bezpečnostní zálohou.

Evidování činnosti uživatelů v systému [redacted] pomocí logů činnosti je dle kontrolované osoby nastaven nativně (základní logy jsou vždy nastaveny). S nabytím účinnosti nařízení (EU) 2016/679 přijala kontrolovaná osoba opatření, ve kterém stanovila, že všechny konfigurační prvky týkající se ochrany osobních údajů jsou ve výchozím nastavení nastaveny na podporu ochrany osobních údajů. Mezi tyto prvky patří například síla hesel, rozšíření logování, veškerá

hesla a uživatelská jména týkající se připojení do systému třetích stran (SUKL, ČSSZ). Uvedené prvky jsou zašifrované pomocí hesla uživatele, tzn. ani jiný lékař v rámci jedné organizace se nemůže k heslům dostat. Správce si však může upravit toto nastavení. (podklad č. 3.)

Zálohování dat v systému [redacted]
V zálohách, ve kterých jsou obsaženy osobní údaje subjektů údajů, které již mají být vymazány z důvodu uplynutí doby od změny poskytovatele, dle vyjádření [redacted] neexistuje automatické upozornění pro správce o nutnosti smazat tyto osobní údaje i z ostatních záloh. Do budoucna [redacted] plánuje rozšířit funkcionalitu, která by uživatele poskytovatele zdravotních služeb upozornila na nutnost odstranit osobní údaje i ze všech existujících záloh. V samotném programu [redacted] existuje skartační koncept, který správce informuje, jaké údaje, jaké pacienty má vymazat z programu. (podklad č. 3.)

V rámci zabezpečení osobních údajů, které [redacted] zpracovává, byla zavedena a přijata vhodná opatření pro zajištění úrovně zabezpečení odpovídající danému riziku.

Na základě výše uvedených skutečností dospěli kontrolující k závěru, že kontrolovaná osoba plní povinnosti dle čl. 32 nařízení (EU) 2016/679, **porušení nebylo shledáno**.

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:

otisk
úředního
razítka

Mgr. et Mgr. Božena Čajková	inspektorka Úřadu	*(podepsáno elektronicky)* podpis
Bc. Hana Imiolková	pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis
Josef Polák	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Ing. David Mrňák, DiS	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis