

Smlouva o zpracování osobních údajů

Všeobecná fakultní nemocnice v Praze

se sídlem: U Nemocnice 499/2, PSČ: 128 08, Praha 2
 IČO: 000 64 165 DIČ: CZ00064165
 zastoupená: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem

(dále též „**Nemocnice**“)

a

Lekis s.r.o.

zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě pod spisovou značkou C 9921
 se sídlem: Těšínská 1349/296, Ostrava – Radvanice 716 00
 IČO: 25356089 DIČ: CZ25356089
 zastoupená: xxxxx, na základě plné moci

(dále též „**Zpracovatel**“)

(Zpracovatel a Nemocnice dále též souhrnně jako „**smluvní strany**“)

Smluvní strany uzavírají níže uvedeného dne, měsíce a roku dle čl. 28 nařízení EU č. 2016/679, obecného nařízení o ochraně osobních údajů (dále také jen „**GDPR**“) a příslušných ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „**zákon**“) tuto

SMLOUVU O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

(dále též „**smlouva**“)

I. Předmět smlouvy

- Nemocnice je ve smyslu GDPR správcem osobních údajů, neboť v souvislosti se svojí činností zejména v oblasti poskytování zdravotních služeb zpracovává osobní údaje, včetně údajů o zdravotním stavu, genetických a biometrických údajů (dále jen „osobní údaje“) svých pacientů, zaměstnanců, popřípadě dalších osob (dále všichni jen „subjekty údajů“). Právním základem zpracování osobních údajů je zejm. splnění právní povinnosti, která se na správce vztahuje, popř. oprávněný zájem správce.
- Zpracovatel poskytuje Nemocnici na základě smlouvy č. PO 95/S/26, případně dalších smluv (dále jen „původní smlouvy“) mj. následující služby: zajištění a podporu provozu informačních systémů Nemocnice, resp. zajištění a podporu provozu vybraných informačních technologií. Seznam aplikačního SW, seznam dotčených technických prostředků a specifikace poskytovaných služeb jsou uvedeny v příloze č. 1 výše uvedené původní smlouvy.
- V rámci poskytování uvedených služeb zpracovává Zpracovatel osobní údaje, jejichž správcem je Nemocnice.
- Zpracovatel je ve smyslu GDPR osobou, která poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření při provádění zpracování osobních údajů, a to tak, aby nedocházelo k překračování právního rámce vymezujícího možnost takového zpracování.
- Smluvní strany mají zájem upravit touto smlouvou svá vzájemná práva a povinnosti při zpracování osobních údajů podle čl. 28 GDPR.

II. Definice

- Osobním údajem se 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.
- Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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.
- Další pojmy používané v této smlouvě mají totožný význam, jako pojmy užívané v GDPR, ev. mají význam, který je jim přisuzován jinými závaznými právními předpisy.

III. Předmět, povaha a účel zpracování

- Předmětem zpracování osobních údajů ve smyslu čl. I. a II. této smlouvy je zejména:
 - přístup Zpracovatele k osobním údajům v rámci zajištění podpory provozu a rozvoje SW řešení,
 - zpracování osobních údajů zaměstnanci Zpracovatele během výkonu činnosti vyplývající z původní smlouvy.

2. Osobní údaje jsou zpracovávány jak automatickým způsobem bez lidského zásahu (např. automatická tvorba reportů na základě databáze osobních údajů), tak i manuálně (např. ruční opravy chyb v datech) v elektronické i papírové podobě. Účelem tohoto zpracování osobních údajů je zajištění chodu uvedených informačních systémů.
3. Zpracovatel není oprávněn zpracovávat osobní údaje za jiným účelem, než který mu byl stanoven Nemocnicí prostřednictvím původní smlouvy a této smlouvy.

IV. Typy zpracovávaných osobních údajů a kategorie subjektů

1. Předmětem zpracování jsou následující typy osobních údajů:
 - osobní údaje pacientů a údaje ze zdravotnické dokumentace předávané v rámci datového rozhraní.
2. Kategorie subjektů údajů:
 - zaměstnanci Nemocnice,
 - pacienti Nemocnice,
 - klienti lékáren Nemocnice.

V. Doba trvání zpracování osobních údajů

Zpracovatel zpracovává osobní údaje dle čl. III. a IV. po dobu nezbytnou, nejdéle však po dobu zpracování a uchování patientských záznamů definovaných původní smlouvou.

VI. Práva a povinnosti Zpracovatele

1. V souladu s čl. 28. odst. 3 GDPR Zpracovatel zejména:
 - a) zpracovává osobní údaje výhradně na základě původní smlouvy, této smlouvy a doložených pokynů Nemocnice, a v souladu s GDPR;
 - b) plní bezodkladně veškeré pokyny udělené mu Nemocnicí ve vztahu ke zpracování osobních údajů, například přerušení zpracování osobních údajů, jejich úprava, výmaz či vydání kopie;
 - c) zajišťuje, že se jeho zaměstnanci a případně další osoby mající přístup k osobním údajům Nemocnice zavázaly k mlčenlivosti;
 - d) přijme veškerá opatření stanovená článkem 32 GDPR, která jsou blíže stanovena v odst. 3 tohoto článku;
 - e) udržuje technická a organizační opatření blíže popsaná v příloze č. 1. - Pokyny pro zpracovatele osobních údajů, aby nemohlo dojít k neoprávněnému přístupu k předmětným osobním údajům, jejich neoprávněné změně, zničení či ztrátě, jakož i k jinému zneužití.
 - f) poskytne Nemocnici, příp. třetí straně pověřené Nemocnicí nebo státnímu orgánu veškerou součinnost nezbytnou ke kontrole činností Zpracovatele vykonávaných na základě původní smlouvy a/nebo této smlouvy. V této souvislosti Zpracovatel bez zbytečného odkladu poskytne zejména informace, dokumenty, přístup do svých prostor a ke svým zařízením a dá k dispozici své relevantní zaměstnance;
 - g) poskytne Nemocnici veškerou součinnost nezbytnou pro včasné vyřízení uplatnění práva subjektu údajů ve smyslu zejm. článků č. 15 až 22 GDPR způsobem stanoveným v Pokynech pro zpracovatele osobních údajů;
 - h) je Nemocnici nápomocen při zajišťování souladu s jeho povinnostmi podle článků 32 až 36 GDPR;
 - i) je-li relevantní čl. 35 odst. 1 GDPR, provede Zpracovatel posouzení vlivu zpracování osobních údajů a informuje Nemocnici o výsledku posouzení bez zbytečného odkladu;
 - j) je-li relevantní čl. 37 GDPR, jmenuje Zpracovatel pověřence pro ochranu osobních údajů a informuje Nemocnici o kontaktních údajích tohoto pověřence bez zbytečného odkladu;
 - k) nepředá osobní údaje do země mimo území Evropské unie bez souhlasu Nemocnice.
2. Zpracovatel bez souhlasu Nemocnice nesmí svěřit zpracování osobních údajů dle původní smlouvy a této smlouvy třetí osobě. Z tohoto důvodu je Zpracovatel povinen si s dostatečným předstihem vyžádat písemný souhlas Nemocnice ke každému novému třetímu zpracovateli, a stejně tak neprodleně informovat Nemocnici o ukončení spolupráce se třetím zpracovatelem způsobem stanoveným v příloze č. 1 Pokyny pro zpracovatele osobních údajů. Pokud Zpracovatel do zpracování osobních údajů dle této smlouvy zapojí dalšího zpracovatele, musí se tento další zpracovatel smluvně zavázat k dodržování stejných zásad pro zpracování osobních údajů, které jsou stanoveny touto smlouvou. Poruší-li další zpracovatel své povinnosti v oblasti zpracování nebo ochrany osobních údajů, za toto porušení odpovídá Nemocnici Zpracovatel.
3. Zpracovatel se zavazuje zavést a udržovat organizační a technická opatření za účelem ochrany zpracovávaných osobních údajů, aby byla zajištěna zejména:
 - a) důvěrnost, dostupnost a integrita osobních údajů;
 - b) odolnost systémů a IT služeb sloužících zpracování osobních údajů, aby splňovala požadavky GDPR.Blížší požadavky stanoví příloha č. 1 - Pokyny pro zpracovatele osobních údajů.
4. Pro případ incidentu, který způsobí narušení některého z principů uvedených v odst. 3 tohoto článku se Zpracovatel zavazuje mít připraveny postupy a zdroje umožňující odstranění následků incidentu a obnovu řádného stavu bez zbytečného odkladu. Zpracovatel o takovém incidentu neprodleně informuje odpovědné osoby Nemocnice v souladu s přílohou č. 1 - Pokyny pro zpracovatele osobních údajů.
5. V případě ukončení původní smlouvy nebo této smlouvy je Zpracovatel povinen:

- a) bez zbytečného odkladu přestat zpracovávat osobní údaje poskytnuté mu Nemocnicí na základě původní smlouvy a/nebo této smlouvy, ledaže mu Nemocnice vydá jiný pokyn nebo není-li další zpracovávání osobních údajů vyžadováno právem EU nebo právními předpisy ČR;
 - b) veškeré osobní údaje předat zpět Nemocnici v běžně využívané elektronické podobě vhodné pro takovéto předání;
 - c) po potvrzení převzetí osobních údajů Nemocnicí dle výše uvedeného písm. b) zničit veškeré osobní údaje, které zpracovával na základě původní smlouvy a/nebo této smlouvy není-li uložení dalších zpracovávaných osobních údajů vyžadováno platnými právními předpisy EU nebo právními předpisy ČR. Povinnost likvidace osobních údajů se týká jejich elektronické i papírové podoby, včetně záloh.
6. Zpracovatel se dále zavazuje pravidelně testovat, posuzovat a hodnotit účinnost zavedených technických a organizačních opatření.
 7. Zpracovatel na požadavek Nemocnice kdykoli předloží dokumentaci prokazující zavedení a/nebo hodnocení výše uvedených opatření.

VII. Práva a povinnosti Nemocnice

1. Nemocnice je ve vztahu k čl. III. této smlouvy správcem osobních údajů.
2. Nemocnice se zavazuje:
 - a) umožnit Zpracovateli přístup k těm osobním údajům, které má Zpracovatel na základě původní smlouvy pro Nemocnici zpracovávat;
 - b) předávat Zpracovateli včas informace a pokyny nezbytné k řádnému výkonu činností dle článku I. této smlouvy;
 - c) písemně sdělit Zpracovateli jména, příjmení, pracovní pozice, kontaktní telefonní čísla a e-mailové adresy osob, které jsou oprávněny Zpracovateli dávat pokyny v souvislosti se zpracováním osobních údajů;
 - d) písemně sdělit Zpracovateli jména, příjmení, pracovní pozice, kontaktní telefonní čísla a e-mailové adresy osob, kterým je Zpracovatel povinen hlásit incidenty ve smyslu článku VI. odst. 4 této smlouvy;
 - e) v případě, že dojde ke změně osob vzhledem k výše uvedeným písm. c) a d); Nemocnice tuto změnu písemně nahlásí Zpracovateli bez zbytečného odkladu.
3. Nemocnice je jako správce osobních údajů povinna v souladu s GDPR vyhodnotit Zpracovatele z hlediska rizik, která přináší zpracování osobních údajů s ohledem na práva a svobody subjektů údajů. Zpracovatel je povinen poskytnout Nemocnici potřebnou součinnost.

VIII. Mlčenlivost

1. Zpracovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o Nemocnici, jejich zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním původní smlouvy a této smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Zpracovatel je povinen nakládat s osobními údaji v souladu s GDPR a zákonem.
2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
3. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu, k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících osobní údaje trvá bez časového omezení.

IX. Porušení smlouvy a smluvní pokuty

Poruší-li Zpracovatel některou ze svých povinností ve vztahu ke zpracování osobních údajů dle této smlouvy, je:

- a) Nemocnice oprávněna požadovat po Zpracovateli úhradu smluvní pokuty ve výši 100.000 Kč. Úhradou smluvní pokuty není dotčena povinnost Zpracovatele odstranit závadný stav, ani povinnost Zpracovatele uhradit Nemocnici případně vzniklou majetkovou i nemajetkovou újmu, např. v podobě sankce, která byla Nemocnici uložena kvůli pochybení Zpracovatele.
- b) Nemocnice oprávněna požadovat po Zpracovateli nápravu závadného stavu.

X. Prohlášení Zpracovatele

Zpracovatel prohlašuje, že k datu podpisu této smlouvy zavedl a udržuje veškerá opatření touto smlouvou požadovaná.

XI. Kontaktní osoby

1. Osobou oprávněnou jednat za Nemocnici ve věcech, které se týkají plnění dle této smlouvy je Pověřenec pro ochranu osobních údajů, e-mail: xxxxx.
2. Osobou oprávněnou jednat za Zpracovatele ve věcech, které se týkají plnění dle této smlouvy je xxxxx, tel. xxxxx, e-mail: xxxxx.
3. Každá ze stran může změnit svou kontaktní osobu písemným oznámením zaslaným druhé straně v souladu s tímto ustanovením.

XII. Závěrečná ustanovení

1. Tato smlouva se uzavírá na dobu neurčitou.
2. Tato smlouva může být ukončena písemnou dohodou smluvních stran, písemným odstoupením od smlouvy dle odst. 3 tohoto článku nebo písemnou výpovědí dle odst. 4 tohoto článku.
3. Každá smluvní strana je oprávněna od této smlouvy odstoupit, pokud druhá smluvní strana poruší svoji povinnost vyplývající z této smlouvy podstatným způsobem a nezjedná nápravu ani v přiměřené lhůtě určené jí v písemné výzvě dotčenou smluvní stranou.
4. Každá ze smluvních stran je oprávněna kdykoliv vypovědět tuto smlouvu i bez uvedení důvodu s výpovědní dobou 6 měsíců, která začíná plynout prvním dnem kalendářního měsíce následujícího po doručení výpovědi druhé smluvní straně. Smluvní strany rovněž berou na vědomí, že za předpokladu zániku této smlouvy automaticky zanikají i původní smlouvy č. PO 95/S/26, nedohodnou-li se smluvní strany výslovně jinak.
5. Odstoupením Nemocnice od této smlouvy nebo výpovědí Nemocnice nezanikají povinnosti Zpracovatele týkající se bezpečnosti a ochrany zpracovávaných osobních údajů až do okamžiku jejich výmazu, povinnost mlčenlivosti ani povinnost k náhradě újmy dle čl. IX.
6. Vztahy mezi smluvními stranami výslovně v této smlouvě neupravené se řídí právním řádem České republiky a EU, zejména GDPR, zákonem a Občanským zákoníkem.
7. Veškeré změny této smlouvy je možné provést pouze formou očíslovaných písemných dodatků, které se po jejich podpisu oprávněnými zástupci obou smluvních stran stanou nedílnou součástí této smlouvy.
8. Smlouva je vyhotovena ve dvou stejnopisech s platností originálu, přičemž každá smluvní strana obdrží po jednom řádně podepsaném vyhotovení. Pokud je smlouva podepisována elektronicky, je vyhotovena v jednom stejnopise podepsaném oběma smluvními stranami elektronickým podpisem dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
9. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.

Příloha č. 1: Pokyny pro zpracovatele osobních údajů

V Benešově dle el. podpisu

V Praze dne dle el. podpisu

xxxxx
ředitel ICT

prof. MUDr. David Feltl, Ph.D., MBA
ředitel



VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE

U Nemocnice 499/2, 128 08 Praha 2 | IČ: 00064165, tel. 224 961 111

Verze 02, strana 1 z 4

Pokyny pro zpracovatele osobních údajů Ochrana osobních údajů

1. Úvod

- 1.1 Všeobecná fakultní nemocnice v Praze, IČO: 000 64 165, se sídlem U Nemocnice 499/2, 128 08 Praha 2, zastoupená prof. MUDr. David Feltl, Ph.D., MBA, ředitelem, jako správce údajů (dále jen „správce“ nebo také „Nemocnice“), díky kterým je možné zjistit totožnost (identifikovat) konkrétní fyzickou osobu (dále jen „Osobní údaje“) a to lhostejno, zda se jedná o jakékoliv typy pacientů nemocnice, zaměstnance nemocnice, bývalé zaměstnance nemocnice, uchazeče o zaměstnání v nemocnici nebo jiných fyzických osob, které jsou předávány v rámci plnění vzájemných smluvních vztahů, které nemocnice uzavřela s Vámi jako zpracovatelem Osobních údajů (dále také jen „Smlouva“), se nemocnice v rámci smluv uzavřených s Vámi nebo dodatků k těmto smlouvám dohodla na obecných pravidlech zajišťujících ochranu Osobních údajů, které v rámci uzavřené Smlouvy zpracováváte (dále jste také označen jen jako „Zpracovatel“) a to v souvislosti se splněním požadavků nové právní úpravy týkající se ochrany osobních údajů, především Nařízení Evropského parlamentu a Rady č. 2016/79 (dále jen „Nařízení“ nebo také „GDPR“).
- 1.2 V rámci plnění Smlouvy, stejně jako dle Nařízení, Nemocnice jako správce uděluje pokyny zpracovateli pro zpracování Osobních údajů. Tyto pokyny, udělované Nemocnicí zpracovateli, jsou zpřesněním a specifikací pravidel pro zpracování Osobních údajů upravených v uzavřené Smlouvě.
- 1.3 Pokud s Osobními údaji nakládáte v rámci stanovených podmínek pro své podnikatelské nebo jiné vlastní aktivity, nejste v pozici zpracovatele Osobních údajů, ale jednáte jako správce Osobních údajů.
- 1.4 Pokud s Osobními údaji nakládáte pro účely Nemocnice a pro její vlastní aktivity, jste v pozici zpracovatele Osobních údajů.

2. Incident

V Případě vzniku incidentu, tedy ztráty nebo úniku Osobních údajů, neoprávněné manipulaci s nimi nebo jiného porušení zabezpečení Osobních údajů (dále jen „Incident“), je zpracovatel povinen neprodleně informovat Nemocnici dle Smlouvy a těchto Pokynů.

Zpracovatel je povinen hlásit Incident (Porušení zabezpečení Osobních údajů) prostřednictvím e-mailu na adresy: [REDACTED]

V e-mailu bude uvedeno:

- kontaktní údaj ohlašovatele Incidentu (jméno, příjmení, telefon nebo e-mail a identifikace zpracovatele (název/Jméno a příjmení, IČO/datum narození))
- popis incidentu, tedy podrobný popis porušení zabezpečení Osobních údajů všemi dostupnými informacemi, tedy zejména kdy k incidentu došlo, kde k němu došlo, jak k němu došlo či co se stalo apod.

V pracovní dny je Zpracovatel dále povinen nahlásit Incident i telefonicky na linku 224 962 119 (Dispečink Úseku informatiky VFN).



Pokyny pro zpracovatele osobních údajů

Ochrana osobních údajů

Nařízení v případě potvrzeného Incidentu (Porušení zabezpečení Osobních údajů) stanovuje přísné lhůty pro řešení Incidentu. Správce tedy může po Zpracovateli vyžadovat součinnost při řešení Incidentu i mimo standardní pracovní dobu nebo během dní pracovního klidu. Zpracovatel je povinen bez dalšího vyžadovanou součinnost poskytnout.

3. Žádosti subjektů údajů

Pokud se bude kdokoliv domnívat, že Nemocnice nebo zpracovatel zpracovává jeho Osobní údaje v rozporu s platnou právní úpravou, především v rozporu s Nařízením nebo v rozporu s dalšími právy subjektu údajů a tato osoba požádá Zpracovatele o vysvětlení nebo odstranění tohoto stavu, zejména ve smyslu článků 16 až 18 Nařízení, Zpracovatel je povinen o tomto požadavku neprodleně informovat Nemocnici prostřednictvím e-mailu: [redacted] případně může Zpracovatel doporučit této osobě, aby se obrátila přímo na Nemocnici jako správce Osobních údajů a to těmito způsoby:

- a) e-mailem: [redacted]
- b) písemně poštou na adresu Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2,
- c) osobním doručením dotazu, žádosti či stížnosti do podatelny Všeobecné fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2, budova ředitelství A5, 4. patro (PO-ČT 9-15 hod., PÁ 9-14 hod.),

a následně v procesu vyřízení žádosti bude ověřena totožnost žadatele osobních údajů.

4. Informování o zjištěném porušení povinností vyplývajících z Nařízení

Pokud Zpracovatel zjistí, že Nemocnice porušuje povinnosti vyplývající z Nařízení, případně jiných právních předpisů, je dle článku 28 odst. 3 písm. h) Nařízení, povinen neprodleně Nemocnici o tomto zjištění informovat prostřednictvím e-mailu: [redacted]

5. Zapojení dalších zpracovatelů

Zpracovatel bez souhlasu Nemocnice nesmí svěřit jakékoliv zpracování třetí osobě. Z tohoto důvodu je Zpracovatel povinen s dostatečným předstihem vyžádat si písemný souhlas Nemocnice ke každému novému třetímu zpracovateli, a stejně tak neprodleně informovat Nemocnici o ukončení spolupráce se třetím zpracovatelem a to prostřednictvím e-mailu na: [redacted]

Součástí tohoto e-mailu bude identifikace Vás jako Zpracovatele (název/jméno a příjmení, IČO/datum narození) a seznam dalších zapojovaných třetích zpracovatelů dle následujících požadavků:

- formát přílohy je MS Excel – XLSX.
- povinná pole jsou:
 - název/jméno a příjmení.
 - IČO/datum narození.



Pokyny pro zpracovatele osobních údajů

Ochrana osobních údajů

- telefonní číslo,
- e-mailová adresa,
- osobní číslo v rámci společnosti, je-li přiděleno,
- seznam je nutné znovu zaslat vždy, pokud má dojít k zapojení nového zpracovatele nebo ukončení spolupráce s jiným zpracovatelem,
- první seznam bude obsahovat všechny současně zapojované další zpracovatele a následující seznamy budou obsahovat jen nové třetí zpracovatele a zpracovatele, s nimiž byla spolupráce ukončena. Tento první seznam bude zpracovatelem zaslán do 14 dní od uzavření Smlouvy či dodatku k již existující smlouvě.

6. Technická a organizační opatření zpracovatele

Zpracovatel je povinen přijmout vhodná technická a organizační opatření dle Smlouvy, dodatku ke smlouvě nebo dle Smlouvy o zpracování osobních údajů uzavřené s Všeobecnou fakultní nemocnicí v Praze:

- a) zpracovatel při zpracování Osobních údajů zejména:
- zpřístupní Osobní údaje pouze omezenému okruhu osob, které tento přístup za účelem konkrétního zpracování Osobních údajů nutně potřebují a to tak, že:
 - toto zpřístupnění nepochybně souvisí s činností Zpracovatele a zároveň
 - Zpracovatel toto oprávnění uděluje individuálně a pouze dokladovatelným způsobem;
 - dodrží povinnost mlčenlivosti o všech Osobních údajích a také o bezpečnostních opatřeních, které slouží k ochraně osobních údajů a to ze strany těch zaměstnanců nebo jiných osob, které se na zpracování Osobních údajů podílejí,
 - musí být schopen prokázat, že všichni zaměstnanci nebo jiné osoby, na které se povinnost mlčenlivosti vztahuje, jsou s touto povinností prokazatelně seznámeni a dodržováním vázáni,
 - zajistí, aby pracovníci mající přístup k osobním údajům byli proškoleni, že osobní údaje mohou být zpracovávány výhradně v souladu s právními předpisy a těmito Pokyny.
- b) Zpracovatel zajistí bezpečnost informací - Zpracovatel je povinen zajistit bezpečnost zpracovávaných Osobních údajů zejm. zavedením vhodných prvků systému řízení bezpečnosti informací, formalizací jednotlivých postupů, prováděním pravidelných kontrol, a přípravou a testováním plánů pro případ havárií.
- c) Zpracovatel zabezpečí objekty a místnosti - Zpracovatel je povinen uchovávat a zpracovávat Osobní údaje předané nebo sdělené mu Nemocnicí v důsledně zabezpečených objektech a místnostech, tj. v prostorách, které jsou vybaveny alespoň základními prvky fyzického zabezpečení (přístupnost prostor jen pro oprávněné osoby, uzamykatelnost úložišť papírové dokumentace apod.), přičemž tato úroveň zabezpečení musí být přiměřená rozsahu, objemu a citlivosti zpracovávaných osobních údajů. Toto platí zejména pro prostory, kde jsou uchovávány papírové dokumenty obsahující osobní údaje.
- d) Zpracovatel zajistí logické zabezpečení dat zpracovávaných v elektronické podobě – zejména používáním: osobních uživatelských účtů a hesel, spořičů obrazovek s ochranou heslem při nečinnosti,



Pokyny pro zpracovatele osobních údajů

Ochrana osobních údajů

- pravidelně aktualizovaných antivirových a anti-malware programů na počítačích a mobilních zařízeních; firewallů a šifrování.
- e) dálkový přenos Osobních údajů - Zpracovatel zajistí zabezpečení elektronické komunikace vhodnými mechanismy autentizace a šifrování přenosu. V případě převozu fyzického nosiče dat přijme opatření, která brání neautorizovaným osobám v přístupu k těmto datům (šifrování). Nosiče dat jsou likvidovány bezpečnou cestou.
- f) Zpracovatel zajistí pseudonymizaci a šifrování osobních údajů - Zpracovatel je povinen zpracovávat osobní údaje v pseudonymizované a šifrované podobě, je-li to technicky možné a umožňují-li to podmínky Smlouvy uzavřené s Nemocnicí. Pseudonymizované údaje jsou takové údaje, které nelze přiřadit ke konkrétní osobě bez použití dodatečných informací, tzv. klíče, přičemž tento klíč musí být uchováván odděleně a musí být přijata taková opatření technického a organizačního rázu, že tento klíč nebude přiřazen k osobním údajům, nebude-li to nutné. Klíč je znám pouze Nemocnici nebo Zpracovateli.
- g) důvěrnost, integrita, dostupnost a odolnost systémů - Zpracovatel je povinen zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování osobních údajů.
- h) Zpracovatel zajistí testování a hodnocení - Zpracovatel je povinen pravidelně testovat, posuzovat a hodnotit účinnost a úspěšnost zavedených technických, organizačních a administrativních opatření pro zajištění bezpečnosti zpracování osobních údajů, a to např. formou interního nebo externího auditu, vyhodnocením pomocí dotazníků (self-assessment), na základě zachycených bezpečnostních událostí či incidentů apod. O testování Zpracovatel vždy pořídí záznam, kterým bude v případě potřeby schopen prokázat, že testování proběhlo a s jakým výsledkem. Toto testování či ověřování bude provádět alespoň jednou za rok.
- i) ukončení zpracování Osobních údajů – Zpracovatel je povinen při ukončení zpracování osobních údajů, které získal nebo mu je předala Nemocnice, předat tyto Osobní údaje Nemocnici nebo dle dohody s Nemocnicí zajistit bezpečnou likvidaci Osobních údajů. Zpracovatel je povinen zajistit soulad především s těmito pravidly likvidace Osobních údajů:
- papírové dokumenty je nutno likvidovat skartovacím zařízením;
 - elektronické dokumenty je nutné likvidovat prostřednictvím standardních nástrojů nenávratného vymazání elektronického obsahu (např. vícenásobné přepsání paměťových bloků náhodnými daty), nebo jiným obdobným způsobem, který zajistí, že nebude moci dojít k neoprávněnému zpřístupnění takto zlikvidovaných Osobních údajů. Pro Osobní údaje zvláštní kategorie je nutné pro likvidaci využít zvláště bezpečného mechanismu (např. degaussing HDD).