NON-INTERVENTIONAL STUDY AGREEMENT

(hereinafter called the “Agreement”)

between

Fakultní nemocnice Ostrava
Department of Internal Medicine and Cardiology
17. listopadu 1790/5
70852 Ostrava-Poruba
Czech Republic
ID. No: 00843989
VAT No.: CZ00843989
Deed of Foundation MoH ČZ from November 25, 1990, file no.: OP-054-25.11.90
Registration number: 017/OVZ/23/010-P
Variable symbol: 649071494
To act and sign in matters of this agreement: doc. MUDr. Ing. Jakub Cvek, Ph.D. MBA, deputy director for science, research and education
Bank: Česká národní banka
Bank address: Na Příkopě 28, 115 03 Praha 1
Account No.: 66332761/0710
IBAN: CZ59 0710 0000 0000 6633 2761
BIC code (SWIFT): CNBACZPP

(hereinafter called "Institution")

and

prof. MUDr. Jan Václavík, Ph.D.
17. listopadu 1790/5
708 52 Ostrava-Poruba
Czech Republic

(hereinafter called "Contract Physician")

and

Alcedis GmbH
Winchesterstr. 3
35394 Giessen
Germany
VAT No.: DE195369444

(hereinafter called "CRO")

SMLOUVA O NEINTERVENČNÍ STUDII

(dále označovaná jako „Smlouva“)

uzavřená mezi těmito smluvními stranami:

Fakultní nemocnice Ostrava
Interní a kardiologická klinika

17. listopadu 1790/5
70852 Ostrava-Poruba
Česká republika
IČ: 00843989
DIČ: CZ00843989
Zřizovací listina MZ ČR ze dne 25. listopadu 1990, č.j. OP-054-25.11.90
Evidenční číslo: 017/OVZ/23/010-P
Variabilní symbol: 649071494
ve věcech této smlouvy je oprávněn jednat a podepisovat: doc. MUDr. Ing. Jakub Cvek, Ph.D. MBA, náměstek ředitele pro vědu, výzkum a výuku
Banka: Česká národní banka
Adresa banky: Na Příkopě 28, 115 03 Praha 1
Číslo účtu: 66332761/0710
IBAN: CZ59 0710 0000 0000 6633 2761
BIC kód (SWIFT): CNBACZPP

(dále označované jako „Zdravotnické zařízení“)

a

prof. MUDr. Jan Václavík, Ph.D.
17. listopadu 1790/5
708 52 Ostrava-Poruba
Česká republika

(dále označovaný jako „Smluvní lékař“)

a

Alcedis GmbH
Winchesterstr. 3
35394 Giessen
Německo
DIČ: DE195369444

(dále označovaná jako „CRO“)

	Workstation security	**N.1**	Users should not be able to deactivate or bypass security settings.	**A. 14.1 Security requirements of information systems**
	Workstation security	**N.2**	Anti-virus applications and detection signatures should be configured on a weekly basis.	**A. 14.1 Security requirements of information systems**
	Workstation security	**N.3**	Users should not have privileges to install or deactivate unauthorized software applications.	**A. 14.1 Security requirements of information systems**
	Workstation security	**N.4**	The system should have session time-outs when the user has not been active for a certain time period.	**A. 14.1 Security requirements of information systems**
	Workstation security	**N.5**	Critical security updates released by the operating system developer should be installed regularly.	**A. 14.1 Security requirements of information systems**
	Network/Communication security	**O.1**	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	**A.13 Communications Security**
	Back-ups	**P.1**	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	**A.12.3 Back-Up**
	Back-ups	**P.2**	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	**A.12.3 Back-Up**
	Back-ups	**P.3**	Execution of backups should be monitored to ensure completeness.	**A.12.3 Back-Up**
	Back-ups	**P.4**	Full backups should be carried out regularly.	**A.12.3 Back-Up**
	Mobile/Portable devices	**Q.1**	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	**A. 6.2 Mobile devices and teleworking**
	Mobile/Portable devices	**Q.2**	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	**A. 6.2 Mobile devices and teleworking**
	Mobile/Portable devices	**Q.3**	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	**A. 6.2 Mobile devices and teleworking**
	MEASURE CATEGORY	**MEASURE**	**MEASURE DESCRIPTION**	**RELEVANT ISO/IEC 27001: 2013 CONTROL**
	Application lifecycle security	**R.1**	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**

	Application lifecycle security	**R.2**	Specific security requirements should be defined during the early stages of the development lifecycle.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
	Application lifecycle security	**R.3**	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
	Application lifecycle security	**R.4**	Secure coding standards and practises should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
	Application lifecycle security	**R.5**	During the development, testing and validation against the implementation of the initial security requirements should be performed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
	Data deletion/disposal	**S.1**	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
	Data deletion/disposal	**S.2**	Shredding of paper and portable media used to store personal data shall be carried out.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
	Physical security	**T.1**	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	**A.11 – Physical and environmental security**

PŘÍLOHA 2
KE SMLOUVĚ O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Popis technických a organizačních bezpečnostních opatření zavedených Zpracovatelem údajů

KATEGORIE OPATŘENÍ	OPATŘENÍ	POPIS OPATŘENÍ	PŘÍSLUŠNÝ STANDARD ISO/IEC 27001: KONTROLA 2013
Bezpečnostní politika a postupy pro ochranu osobních údajů	**A.1**	Organizace by měla zdokumentovat svou politiku týkající se zpracování osobních údajů jako součást své politiky zabezpečení informací	**A.5 Bezpečnostní politika**
Bezpečnostní politika a postupy pro ochranu osobních údajů	**A.2**	Bezpečnostní politika by se měla každoročně zkontrolovat a v případě potřeby revidovat.	**A.5 Bezpečnostní politika**
Role a povinnosti	**B.1**	Role a povinnosti související se zpracováním osobních údajů, přidělené v souladu s bezpečnostní politikou.	**A.6.1.1 Role a povinnosti v oblasti zabezpečení informací**
Role a povinnosti	**B.2**	Při interní reorganizaci nebo ukončení pracovního poměru a změně zaměstnání by mělo být jasně definováno zrušení práv a povinností s příslušnými postupy pro předání	**A.6.1.1 Role a povinnosti v oblasti zabezpečení informací**
Politika kontroly přístupu	**C.1**	Každé roli (podílející se na zpracování osobních údajů) by měla být přidělena zvláštní práva pro řízení přístupu podle zásady „need to know“ (jen kdo nutně potřebuje vědět)	**A.9.1.1 Politika kontroly přístupu**
Správa zdrojů/aktiv	**D.1**	Organizace by měla mít evidenci IT zdrojů používaných ke zpracování osobních údajů (hardware, software a síť). Evidence by mohla obsahovat alespoň tyto informace: IT zdroj, typ (např. server, pracovní stanice), umístění (fyzické nebo elektronické). Vedením a aktualizací evidence by měla být pověřena konkrétní osoba (např. pracovník IT).	**A.8 Správa majetku**
Správa zdrojů/aktiv	**D.2**	Prostředky IT by se měly pravidelně revidovat a aktualizovat.	**A.8 Správa majetku**
Správa změn	**E.1**	Organizace by měla zajistit, aby všechny změny v systému IT registrovala a sledovala konkrétní osoba (např. IT nebo bezpečnostní pracovník). Tento proces by se měl pravidelně monitorovat.	**A. 12.1 Provozní postupy a povinnosti**
Správa změn	**E.2**	Vývoj softwaru by měl probíhat ve zvláštním prostředí, které není propojeno s IT systémem používaným pro zpracování osobních údajů. V případě potřeby testování by se měla použít fiktivní data (nikoli skutečná data). V případech, kdy to není možné, by se měly zavést zvláštní postupy pro ochranu osobních údajů používaných při testování.	**A. 12.1 Provozní postupy a povinnosti**

KATEGORIE OPATŘENÍ	OPATŘENÍ	POPIS OPATŘENÍ	PŘÍSLUŠNÝ STANDARD ISO/IEC 27001: KONTROLA 2013
Zpracovatelé údajů	**F.1**	Formální směrnice a postupy týkající se zpracování osobních údajů Zpracovateli údajů (dodavatelé/outsourcing) by měl správce údajů a zpracovatel údajů definovat, zdokumentovat a odsouhlasit před zahájením činností zpracování. Tyto pokyny a postupy by měly povinně stanovit stejnou úroveň zabezpečení osobních údajů, jaká je stanovena v bezpečnostní politice organizace.	**A.15 Vztahy s dodavateli**
Zpracovatelé údajů	**F.2**	Po zjištění porušení zabezpečení osobních údajů zpracovatel údajů bez zbytečného odkladu informuje správce.	**A.15 Vztahy s dodavateli**
Zpracovatelé údajů	**F.3**	Správce údajů a zpracovatel údajů by měli mít formální dohodu o formálních požadavcích a povinnostech. Zpracovatel údajů by měl poskytnout dostatečně zdokumentované důkazy o splnění požadavků.	**A.15 Vztahy s dodavateli**
Řešení incidentů / Porušení zabezpečení osobních údajů	**G.1**	Je třeba definovat plán reagování na incidenty s podrobnými postupy, kterými se zajistí účinné a řádné reagování na incidenty související s osobními údaji.	**A.16 Řízení incidentů v oblasti zabezpečení informací**
Řešení incidentů / Porušení zabezpečení osobních údajů	**G.2.**	Porušení bezpečnosti osobních údajů by se mělo okamžitě hlásit vedení. Měly by se zavést postupy pro oznamování porušení předpisů příslušným orgánům a subjektům údajů v souladu s čl. 33 a 34 GDPR.	**A.16 Řízení incidentů v oblasti zabezpečení informací**
Kontinuita podnikání	**H.1**	Organizace by měla stanovit hlavní postupy a kontrolní mechanismy, které je třeba dodržovat, aby se zajistila požadovaná úroveň kontinuity a dostupnosti IT systému zpracovávajícího osobní údaje (v případě incidentu/porušení zabezpečení osobních údajů).	**A. 17 Aspekty zabezpečení informací při řízení kontinuity podnikání**
Zachování důvěrnosti ze strany personálu	**I.1**	Organizace by měla zajistit, aby všichni zaměstnanci chápali svoji odpovědnost a povinnosti související se zpracováním osobních údajů. Úkoly a povinnosti by se měly jasně sdělovat již během procesu před nástupem do zaměstnání a/nebo během úvodního zaškolování.	**A.7 Zabezpečení lidských zdrojů**

KATEGORIE OPATŘENÍ	OPATŘENÍ	POPIS OPATŘENÍ	PŘÍSLUŠNÝ STANDARD ISO/IEC 27001: KONTROLA 2013
Školení	**J.1**	Organizace by měla zajistit, aby všichni zaměstnanci byli dostatečně informováni o bezpečnostních kontrolách systému IT, které se týkají jejich každodenní práce. Zaměstnanci, kteří se podílejí na zpracování osobních údajů, by měli být prostřednictvím pravidelných osvětových kampaní rovněž řádně informováni o příslušných požadavcích na ochranu údajů a právních povinnostech.	**A.7.2.2 Informovanost, vzdělávání a školení o zabezpečení informací**
Řízení přístupu a ověřování	**K.1**	Měl by být zaveden systém řízení přístupu vztahující se na všechny uživatele přistupující k systému IT. Systém by měl umožňovat vytváření, schvalování, kontrolu a mazání uživatelských účtů.	**A.9 Kontrola přístupu**
Řízení přístupu a ověřování	**K.2**	Je třeba se vyhnout používání běžných uživatelských účtů. V případech, kdy je to nezbytné, je třeba zajistit, aby všichni uživatelé běžného účtu měli stejné role a povinnosti.	**A.9 Kontrola přístupu**
Řízení přístupu a ověřování	**K.3**	Měl by být zaveden mechanismus ověřování, který umožní přístup do IT systému (na základě politiky a systému řízení přístupu). Měla by se používat minimálně kombinace uživatelského jména a hesla. Hesla by měla dodržovat určitou (konfigurovatelnou) úroveň složitosti.	**A.9 Kontrola přístupu**
Řízení přístupu a ověřování	**K.4**	Systém řízení přístupu by měl mít možnost zjistit a nepovolit používání hesel, která nedodržují určitou (konfigurovatelnou) úroveň složitosti.	**A.9 Kontrola přístupu**
Protokolování a monitorování	**L.1**	Pro každý systém/aplikaci používaný/ou ke zpracování osobních údajů by se měly aktivovat protokolové soubory. Měly by zahrnovat všechny typy přístupu k datům (zobrazení, modifikace, mazání).	**A.12.4 Protokolování a monitorování**
Protokolování a monitorování	**L.2**	Protokolové soubory by měly být opatřeny časovou značkou a dostatečně chráněny proti manipulaci a neoprávněnému přístupu. Hodiny by se měly synchronizovat s jediným referenčním zdrojem času	**A.12.4 Protokolování a monitorování**
Zabezpečení serverů/databází	**M.1**	Servery s databázemi a aplikacemi by se měly nakonfigurovat tak, aby pro správnou funkci používaly samostatný účet s minimálními právy operačního systému.	**A. 12 Zabezpečení provozu**
KATEGORIE OPATŘENÍ	**OPATŘENÍ**	**POPIS OPATŘENÍ**	**PŘÍSLUŠNÝ STANDARD ISO/IEC 27001: KONTROLA 2013**

	Zabezpečení serverů/databází	**M.2**	Servery s databázemi a aplikacemi by měly zpracovávat pouze ty osobní údaje, které jsou skutečně nutné ke zpracování za účelem dosažení účelu zpracování.	**A. 12 Zabezpečení operací**
	Zabezpečení pracovních stanic	**N.1**	Uživatelé by neměli mít možnost deaktivovat nebo obejít nastavení zabezpečení.	**A. 14.1 Bezpečnostní požadavky na informační systémy**
	Zabezpečení pracovních stanic	**N.2**	Antivirové aplikace a detekční signatury by se měly konfigurovat každý týden.	**A. 14.1 Bezpečnostní požadavky na informační systémy**
	Zabezpečení pracovních stanic	**N.3**	Uživatelé by neměli mít oprávnění instalovat nebo deaktivovat neautorizované softwarové aplikace.	**A. 14.1 Bezpečnostní požadavky na informační systémy**
	Zabezpečení pracovních stanic	**N.4**	Systém by měl mít časový limit relace, pokud uživatel nebyl po určitou dobu aktivní.	**A. 14.1 Bezpečnostní požadavky na informační systémy**
	Zabezpečení pracovních stanic	**N.5**	Kritické aktualizace zabezpečení vydané vývojářem operačního systému by se měly pravidelně instalovat.	**A. 14.1 Bezpečnostní požadavky na informační systémy**
	Zabezpečení sítí/komunikace	**O.1**	Při každém přístupu přes internet by měla být komunikace šifrována pomocí kryptografických protokolů (TLS/SSL).	**A.13 Zabezpečení komunikace**
	Zálohy	**P.1**	Postupy zálohování a obnovy dat by se měly jasně definovat, zdokumentovat a jasně propojit s rolemi a povinnostmi.	**A.12.3 Zálohování**
	Zálohy	**P.2**	Zálohám by se měla poskytnout odpovídající úroveň fyzické ochrany a ochrany životního prostředí v souladu se standardy uplatňovanými na výchozí data.	**A.12.3 Zálohování**
	Zálohy	**P.3**	Provádění záloh by se mělo monitorovat, aby byla zajištěna jejich úplnost.	**A.12.3 Zálohování**
	Zálohy	**P.4**	Úplné zálohování by se mělo provádět pravidelně.	**A.12.3 Zálohování**
	Mobilní/přenosná zařízení	**Q.1**	Měly by se definovat a zdokumentovat postupy správy mobilních a přenosných zařízení, které stanoví jasná pravidla pro jejich správné používání.	**A. 6.2 Mobilní zařízení a práce na dálku**
	Mobilní/přenosná zařízení	**Q.2**	Mobilní zařízení, kterým je povolen přístup do informačního systému, by se měla předem zaregistrovat a autorizovat.	**A. 6.2 Mobilní zařízení a práce na dálku**
	Mobilní/přenosná zařízení	**Q.3**	Mobilní zařízení by měla podléhat stejným postupům kontroly přístupu (k systému zpracování dat) jako ostatní koncová zařízení.	**A. 6.2 Mobilní zařízení a práce na dálku**
	KATEGORIE OPATŘENÍ	**OPATŘENÍ**	**POPIS OPATŘENÍ**	**PŘÍSLUŠNÝ STANDARD ISO/IEC 27001: KONTROLA 2013**

	Zabezpečení životního cyklu aplikací	**R.1**	Během životního cyklu vývoje by se měla dodržovat nejlepší praxe, nejmodernější a uznávané postupy, rámce nebo standardy bezpečného vývoje.	**A.12.6 Technická správa zranitelnosti a A.14.2 Zabezpečení u procesů vývoje a podpory**
	Zabezpečení životního cyklu aplikací	**R.2**	Konkrétní bezpečnostní požadavky by se měly definovat v raných fázích životního cyklu vývoje.	**A.12.6 Technická správa zranitelnosti a A.14.2 Zabezpečení u procesů vývoje a podpory**
	Zabezpečení životního cyklu aplikací	**R.3**	Analogicky k bezpečnostním požadavkům by se měly přijmout specifické technologie a postupy určené k podpoře ochrany soukromí a osobních údajů (označované také jako technologie pro zvýšení ochrany soukromí (*Privacy Enhancing Technologies* - PET)).	**A.12.6 Technická správa zranitelnosti a A.14.2 Zabezpečení u procesů vývoje a podpory**
	Zabezpečení životního cyklu aplikací	**R.4**	Měly by se dodržovat standardy a postupy bezpečného kódování.	**A.12.6 Technická správa zranitelnosti a A.14.2 Zabezpečení u procesů vývoje a podpory**
	Zabezpečení životního cyklu aplikací	**R.5**	V průběhu vývoje by se mělo provádět testování a validace zavedení původních bezpečnostních požadavků.	**A.12.6 Technická správa zranitelnosti a A.14.2 Zabezpečení u procesů vývoje a podpory**
	Vymazání/likvidace dat	**S.1**	Před likvidací všech médií by se mělo provést jejich softwarové přepsání. V případech, kdy to není možné (CD, DVD atd.), je třeba provést fyzickou likvidaci.	**A. 8.3.2 Likvidace médií a A. 11.2.7 Bezpečná likvidace nebo opětovné použití zařízení**
	Vymazání/likvidace dat	**S.2**	Provede se skartace papírových a přenosných nosičů používaných k ukládání osobních údajů.	**A. 8.3.2 Likvidace médií a A. 11.2.7 Bezpečná likvidace nebo opětovné použití zařízení**
	Fyzické zabezpečení	**T.1**	Fyzický okruh infrastruktury systému IT by neměl být přístupný neautorizovaným osobám.	**A.11 - Fyzické zabezpečení a bezpečnost životního prostředí**