|  |  |
| --- | --- |
| **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  **DATAMED, SIA** společnost s ručením omezeným,  Se sídlem: Sūnu iela 6, Jūrmala, LV-2008, Lotyšsko  IČO: 40003863787 DIČ: LV40003863787  Zastoupená: Normundsem Ančupānsem, členem představenstva,  (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  **S M L O U V U O Z P R A C O V Á N Í O S O B N Í C H Ú D A J Ů**  (dále též „**smlouva**“)   1. **Předmět smlouvy**    1. 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.    2. Zpracovatel poskytuje Nemocnici na základě smlouvy č. PO 488/S/23, případně dalších smluv (dále jen „původní smlouva“) 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 smlouvy.    3. V rámci poskytování uvedených služeb zpracovává Zpracovatel osobní údaje, jejichž správcem je Nemocnice.    4. 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.    5. Smluvní strany mají zájem upravit touto smlouvou svá vzájemná práva a povinnosti při zpracování osobních údajů podle čl. 28 GDPR. 2. **Definice** 3. 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. 4. 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. 5. Další pojmy používané v této smlouvě mají totožný význam, jako pojmy užité v GDPR, ev. mají význam, který je jim přisuzován jinými závaznými právními předpisy. 6. **Předmět, povaha a účel zpracování** 7. Předmětem zpracování osobních údajů ve smyslu čl. 1 a 2 této smlouvy je zejména zajištění a podpora provozu informačních technologii dle I.2. 8. Osobní údaje jsou zpracovávány pro následující účely:   − instalace a údržba;  − data hosting;  − zničení dat;  − analýza dat pro detekci anomálií.   1. Zpracovatel není oprávněn zpracovávat osobní údaje za jiným účelem, než který mu byl stanoven Nemocnicí prostřednictvím původní smlouvy a této smlouvy. 2. **Typy zpracovávaných osobních údajů a kategorie subjektů** 3. Předmětem zpracování jsou následující typy osobních údajů:  * administrativní údaje o pacientech; * zdravotní údaje týkající se pacientů, diagnostické informace, snímky; * administrativní údaje týkající se uživatelů systému  1. Kategorie subjektů údajů jsou koncoví uživatelé a pacienti koncových uživatelů. 2. **Doba trvání zpracování osobních údajů** 3. Zpracovatel zpracovává osobní údaje dle čl. III. a IV. po dobu trvaní této smlouvy, nejdéle však po dobu účinnosti původní smlouvy. 4. **Práva a povinnosti Zpracovatele** 5. V souladu s čl. 28. odst. 3 GDPR Zpracovatel zejména: 6. zpracovává osobní údaje výhradně na základě původní smlouvy, této smlouvy a doložených pokynů Nemocnice, a v souladu s GDPR; 7. plní bezodkladně veškeré pokyny udělené mu Nemocnicí ve vztahu ke zpracování osobních údajů, například přerušení zpracování osobních údajů, jejich úprava, výmaz či vydání kopie; 8. zajišťuje, že se jeho zaměstnanci a případně další osoby mající přístup k osobním údajům Nemocnice zavázaly k mlčenlivosti; 9. přijme veškerá opatření stanovená článkem 32 GDPR, která jsou blíže stanovena v odst. 3 tohoto článku 10. udržuje technická a organizační opatření blíže popsaná v Pokynech 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. 11. 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; 12. 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; 13. je Nemocnici nápomocen při zajišťování souladu s jeho povinnostmi podle článků 32 až 36 GDPR; 14. je-li relevantní čl. 35 odst. 1 GDPR, provede Zpracovatel posouzení vlivu zpracování osobních údajů a informuje Nemocnici o výsledku posouzení bez zbytečného odkladu; 15. je-li relevantní čl. 37 GDPR, jmenuje Zpracovatel pověřence pro ochranu osobních údajů a informuje Nemocnici o kontaktních údajích tohoto pověřence bez zbytečného odkladu; 16. nepředá osobní údaje do země mimo území Evropské unie bez souhlasu Nemocnice. 17. 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 Pokynech 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 stanovený touto smlouvou. Poruší-li další zpracovatel své povinnosti v oblasti zpracování nebo ochrany osobních údajů, za toto porušení odpovídá Nemocnici Zpracovatel. 18. Zpracovatel se zavazuje zavést a udržovat organizační a technická opatření za účelem ochrany zpracovávaných osobních údajů, aby byla zajištěna zejména: 19. důvěrnost, dostupnost a integrita osobních údajů; 20. odolnost systémů a IT služeb sloužících zpracování osobních údajů, aby splňovala požadavky GDPR.   Bližší požadavky stanoví Pokyny pro zpracovatele osobních údajů.   1. Pro případ incidentu, který způsobí narušení některého z principů uvedených v odst. 3 se Zpracovatel zavazuje mít připraveny postupy a zdroje umožňující odstranění následků incidentu a obnovu řádného stavu bez zbytečného odkladu. Dodavatel o takovém incidentu neprodleně informuje odpovědné osoby Nemocnice v souladu s Pokyny pro zpracovatele osobních údajů. 2. V případě ukončení původní smlouvy nebo této smlouvy je Zpracovatel povinen: 3. 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; 4. veškeré osobní údaje předat zpět Organizaci v běžně využívané elektronické podobě vhodné pro takovéto předání; 5. po potvrzení převzetí osobních údajů Organizací dle výše uvedeného písm. b) zničit veškeré osobní údaje, které zpracovával na základě Smlouvy a/nebo tohoto Dodatku 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. Dodavatel 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. 8. **Práva a povinnosti Nemocnice** 9. Nemocnice je ve vztahu k čl. III. této smlouvy správcem osobních údajů. 10. Nemocnice se zavazuje: 11. umožnit Zpracovateli přístup k těm osobním údajům, které má Zpracovatel na základě původní smlouvy pro Nemocnici zpracovávat; 12. předávat Zpracovateli včas informace a pokyny nezbytné k řádnému výkonu činností dle článku 1 této smlouvy; 13. v případě změny osob uvedených v příloze č. 2 smlouvy o výpůjčce 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; 14. v případě změny osob uvedených v příloze č. 2 smlouvy o výpůjčce 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; 15. 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. 16. **Mlčenlivost** 17. 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. 18. 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. 19. 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. 20. **Porušení smlouvy a smluvní pokuty**   Poruší-li Zpracovatel některou ze svých povinností ve vztahu ke zpracování osobních údajů dle této smlouvy, je:   1. Nemocnice oprávněna požadovat po Zpracovateli úhradu smluvní pokuty ve výši 100.000Kč. 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. 2. Nemocnice oprávněna požadovat po Zpracovateli nápravu závadného stavu. 3. **Prohlášení Zpracovatele**   Zpracovatel prohlašuje, že k datu podpisu této smlouvy zavedl a udržuje veškerá opatření touto smlouvou požadovaná.   1. **Kontaktní osoby** 2. Osobou oprávněnou jednat za Nemocnici ve věcech, které se týkají plnění dle této smlouvy je Pověřenec pro ochranu osobních údajů, e-mail: XXXXXXXXXXXXXXXX 3. Osobou oprávněnou jednat za Zpracovatele ve věcech, které se týkají plnění dle této smlouvy je XXXXX XXXXXXXXXX, e-mail: XXXXXXXXXXXXXXXX, tel. XXX XXX XXX. 4. Každá ze stran může změnit svou kontaktní osobu písemným oznámením zaslaným druhé straně v souladu s tímto ustanovením. 5. **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 zaniká i smlouva o poskytování služeb podpory software č. PO 488/S/23, jejímž předmětem je poskytování servisních služeb ze strany zpracovatele (smlouva o poskytování podpory software), 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, přičemž každá smluvní strana obdrží po jednom řádně podepsaném vyhotovení.    9. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.   Příloha č. 1: Pokyny pro zpracovatele osobních údajů | **Personal Data Processing Agreement**  **General University Hospital in Prague**  Based: U Nemocnice 499/2, Postal Code: 128 08, Prague 2  Company ID: 000 64 165 VAT: CZ00064165  Represented by: David Feltl, Ph.D., MBA, Director  (hereinafter referred to as "**Hospitals**")  and  **DATAMED, SIA** Limited Liability Company  Based: Sūnu iela 6, Jūrmala, LV-2008, Latvia  Company ID: 40003863787 VAT: LV40003863787  Represented by Normunds Ančupāns, member of the Board  (hereinafter referred to as the "**Processor**")  (Processor and the Hospital hereinafter collectively referred to as the "**Parties**")  The Contracting Parties conclude on the following date, month and year pursuant to Article 28 of EU Regulation No. 2016/679, the General Data Protection Regulation **(hereinafter referred to as the "GDPR")** and the relevant provisions of Act No. 110/2019 Coll., on the processing of personal data (hereinafter referred to as the "**Act**") this  **Personal Data Processing Agreement**  (hereinafter referred to as the "**Agreement**")   1. **Subject of the contract**    1. Within the meaning of the GDPR, the hospital is a personal data controller, as in connection with its activities, especially in the area of providing health services, it processes personal data, including health data, genetic and biometric data (hereinafter referred to as "personal data") of its patients, employees, or other persons (hereinafter referred to as "datasubjects") "). The legal basis for the processing of personal data is, in particular, the fulfillment of a legal obligation that applies to the Administrator, or the legitimate interest of the Administrator.    2. The Processor provides the Hospital on the basis of contract no. PO 488/S/23 or other contracts (hereinafter referred to as the "original contract"), including the following services: ensuring and supporting the operation of the Hospital's information systems, respectively ensuring and supporting the operation of selected information technologies. The list of application SW, the list of the technical means concerned and the specifications of the services provided are given in Annex 1 of the above Agreement.    3. As part of the provision of these services, the Processor processes personal data the administrator of which is the Hospital.    4. Within the meaning of the GDPR, the processor is a person who provides sufficient guarantees of implementing appropriate technical and organizational measures when processing personal data, so as not to exceed the legal framework defining the possibility of such processing.    5. The contracting parties are interested in regulating their mutual rights and obligations in the processing of personal data pursuant to Article 28 of the GDPR by means of this contract. 2. **Definition** 3. Personal data means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable natural person is one who can be identified, directly or indirectly. 4. Processing of personal data means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. 5. Other terms used in this Agreement have the same meaning as the terms used in the GDPR, or have the meaning attributed to them by other binding legal regulations. 6. **Subject, nature and purpose of processing** 7. The subject of personal data processing within the meaning of Articles 1 and 2 of this Agreement is in particular: ensuring and supporting the operation of selected information technologies according I.2. 8. Personal data is processed for the following purposes:   − installation and maintenance;  − data hosting;  − data destruction;  − data analysis to detect anomalies.   1. The Processor is not authorized to process personal data for a purpose other than that set by the Hospital through the original contract and this contract. 2. **Types of processed personal data and categories of subjects** 3. The following types of personal data are subject to processing:  * administrative data concerning the patients; * health data concerning the patients, diagnostic information, images; * administrative data concerning the system users  1. The categories of data subjects are the End-Users and the End-Users’ patients 2. **Duration of personal data processing** 3. The Processor processes personal data pursuant to Articles III and IV for the period of this agreement, but no longer than for the duration of the original contract. 4. **Rights and obligations of the Processor** 5. In accordance with Article 28(2). 3 GDPR In particular, the Processor shall: 6. processes personal data exclusively on the basis of the original contract, this contract and documented instructions of the Hospital, and in accordance with the GDPR; 7. immediately comply with all instructions given to him by the Hospital in relation to the processing of personal data, such as suspending the processing of personal data, modifying them, deleting them or issuing a copy; 8. ensures that its employees and, where applicable, other persons having access to the Hospital's personal data have committed themselves to confidentiality; 9. shall take all measures specified in Article 32 of the GDPR, which are specified in para. 3 of this article 10. maintains the technical and organizational measures described in more detail in the Instructions for Personal Data Processors to prevent unauthorized access to the personal data in question, their unauthorized change, destruction or loss, as well as other misuse. 11. provide the Hospital or a third party authorized by the Hospital or a state authority with all the cooperation necessary to control the Processor's activities performed on the basis of the original contract and/or this contract. In this context, the Processor shall, without undue delay, provide in particular information, documents with access to its premises and facilities and make available its relevant employees; 12. provide the Hospital with all cooperation necessary for the timely processing of the exercise of the data subject's right within the meaning of Articles 15 to 22 of the GDPR in the manner specified in the Instructions for Personal Data Processors; 13. assists the Hospital in ensuring compliance with its obligations under Articles 32 to 36 of the GDPR; 14. where Article 35(3) is applicable. 1 of the GDPR, the Processor shall carry out an assessment of the impact of the processing of personal data and inform the Hospital of the result of the assessment without undue delay; 15. if Art. 37 GDPR is applicable, the Processor shall appoint a Data Protection Officer and inform the Hospital of the contact details of this Data Protection Officer without undue delay; 16. does not transfer personal data to a country outside the European Union without the consent of the Hospital. 17. Without the consent of the Hospital, the Processor may not entrust the processing of personal data under the original contract and this contract to a third party. For this reason, the Processor is obliged to request the written consent of the Hospital to each new third processor sufficiently in advance, as well as to immediately inform the Hospital of the termination of cooperation with the third processor in the manner specified in the Instructions for Personal Data Processors. If the Processor engages another processor in the processing of personal data under this contract, the other processor must contractually undertake to comply with the same principles for the processing of personal data that are set out in this contract. If another processor breaches its obligations in the area of processing or protection of personal data, the Processor is liable to the Hospital for this breach. 18. The Processor undertakes to implement and maintain organizational and technical measures to protect the processed personal data in order to ensure, in particular: 19. the confidentiality, availability and integrity of personal data; 20. the resilience of systems and IT services used to process personal data to meet the requirements of the GDPR.   More detailed requirements are set out in the Guidelines for Personal Data Processors.   1. In the event of an incident that causes a violation of any of the principles referred to in para. 3, the Processor undertakes to have procedures and resources in place to eliminate the consequences of the incident and restore the order state without undue delay. The Supplier shall immediately inform the responsible persons of the Hospital of such an incident in accordance with the Instructions for Personal Data Processors. 2. In the event of termination of the original contract or this contract, the Processor shall: 3. Stop processing personal data provided to him by the Hospital on the basis of the original contract and/or this contract without undue delay, unless the Hospital gives him another instruction or unless further processing of personal data is required by EU law or Czech legislation; 4. transmit all personal data back to the Organization in commonly used electronic form suitable for such transfer; 5. after confirmation of the receipt of personal data by the Organization according to the above point. b) destroy all personal data processed on the basis of the Contract and/or this Addendum, unless the storage of further processed personal data is required by applicable EU legislation or Czech legislation. The obligation to dispose of personal data applies to their electronic and paper form, including backups. 6. The Supplier further undertakes to regularly test, assess and evaluate the effectiveness of the technical and organizational measures implemented. 7. At the request of the Hospital, the Processor shall at any time submit documentation demonstrating the implementation and/or evaluation of the above measures. 8. **Rights and obligations of the Hospital** 9. The hospital is the controller of personal data in relation to Article III of this Agreement. 10. The hospital undertakes: 11. to enable the Processor to access the personal data that the Processor is to process under the original contract for the Hospital; 12. to provide the Processor with timely information and instructions necessary for the proper performance of activities pursuant to Article 1 of this Agreement; 13. In case of changes to the persons referred in Annex No. 2 of the loan agreement to inform the Processor in writing of the names, surnames, job positions, contact telephone numbers and e-mail addresses of persons who are authorized to give instructions to the Processor in connection with the processing of personal data; 14. In case of changes to the persons referred in Annex No. 2 of the loan agreement to inform the Processor in writing of the names, surnames, job titles, contact telephone numbers and e-mail addresses of persons to whom the Processor is obliged to report incidents within the meaning of Article VI. 4 of this Agreement; 15. The Hospital, as a personal data controller, is obliged to evaluate the Processor in accordance with the GDPR in terms of the risks posed by the processing of personal data with regard to the rights and freedoms of data subjects. The Processor is obliged to provide the Hospital with the necessary cooperation. 16. **Coyness** 17. The Processor undertakes to maintain confidentiality in relation to all information and facts that he learns about the Hospital, its employees, patients, etc. in connection with the conclusion and performance of the original contract and this contract, if such information is of the nature of trade secrets, personal data or is to be protected from disclosure for other reasons. The processor is obliged to handle personal data in accordance with the GDPR and the law. 18. The obligation of confidentiality also applies to facts covered by the confidentiality obligation of healthcare professionals, in particular under the provisions of Section 51 of Act No. 372/2011 Coll., on health services and the conditions for their provision (the Health Services Act), and on security measures, the disclosure of which would jeopardize the security of personal data. 19. The Contracting Parties undertake to maintain confidentiality also about all other facts in relation to which they will be asked to do so in writing by the other Party. The Contracting Parties also undertake not to use the information referred to in this paragraph for their own benefit or for the benefit of third parties contrary to the purpose of their transmission. The obligation of confidentiality of information and facts of a commercial nature lasts for a period of 5 years from the termination of this contract, information containing personal data lasts without time limit. 20. **Breach of contract and contractual penalties**   If the Processor breaches any of its obligations in relation to the processing of personal data under this contract, it is:   1. The Hospital is entitled to require the Processor to pay a contractual penalty of CZK 100,000. The payment of the contractual penalty shall not affect the Processor's obligation to remedy the defective condition or the Processor's obligation to pay the Hospital any material and non-material damage incurred, e.g. in the form of a sanction imposed on the Hospital due to the Processor's misconduct. 2. The Hospital is entitled to require the Processor to remedy the defective condition. 3. **Declaration by the processor**   The Processor declares that, on the date of signature of this contract, it has implemented and maintains all measures required by this contract.   1. **Contact persons** 2. The person authorized to act on behalf of the Hospital in matters relating to the performance under this contract is the Data Protection Officer, e-mail: XXXXXXXXXXXXXXXX 3. The person authorized to act on behalf of the Processor in matters relating to the performance under this contract is XXXXX XXXXXXXXXX, e-mail: XXXXXXXXXXXXXXXX, tel. XXX XXX XXX. 4. Each Party may change its contact person by written notification to the other Party in accordance with this provision. 5. **Final provisions** 6. This contract is concluded for an indefinite period of time.    1. This contract may be terminated by written agreement of the parties, written withdrawal from the contract pursuant to par. 3 of this Article or written notice pursuant to paragraph. 4 of this Article.    2. Each Contracting Party shall be entitled to withdraw from this Agreement if the other Party substantially breaches its obligation under this Agreement and fails to remedy it within a reasonable period specified by the Party concerned in a written notice.    3. Each of the Contracting Parties is entitled to terminate this Agreement at any time without giving any reason with a notice period of 6 months, which begins on the first day of the calendar month following the delivery of the notice to the other Party. The Parties also acknowledge that upon termination of this Agreement, the Contract for the Provision of Software Support Services No. PO 488/S/23, the subject of which is the provision of maintenance services by the Processor (Software Support Agreement), shall automatically terminate, unless the Parties expressly agree otherwise.    4. The Hospital's withdrawal from this contract or the Hospital's notice of termination does not terminate the Processor's obligations regarding the security and protection of the processed personal data until the moment of their deletion, the obligation of confidentiality or the obligation to compensate for damage under Article IX.    5. Relations between the contracting parties not expressly regulated in this contract are governed by the laws of the Czech Republic and the EU, in particular the GDPR, the Act and the Civil Code.    6. Any changes to this Agreement may be made only in the form of numbered written amendments, which, upon signature by authorized representatives of both Parties, will become an integral part of this Agreement.    7. The contract shall be drawn up in two copies, each contracting party receiving one duly signed copy.    8. The contract comes into force and effect on the date of signature by both parties.   Annex No. 1: Instructions for personal data processors |
| **Zákazník / The Customer**  Místo / Place: v Praze / in Prague  Datum / Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Jméno a příjmení / First and last name:  Funkce / Position:  **Dodavatel / The Supplier**  Místo / Place: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Datum / Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Jméno a příjmení / First and last name: **Normunds Ancupans**  Funkce / Position: member of the Board of Datamed LLC | |

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**

# Úvod

* 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 dodatkům k těmto smlouvám dohodla na obecných pravidlech zajištujících 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“).
  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.
  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.
  4. Pokud s Osobními údaji nakládáte pro účely Nemocnice a pro její vlastní aktivity, jste v pozici zpracovatele Osobních údajů.

# 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: xxxxxx a xxxxxx

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).

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 standartní pracovní dobu nebo během dní pracovního klidu. Zpracovatel je povinen bez dalšího vyžadovanou součinnost poskytnout.

# 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: xxxxxx, případně může Zpracovatel doporučit této osobě, aby se obrátila přímo na Nemocnici jako správce Osobních údajů a to těmito způsoby:

1. emailem: xxxxxx,
2. písemně poštou na adresu Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2,
3. osobním doručením dotazu, žádostí či stížností 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.

# Informování o zjištěném porušení povinností vyplývající 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: xxxxxx.

# 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: xxxxxx.

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,
  + 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.

# 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:

1. 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.

1. 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.
2. 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.
3. Zpracovatel zajistí logické zabezpečení dat zpracovávaných v elektronické podobě – zejména používáním: osobních uživatelských účtů a hesel, spořičů obrazovek s ochranou heslem při nečinnosti, pravidelně aktualizovaných antivirových a anti-malware programů na počítačích a mobilních zařízeních; firewallů a šifrování.
4. 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.
5. 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.
6. důvěrnost, integrita, dostupnost a odolnost systémů - Zpracovatel je povinen zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování osobních údajů.
7. 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.
8. 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).