STANDARD CONTRACTUAL CLAUSES /STANDARDNÍ SMLUVNÍ DOLOŽKY

These **Standard Contractual Clauses** (hereinafter referred to as "SCC") effective on the day of the publishing in accordance with the Act No 340/2015 Coll. on the Register of Contracts (the Standard Contractual Clauses Effective Date"), are by and between

Tyto **Standardní smluvní doložky** (dále jen „SCC") nabývající účinnost dnem zveřejnění dle zákona č. 340/2015 Sb. o registru smluv (dále jen „datum účinnosti Standardních smluvních doložek"), se uzavírají mezi

Vojenská nemocnice Brno p.o., located at Zábrdovická 3, 615 00 Brno, Czech Republic, IČO (Company ID): 60555530, DIČ (VAT ID): CZ60555530, represented by plk. gšt. MUDr. Václav Masopust, Ph.D., MBA, LL.M, DBA, Director (the "Institution"),

Vojenskou nemocnicí Brno p.o., se sídlem Zábrdovická 3, 615 00 Brno, Česká republika , IČO : 60555530, DIČ: CZ60555530, zastoupenou plk. gšt. MUDr. Václavem Masopustem, Ph.D., MBA, LL.M, DBA, ředitelem (dále jen „Zdravotnické zařízení"),

ICON Clinical Research Limited, located at South County Business Park, Leopardstown, Dublin 18, Ireland, VAT ID IE-8201978R, represented by [redacted] ("ICON"), acting as an independent contractor for **Akros Pharma Inc.**, located at 302 Carnegie Center, Suite 300, Princeton, NJ 08540, United States of America (the "Sponsor"). ICON has agreed to accept certain obligations and duties of in respect of the conduct of the clinical trial in Czech Republic.

společností **ICON Clinical Research Limited**, se sídlem South County Business Park, Leopardstown, Dublin 18, Irsko, DIČ EU-IE8201978R, zastoupenou [redacted] (dále jen „ICON"), jednající jako nezávislý dodavatel společnosti **Akros Pharma, Inc.**, se sídlem 302 Carnegie Center, Suite 300, Princeton, NJ 08540, Spojené státy americké (dále jen „Zadavatel"). Společnost ICON se zavazuje převzít určité závazky a povinnosti týkající se provádění klinického hodnocení v České republice.

[redacted] serves as the principal investigator ("Investigator") for the Study.

[redacted] vystupuje jako hlavní zkoušející (dále jen „Zkoušející") odpovídající za Studii.

The Institution and the Investigator may be collectively referred to as the "Site".

Zdravotnické zařízení a Zkoušející mohou být dále společně označováni jen jako „Řešitelské centrum".

INTRODUCTORY PROVISIONS:

WHEREAS, under the terms of a certain Clinical Trial Agreement, dated February 26, 2024 (the "Agreement") by and among the parties, ICON on behalf of Sponsor, retained the Institution and Investigator to perform the research study entitled **"A Phase 2a, Multicenter, Randomized, Double-blind, Placebo-controlled, Parallel-group Study to Evaluate the Efficacy, Safety and Tolerability of JTT-861 Administered for 12 Weeks in Subjects with Heart Failure with Reduced Ejection Fraction (POWER-HF)"** (the "Study"), bearing protocol number **AT861-G-22-002** as may be amended from time to time (the "Protocol"), sponsored by ("Sponsor"), as more particularly described in the Agreement;

WHEREAS, ICON has been engaged by Sponsor to arrange, monitor, oversee and perform, or have performed, the Study pursuant to the Protocol by Site; and

WHEREAS, the parties hereto have entered into certain additional agreements with respect to modification of the Agreement and which they desire to memorialize in these SCC.

NOW, THEREFORE, in consideration of the premises and of the following mutual promises, covenants and conditions hereinafter set forth, the parties hereto agree as follows:

ÚVODNÍ USTANOVENÍ:

VZHLEDEM K TOMU, ŽE podle podmínek určité smlouvy o klinickém hodnocení ze dne 26. února 2024 (dále jen „Smlouva") mezi smluvními stranami, najala společnost ICON jménem Zadavatele Zdravotnické zařízení a Zkoušejícího k provedení výzkumné studie s názvem " „**Multicentrická, randomizovaná, dvojitě zaslepená, placebem kontrolovaná studie fáze 2a s paralelními skupinami k vyhodnocení účinnosti, bezpečnosti a snášenlivosti přípravku JTT-861 podávaného po dobu 12 týdnů u subjektů se srdečním selháním a sníženou ejekční frakcí (POWER-HF)"** (dále jen „Studie") s číslem protokolu **AT861-G-22-002** ve znění pozdějších dodatků (dále jen „Protokol"); jejímž zadavatelem je (dále jen „Zadavatel"), jak je podrobněji popsáno ve smlouvě;

VZHLEDEM K TOMU, ŽE společnost ICON byla Zadavatelem najata, aby zajistila, monitorovala, dohlížela a prováděla nebo nechala provádět Studii podle protokolu v Řešitelském centru; a

VZHLEDEM K TOMU, ŽE smluvní strany těchto SCC uzavřeli určité dodatečné dohody týkající se úpravy této Smlouvy, které chtějí zaznamenat v těchto SCC:

NA ZÁKLADĚ TOHOTO s ohledem na dále uvedené předpoklady a následující vzájemné přísliby, závazky a podmínky souhlasí smluvní strany s následujícím:

STANDARD CONTRACTUAL CLAUSES

STANDARDNÍ SMLUVNÍ DOLOŽKY

SECTION I

ODDÍL I

Clause 1

Doložka 1

Purpose and scope

Účel a oblast působnosti

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

a) Účelem těchto standardních smluvních doložek je zajistit dodržování požadavků uvedených v 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 (obecné nařízení o ochraně údajů) (1), pokud jde o předávání osobních údajů do třetí země.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

b) Strany:

i) fyzická nebo právnická osoba či osoby, orgán či orgány veřejné moci, agentura či agentury nebo jiný subjekt či jiné subjekty (dále jen „subjekt" či „subjekty") předávající osobní údaje, uvedené v příloze I části A (dále jen „vývozce údajů"), a

ii) subjekt či subjekty ve třetí zemi, přijímající přímo nebo nepřímo prostřednictvím jiného subjektu, jenž je rovněž stranou těchto doložek, osobní údaje od vývozce údajů, uvedené v příloze I části A (dále jen „dovozce údajů"),

se dohodly na těchto standardních smluvních doložkách (dále jen: „doložky").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

c) Tyto doložky se použijí s ohledem na předávání osobních údajů podle přílohy I části B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

d) Dodatek k těmto doložkám obsahující přílohy, na něž se v těchto doložkách odkazuje, tvoří nedílnou součást těchto doložek.

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915. / Pokud je vývozcem údajů zpracovatel, na nějž se vztahuje nařízení (EU) 2016/679 a který jedná jménem orgánu nebo subjektu Unie jako správce, spoléhání se na tyto doložky při zapojení jiného zpracovatele (dílčí zpracování), na kterého se nařízení (EU) 2016/679 nevztahuje, rovněž zajišťuje soulad s čl. 29 odst. 4 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie, a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí 1247/2002/ES (Úř. věst. L 295 ze dne 21. 11. 2018, s. 39), v rozsahu, v němž jsou tyto doložky a povinnosti týkající se ochrany údajů stanovené ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle čl. 29 odst. 3 nařízení (EU) 2018/1725 sladěny. To bude zejména případ, kdy se správce a zpracovatel spoléhají na standardní smluvní doložky obsažené v rozhodnutí 2021/915.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Doložka 2

Účinek a neměnnost doložek

a) Tyto doložky stanoví vhodné záruky, včetně vymahatelných práv subjektu údajů a účinné právní ochrany, podle čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) nařízení (EU) 2016/679 a s ohledem na předávání údajů od správců zpracovatelům a/nebo od zpracovatelů zpracovatelům, standardní smluvní doložky podle čl. 28 odst. 7 nařízení (EU) 2016/679, pokud nebudou změněny, s výjimkou výběru vhodného modulu (vhodných modulů) nebo za účelem přidání nebo aktualizace informací v dodatku. To smluvním stranám nebrání v tom, aby zahrnuly standardní smluvní doložky stanovené v těchto doložkách do širší smlouvy a/nebo přidaly další doložky nebo dodatečné záruky, pokud nebudou přímo nebo nepřímo v rozporu s těmito doložkami nebo nebudou dotčena základní práva nebo svobody subjektů údajů.

b) Těmito doložkami nejsou dotčeny povinnosti, které se vztahují na vývozce údajů na základě nařízení (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 9 – Intentionally left blank;

(iv) Clause 12 – Module One: Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Module One: Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Doložka 3

Oprávněné třetí strany

a) Subjekty údajů se mohou jako oprávněné třetí strany ve vztahu k vývozci a/nebo dovozci údajů dovolávat těchto doložek a vymáhat je, a to s následujícími výjimkami:

i) doložka 1, doložka 2, doložka 3, doložka 6, doložka 7;

ii) doložka 8 – modul 1: doložka 8.5 písm. e) a doložka 8.9 písm. b);

iii) doložka 9 – záměrně ponecháno prázdné;

iv) doložka 12 – modul 1: doložka 12 písm. a) a d);

v) doložka 13;

vi) doložka 15.1 písm. c), d) a e);

vii) doložka 16 písm. e);

viii) doložka 18 – modul 1: doložka 18 písm. a) a b).

b) Písmenem a) nejsou dotčena práva subjektů údajů podle nařízení (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the

Doložka 4

Výklad

a) Pokud tyto doložky používají pojmy, které jsou vymezeny v nařízení (EU) 2016/679, mají tyto pojmy

same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

stejný význam jako v uvedeném nařízení.

b) Tyto doložky je třeba číst a vykládat s ohledem na ustanovení nařízení (EU) 2016/679.

c) Tyto doložky nebudou vykládány žádným způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Doložka 5

Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek nebo které byly uzavřeny až po jejich sjednání, mají tyto doložky přednost.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Doložka 6

Popis předávání

Podrobnosti týkající se předávání, zejména kategorie osobních údajů, které jsou předávány, a účel nebo účely, pro které jsou předávány, jsou uvedeny v příloze I části B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Doložka 7 – Volitelná

Doložka o přistoupení

a) Subjekt, který není stranou těchto doložek, může se souhlasem stran k těmto doložkám kdykoli přistoupit, buď jako vývozce údajů, nebo jako dovozce údajů, a to vyplněním dodatku a podepsáním přílohy I části A.

b) Poté, co přistupující subjekt vyplní dodatek a podepíše přílohu I část A, stane se stranou těchto doložek a má práva a povinnosti vývozce údajů nebo dovozce údajů v souladu se svým určením v příloze I části A.

c) Přistupující subjekt nemá žádná práva ani povinnosti na základě těchto doložek plynoucí z období před tím, než se stal stranou.

SECTION II – OBLIGATIONS OF THE PARTIES

ODDÍL II – POVINNOSTI STRAN

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

Doložka 8

Záruky ochrany údajů

Vývozce údajů zaručuje, že vynaložil přiměřené úsilí, aby mohl stanovit, zda je dovozce údajů schopen – zavedením vhodných technických a organizačních opatření – plnit své povinnosti podle těchto doložek.

MODUL 1: Předání od správce správci

8.1. **Účelové omezení**

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání v souladu s přílohou I částí B. Osobní údaje může zpracovávat pro jiný účel pouze tehdy, pokud:

i) získal předchozí souhlas subjektu údajů;

ii) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

iii) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

8.2 **Transparentnost**

a) Aby subjekty údajů mohly účinně vykonávat svá práva podle doložky 10, dovozce údajů je informuje přímo nebo prostřednictvím vývozce údajů:

i) o své totožnosti a kontaktních údajích;

ii) o kategoriích zpracovávaných osobních údajů;

iii) o právu získat kopii těchto doložek;

iv) pokud má v úmyslu osobní údaje dále předat jakékoli třetí straně nebo stranám, o příjemci nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), o účelu takového dalšího předávání a o důvodu pro další předávání podle doložky 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

b) Písmeno a) se nepoužije, pokud subjekt údajů již tyto informace má, a to i v případě, že tyto informace již poskytl vývozce údajů, nebo pokud je poskytnutí těchto informací nemožné nebo by to pro dovozce údajů znamenalo nepřiměřené úsilí. V druhém případě dovozce údajů informace v maximální možné míře zveřejní.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

c) Strany poskytnou subjektu údajů na požádání a bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, mohou strany před sdílením kopie upravit část znění dodatku, ale poskytnou smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

d) Písmeny a) až c) nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.3 **Accuracy and data minimisation**

8.3. **Přesnost a minimalizace údajů**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

a) Každá strana zajistí, aby osobní údaje byly přesné a v případě potřeby aktualizovány. Dovozce údajů přijme veškerá smysluplná opatření, aby zajistil, že osobní údaje, které jsou nepřesné, budou s ohledem na účel nebo účely zpracování bezodkladně vymazány nebo opraveny.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

b) Pokud se jedna ze stran dozví, že osobní údaje, které předala nebo přijala, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje druhou stranu.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

c) Dovozce údajů zajistí, aby osobní údaje byly přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelu nebo účelů, pro které jsou zpracovávány.

8.4 **Storage limitation**

8.4. **Omezení uložení**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization (2) of the data and all back-ups at the end of the retention period.

Dovozce údajů uchová osobní údaje pouze po dobu nezbytnou pro účel nebo účely, pro který (které) jsou zpracovávány. Přijme vhodná technická nebo organizační opatření k zajištění dodržování této povinnosti, včetně vymazání nebo anonymizace (2) údajů a všech záloh na konci doby uchovávání.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible. / To vyžaduje anonymizaci údajů takovým způsobem, aby již nikdo nemohl být nikým identifikovatelný, v souladu s 26. bodem odůvodnění nařízení (EU) 2016/679, a aby byl tento proces nevratný.

8.5 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

8.5 **Zabezpečení zpracování**

a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění uvedených údajů (dále jen „porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení se řádně zohlední aktuální stav techniky, náklady na provedení, povaha, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekt údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování.

b) Strany se dohodly na technických a organizačních opatřeních stanovených v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

c) Dovozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

d) V případě porušení zabezpečení osobních údajů týkajícího se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení osobních údajů, včetně opatření ke zmírnění jeho možných nepříznivých účinků.

e) V případě porušení zabezpečení osobních údajů, které by mohlo vést k ohrožení práv a svobod fyzických osob, dovozce údajů bez zbytečného odkladu informuje vývozce údajů i příslušný dozorový úřad v souladu s doložkou 13. Toto ohlášení obsahuje i) popis povahy daného případu porušení zabezpečení osobních údajů (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů), ii) jeho pravděpodobných důsledků, iii) popis opatření, která byla přijata nebo byla navržena s cílem vyřešit dané porušení zabezpečení, a iv) údaje kontaktního místa, kde lze získat více informací. Není-li možné, aby dovozce údajů veškeré informace poskytl současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

f) V případě porušení zabezpečení osobních údajů, které pravděpodobně bude představovat vysoké riziko pro práva a svobody fyzických osob, dovozce údajů rovněž bez zbytečného odkladu podá hlášení dotčeným subjektům údajů o porušení zabezpečení osobních údajů a jeho povaze – v případě potřeby ve spolupráci s vývozcem údajů – a sdělí jim také informace uvedené v písm. e) bodu ii) až iv), pokud dovozce údajů nezavedl opatření za účelem značného snížení rizika pro práva a svobody fyzických osob nebo pokud dané hlášení nevyžaduje nepřiměřené úsilí. V posledně uvedeném případě dovozce údajů místo toho vydá veřejné oznámení nebo zajistí obdobné opatření, kterým veřejnost o porušení zabezpečení osobních údajů informuje.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

g) Dovozce údajů dokumentuje veškeré relevantní skutečnosti týkající se porušení zabezpečení osobních údajů, včetně jeho účinků a přijatých nápravných opatření, a vede si o tom záznamy.

8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.6 **Citlivé údaje**

Jestliže předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech nebo trestných činů (dále jen „citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky přizpůsobené zvláštní povaze údajů a souvisejícím rizikům. To může zahrnovat omezení personálu, který má povolen přístup k osobním údajům, dodatečná bezpečnostní opatření (jako je pseudonymizace) a/nebo dodatečná omezení s ohledem na další zpřístupnění.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union [3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

8.7 **Další předávání**

Dovozce údajů nezpřístupní osobní údaje třetí straně se sídlem mimo Evropskou unii ([3]) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen „další předávání"), ledaže by tato třetí strana byla podle příslušného modulu těmito doložkami vázána nebo by souhlasila s tím, že jimi bude vázána. K dalšímu předání dovozcem údajů jinak může dojít pouze tehdy, pokud:

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. / Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie na tři státy EHP Island, Lichtenštejnsko a Norsko. Na právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, se vztahuje Dohoda o EHP a byla začleněna do přílohy XI této dohody. Jakékoli zpřístupnění ze strany dovozce údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další přenos.

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

i) se provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dotčené zpracování;

iii) třetí strana uzavře s dovozcem údajů závaznou dohodu zajišťující stejnou úroveň ochrany údajů jako podle těchto doložek a dovozce údajů poskytne kopii těchto záruk vývozci údajů;

iv) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení;

v) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, nebo

vi) pokud neplatí žádná z dalších podmínek, dovozce údajů získal výslovný souhlas subjektu údajů s dalším předáváním v konkrétní situaci poté, co jej informoval o jeho účelu nebo účelech, totožnosti příjemce a možných rizicích, která pro něj vyplývají z takového předávání vzhledem k nedostatku vhodných záruk ochrany údajů. V takovém případě dovozce údajů informuje vývozce údajů a na žádost vývozce údajů mu předá kopii informací poskytnutých subjektu údajů.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.8 **Zpracování z pověření dovozce údajů**

Dovozce údajů zajistí, aby jakákoli osoba, která jedná z jeho pověření, včetně zpracovatele, zpracovávala údaje pouze na základě jeho pokynů.

8.9 **Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

8.9 **Dokumentace a plnění povinností**

a) Každá strana musí být schopna prokázat plnění svých povinností podle těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování, za jejichž provádění odpovídá.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

b) Dovozce údajů tuto dokumentaci na požádání zpřístupní příslušnému dozorovému úřadu.

Clause 9

Intentionally left blank

Doložka 9

Záměrně ponecháno prázdné

Clause 10

Data subject rights

Doložka 10

Práva subjektu údajů

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (4) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

MODUL 1: Předání od správce správci

a) Dovozce údajů, případně za pomoci vývozce údajů, vyřizuje veškeré dotazy a žádosti, které obdrží od subjektu údajů, týkající se zpracování jeho osobních údajů a výkonu jeho práv podle těchto doložek, a to bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení dotazu nebo žádosti. (4) Dovozce údajů přijme vhodná opatření k usnadnění vyřizování těchto dotazů, žádostí a výkonu práv subjektu údajů. Veškeré informace poskytované subjektu údajů musí být ve srozumitelném a snadno přístupném znění za použití jasných a jednoduchých jazykových prostředků.

(4) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension. / Tuto lhůtu lze prodloužit nejvýše o další dva měsíce, a to v rozsahu nezbytném s ohledem na složitost a počet žádostí. Dovozce údajů o každém takovém prodloužení řádně a neprodleně informuje subjekt údajů.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in

b) Na žádost subjektu údajů dovozce údajů zejména bezplatně:

i) poskytne subjektu údajů potvrzení o tom, zda se zpracovávají osobní údaje, které se ho týkají, a v takovém případě mu poskytne kopii údajů, které se ho týkají, a informace uvedené v příloze I; pokud osobní údaje byly nebo budou dále předávány, poskytne informace o příjemcích nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), kterým osobní údaje byly nebo budou dále předávány, účel těchto dalších předání a jejich důvod v souladu s doložkou 8.7; a poskytne informace o právu podat stížnost u dozorového úřadu v souladu s doložkou 12 písm. c) bodem i);

ii) opraví nepřesné nebo neúplné údaje týkající se subjektu údajů;

iii) vymaže osobní údaje týkající se subjektu údajů, pokud tyto údaje jsou nebo byly zpracovávány v rozporu s kteroukoli z těchto doložek, která zajišťuje práva náležející oprávněné třetí straně, nebo pokud subjekt údajů odvolá souhlas, na kterém je zpracování založeno.

c) Pokud dovozce údajů zpracovává osobní údaje pro účely přímého marketingu, přestane je pro tyto účely zpracovávat, vznese-li proti tomu subjekt údajů námitky.

d) Dovozce údajů nepřijme rozhodnutí založené výhradně na automatizovaném zpracování předávaných osobních údajů (dále jen „automatizované rozhodnutí"), které by mělo právní účinky týkající se subjektu údajů nebo by ho obdobně významně ovlivnilo, ledaže by k tomu subjekt údajů dal výslovný souhlas, nebo pokud by mu to bylo na základě právních předpisů země určení povoleno, za předpokladu, že takové právní předpisy stanoví vhodná opatření na ochranu práv a oprávněných zájmů subjektu údajů. V tomto případě dovozce údajů, v případě potřeby ve spolupráci s vývozcem údajů:

i) informuje subjekt údajů o předpokládaném automatizovaném rozhodnutí, předpokládaných důsledcích a použitém postupu; a

ii) zavede vhodná ochranná opatření, přinejmenším tím, že umožní subjektu údajů napadnout rozhodnutí, vyjádřit svůj názor a dosáhnout přezkumu prováděného člověkem.

e) Jestliže jsou žádosti subjektu údajů nepřiměřené,

particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

zejména proto, že se opakují, může dovozce údajů buď uložit přiměřený poplatek, v němž budou zohledněny administrativní náklady související s vyhověním dané žádosti, nebo může odmítnout žádosti vyhovět.

f) Dovozce údajů může žádost subjektu údajů odmítnout, pokud je takové odmítnutí umožněno podle práva země určení a je v demokratické společnosti nezbytné a přiměřené za účelem ochrany jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679.

g) Pokud má dovozce údajů v úmyslu žádost subjektu údajů odmítnout, informuje subjekt údajů o důvodech odmítnutí a možnosti podat stížnost u příslušného dozorového úřadu a/nebo požádat o soudní ochranu.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Doložka 11

Náprava

a) Dovozce údajů transparentně a ve snadno přístupném formátu informuje subjekty údajů prostřednictvím individuálního oznámení nebo na svých internetových stránkách o kontaktním místě oprávněném vyřizovat stížnosti. Takové místo neprodleně vyřídí jakékoli stížnosti, které od subjektu údajů přijme.

MODULE ONE: Transfer controller to controller

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

MODUL 1: Předání od správce správci

b) V případě sporu mezi subjektem údajů a jednou ze smluvních stran týkajícího se dodržování těchto doložek vyvine tato strana veškeré úsilí k tomu, aby takovou záležitost vyřešila smírně a včas. Strany se o těchto sporech navzájem informují a v příslušných případech při jejich řešení spolupracují.

c) Pokud se subjekt údajů dovolává práva ve prospěch oprávněné třetí strany podle doložky 3, dovozce údajů akceptuje rozhodnutí subjektu údajů:

i) podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště nebo místa výkonu práce nebo u příslušného dozorového úřadu podle doložky 13;

ii) postoupit spor příslušným soudům ve smyslu doložky 18.

d) Strany jsou srozuměny s tím, že subjekt údajů může být zastoupen neziskovým subjektem, organizací nebo sdružením za podmínek stanovených v čl. 80 odst. 1 nařízení (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

e) Dovozce údajů dodržuje rozhodnutí závazné podle platného práva EU nebo členského státu.

f) Dovozce údajů souhlasí s tím, že výběr provedený subjektem údajů nebude mít vliv na jeho hmotná a procesní práva požadovat nápravu v souladu s platnými právními předpisy.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

Doložka 12

Odpovědnost

MODUL 1: Předání od správce správci

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

a) Každá strana je vůči druhé straně/ostatním stranám odpovědná za jakoukoli újmu, kterou druhé straně/ostatním stranám při porušení těchto doložek způsobí.

b) Každá strana je odpovědná vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou strana způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek. Tím není dotčena odpovědnost vývozce údajů podle nařízení (EU) 2016/679.

c) Pokud je za újmu způsobenou subjektu údajů v důsledku porušení těchto doložek odpovědná více než jedna strana, nesou společnou a nerozdílnou odpovědnost všechny odpovědné strany a subjekt údajů je oprávněn proti kterékoli z těchto stran podat žalobu u soudu.

d) Smluvní strany se dohodly, že pokud je jedna ze smluvních stran odpovědná podle písmene c), je oprávněna požadovat od druhé smluvní strany/ostatních smluvních stran zpět část náhrady újmy odpovídající její odpovědnosti za újmu.

e) Dovozce údajů se nemůže dovolávat jednání zpracovatele nebo dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

Doložka 13

Dohled

MODUL 1: Předání od správce správci

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

a) [Pokud je vývozce údajů usazen v členském státě EU:] Dozorový úřad uvedený v příloze I části C, který je odpovědný za zajištění, že vývozce údajů dodržuje nařízení (EU) 2016/679, pokud jde o předávání údajů, jedná jako příslušný dozorový úřad.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

b) Dovozce údajů souhlasí s tím, že se podřídí pravomoci příslušného dozorového úřadu a bude s ním spolupracovat v rámci všech postupů zaměřených na zajištění dodržování těchto doložek. Dovozce údajů zejména souhlasí s tím, že bude reagovat na dotazy, podrobovat se auditům a dodržovat opatření přijatá dozorovým úřadem, včetně nápravných a kompenzačních opatření. Dozorovému úřadu poskytne písemné potvrzení, že byla přijata nezbytná opatření.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

ODDÍL III – MÍSTNÍ PRÁVNÍ PŘEDPISY A POVINNOSTI V PŘÍPADĚ PŘÍSTUPU ORGÁNŮ VEŘEJNÉ MOCI

Clause 14

Doložka 14

Local laws and practices affecting compliance with the Clauses MODULE ONE: Transfer controller to controller

Místní právní předpisy a postupy mající dopad na dodržování doložek MODUL 1: Předání od správce správci

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

a) Strany zaručují, že nemají důvod se domnívat, že právní předpisy a postupy ve třetí zemi určení, které se vztahují na zpracování osobních údajů dovozcem údajů, včetně jakýchkoli požadavků na zpřístupnění osobních údajů nebo opatření, kterými se povoluje přístup orgánům veřejné moci, brání dovozci údajů při plnění svých povinností podle těchto doložek. To je založeno na předpokladu, že právní předpisy a postupy, které respektují podstatu základních práv a svobod a nepřekračují to, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679, nejsou v rozporu s těmito doložkami.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

b) Smluvní strany prohlašují, že při poskytování záruky uvedené v písmenu a) náležitě zohlednily zejména následující prvky:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

i) konkrétní okolnosti předání, včetně délky zpracovatelského řetězce, počtu zapojených subjektů a použitých kanálů pro přenos údajů, zamýšlené další předání, druh příjemce, účely zpracování, kategorie a formát předávaných osobních údajů, hospodářské odvětví, v němž se předávání uskutečňuje, místo, kde se předané údaje uchovávají;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant

ii) právní předpisy a postupy třetí země určení – včetně těch, které vyžadují zpřístupnění údajů orgánům veřejné moci nebo povolují přístup těchto orgánů – relevantní s ohledem

in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (5);

na konkrétní okolnosti předání, jakož i použitelná omezení a záruky (5);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

iii) veškeré příslušné smluvní, technické nebo organizační záruky zavedené za účelem doplnění záruk podle těchto doložek, včetně opatření uplatňovaných během předání a zpracování osobních údajů v zemi určení.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

c) Dovozce údajů zaručuje, že při provádění posouzení podle písmene b) vynaložil maximální úsilí, aby poskytl vývozci údajů relevantní informace, a souhlasí s tím, že bude při zajišťování dodržování těchto doložek s vývozcem údajů i nadále spolupracovat.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

d) Strany souhlasí, že posouzení podle písmene b) zdokumentují a na požádání zpřístupní příslušnému dozorovému úřadu.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

e) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, pokud má po vyjádření souhlasu s těmito ustanoveními a po dobu trvání smlouvy důvod se domnívat, že se na něj vztahují, nebo se začaly vztahovat právní předpisy nebo postupy, které nejsou v souladu s požadavky podle písmene a), a to i po změně v právních předpisech třetí země nebo opatření (jako je například žádost o poskytnutí údajů), jež svědčí o tom, že uplatňování těchto právních předpisů v praxi není v souladu s požadavky uvedenými v písmeni a).

(5) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. / Pokud jde o dopad takových právních předpisů a postupů na dodržování těchto doložek, za součást celkového posouzení lze považovat různé prvky. Mezi tyto prvky mohou patřit relevantní a zdokumentované praktické zkušenosti s předchozími případy žádostí o zpřístupnění od orgánů veřejné moci nebo neexistence takových žádostí, které pokrývají dostatečně reprezentativní časový rámec. Týká se to zejména interních záznamů nebo jiné dokumentace vypracovávané průběžně v souladu s náležitou péčí a certifikované na úrovni vrcholového vedení za předpokladu, že tyto informace lze v souladu s právními předpisy sdílet se třetími stranami. Pokud se na základě této praktické zkušenosti dospěje k závěru, že dovozci údajů nebude bráněno v dodržování těchto doložek, je třeba to podpořit dalšími relevantními, objektivními prvky a je na smluvních stranách, aby pečlivě zvážily, zda tyto prvky mají společně dostatečnou váhu na podporu tohoto závěru, pokud jde o jejich spolehlivost a reprezentativnost. Smluvní strany musí zejména zohlednit, zda jsou jejich praktické zkušenosti potvrzeny veřejně dostupnými nebo jinak přístupnými spolehlivými informacemi o existenci či neexistenci žádostí ve stejném odvětví a/nebo o uplatňování práva v praxi, jako je například judikatura a zprávy nezávislých orgánů dohledu, a nejsou s nimi v rozporu.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation . The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

f) Po oznámení podle písmene e), nebo pokud má vývozce údajů jinak důvod se domnívat, že dovozce údajů již nemůže plnit své povinnosti na základě těchto doložek, vývozce údajů neprodleně určí vhodná opatření (např. technická nebo organizační opatření k zajištění bezpečnosti a důvěrnosti), která má přijmout vývozce údajů a/nebo dovozce údajů k řešení situace. Vývozce údajů pozastaví předávání údajů, pokud se domnívá, že pro toto předávání nemohou být zajištěny žádné vhodné záruky, nebo pokud mu dá pokyn příslušný dozorový úřad. V tomto případě je vývozce údajů oprávněn vypovědět smlouvu, pokud jde o zpracování osobních údajů podle těchto doložek. Jestliže smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak. Jestliže je smlouva vypovězena podle této doložky, použije se doložka 16 písm. d) a e).

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

Doložka 15

Povinnost dovozce údajů v případě přístupu orgánů veřejné moci

MODUL 1: Předání od správce správci

15.1 **Oznámení**

a) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, a je-li to možné, subjekt údajů (v případě potřeby s pomocí vývozce údajů), pokud:

i) na základě právních předpisů země určení obdrží právně závaznou žádost od orgánu veřejné moci, včetně soudních orgánů, o zpřístupnění osobních údajů předaných podle těchto doložek; takové oznámení obsahuje informace o požadovaných osobních údajích, dožadujícím orgánu, právním základu žádosti a poskytnuté odpovědi, nebo

ii) se dozví o jakémkoli přímém přístupu orgánů veřejné moci k osobním údajům předávaným podle těchto doložek v souladu s právními předpisy země určení; takové oznámení obsahuje všechny informace dostupné dovozci.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

b) Pokud je podle právních předpisů země určení dovozci údajů zakázáno informovat vývozce údajů a/nebo subjekt údajů, souhlasí dovozce údajů s tím, že za účelem co nejrychlejšího sdělení co největšího množství informací vynaloží maximální úsilí, aby od tohoto zákazu bylo upuštěno. Dovozce údajů souhlasí s tím, že zdokumentuje své maximální úsilí, aby je mohl na žádost vývozce údajů prokázat.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

c) Je-li to povoleno právními předpisy země určení, dovozce údajů souhlasí s tím, že bude poskytovat vývozci údajů v pravidelných intervalech po dobu trvání smlouvy co nejrelevantnější informace o přijatých žádostech (zejména informace o počtu žádostí, druhu požadovaných údajů, dožadujícím orgánu nebo orgánech, zda byly tyto žádosti napadeny a výsledek takového napadení atd.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

d) Dovozce údajů souhlasí s tím, že po dobu trvání smlouvy bude informace podle písmene a) až c) uchovávat a na vyžádání je poskytne příslušnému dozorovému úřadu.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

e) Písmeny a) až c) není dotčena povinnost dovozce údajů podle doložky 14 písm. e) a doložky 16 neprodleně informovat vývozce údajů, pokud není schopen tyto doložky dodržovat.

15.2 **Review of legality and data minimisation**

15.2 **Přezkum zákonnosti a minimalizace údajů**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

a) Dovozce údajů souhlasí s tím, že přezkoumá zákonnost žádosti o poskytnutí údajů, zejména zda nepřekročila meze pravomocí udělených dožadujícímu orgánu veřejné moci, a že žádost napadne, pokud po pečlivém posouzení dojde k závěru, že existují opodstatněné důvody se domnívat, že žádost je podle právních předpisů země určení, platných závazků podle mezinárodního práva a zásad mezinárodní zdvořilosti protiprávní. Dovozce údajů za stejných podmínek využívá možností odvolání. Při napadení žádosti dovozce údajů přijme předběžná opatření s cílem pozastavit účinky žádosti, dokud příslušný soudní orgán nerozhodne o její opodstatněnosti. Nezpřístupní požadované osobní údaje, dokud mu taková povinnost nebude stanovena na základě platných procesních pravidel. Těmito požadavky nejsou dotčeny povinnosti dovozce údajů podle doložky 14 písm. e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

b) Dovozce údajů souhlasí s tím, že zdokumentuje své právní posouzení i jakékoli napadení žádosti o poskytnutí údajů a v rozsahu povoleném právními předpisy země určení zpřístupní dokumentaci vývozci údajů. Na požádání ji rovněž zpřístupní příslušnému dozorovému úřadu.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

c) Dovozce údajů souhlasí s poskytnutím minimálního přípustného množství informací při odpovědi na žádost o zpřístupnění, a to na základě přiměřeného výkladu žádosti.

SECTION IV – FINAL PROVISIONS

ODDÍL IV – ZÁVĚREČNÁ USTANOVENÍ

Clause 16

Doložka 16

Non-compliance with the Clauses and termination

Nedodržení doložek a vypovězení

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

a) Dovozce údajů neprodleně informuje vývozce údajů, pokud není z jakéhokoli důvodu schopen tyto doložky dodržet.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

b) Pokud dovozce údajů poruší tyto doložky nebo není schopen tyto doložky dodržet, vývozce údajů pozastaví předávání osobních údajů dovozci údajů, dokud není dodržování opět zajištěno nebo smlouva vypovězena. Tímto není dotčena doložka 14 písm. f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

c) Vývozce údajů je oprávněn vypovědět smlouvu v rozsahu, v němž se jedná o zpracování osobních údajů podle těchto doložek, pokud:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

i) vývozce údajů pozastavil předávání osobních údajů dovozci údajů podle písm. b) a dodržování těchto doložek není v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení obnoveno;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

ii) dovozce údajů tyto doložky podstatně nebo trvale porušuje; nebo

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

iii) dovozce údajů nedodrží závazné rozhodnutí příslušného soudu nebo dozorového úřadu týkajícího se jeho povinností podle těchto doložek.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties

V takových případech o nedodržení informuje příslušný dozorový úřad. Pokud smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak.

have agreed otherwise.

(d) [For Module One: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

d) [V případě modulu 1: Osobní údaje, které byly předány před vypovězením smlouvy podle písmene c), musí být podle volby vývozce údajů neprodleně vráceny vývozci údajů nebo vymazány v celém rozsahu. To samé se uplatní ve vztahu k veškerým kopiím údajů.] Dovozce údajů potvrdí vývozci údajů, že byly údaje vymazány. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují předané osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to uvedené místní právo vyžaduje.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

e) Kterákoli ze stran může odvolat svůj souhlas s tím, že bude vázána těmito doložkami, pokud i) Evropská komise přijme rozhodnutí podle čl. 45 odst. 3 nařízení (EU) 2016/679 týkající se předávání osobních údajů, na které se tyto doložky vztahují, nebo ii) se nařízení (EU) 2016/679 stane součástí právního rámce země, do které jsou osobní údaje předávány. Tím nejsou dotčeny další povinnosti vztahující se na dotčené zpracování podle nařízení (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of the Czech Republic.

Doložka 17

Rozhodné právo

MODUL 1: Předání od správce správci

Tyto doložky se řídí právem jednoho z členských států EU, pokud takové právo umožňuje uplatňovat práva náležející oprávněné třetí straně. Strany se dohodly, že se budou řídit právem České republiky.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Czech Republic.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Doložka 18

Volba soudu a příslušnost

MODUL 1: Předání od správce správci

a) Veškeré spory vyplývající z těchto doložek budou řešeny soudy členského státu EU.

b) Strany se dohodly, že se budou řídit soudy České republiky.

c) Subjekt údajů může rovněž zahájit soudní řízení proti vývozci údajů a/nebo dovozci údajů před soudy členského státu, v němž má subjekt údajů své obvyklé bydliště.

d) Smluvní strany se dohodly, že se příslušnosti těchto soudů podřídí.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

DODATEK

VYSVĚTLIVKY:

Musí být možné jasně rozlišit informace, které se vztahují na každé předání nebo každou kategorii předání, a v tomto ohledu určit příslušnou úlohu/příslušné úlohy stran v postavení vývozce/vývozců údajů a/nebo dovozce/dovozců údajů. To nemusí nutně vyžadovat vyplnění a podepsání samostatných dodatků pro každé předání/kategorii předání a/nebo smluvní vztah, pokud lze této transparentnosti dosáhnout prostřednictvím jednoho dodatku. Pokud je to však nutné k zajištění dostatečné srozumitelnosti, měly by se použít samostatné dodatky.

ANNEX I

A. **LIST OF PARTIES**

MODULE ONE: Transfer controller to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Vojenská nemocnice Brno, p.o.

   Address: Zábrdovická 3, 615 00 Brno, Czech Republic

   Contact person's name, position and contact details: [redacted]

   Activities relevant to the data transferred under these Clauses: Transfer of personal data to data importer as necessary for data importer to perform clinical research.

   Signature: . . . . . .

   Name: plk. gšt. MUDr. Václav Masopust, Ph.D., MBA, LL.M, DBA

   Title: Director

   Date: . . . . . .

   Role: controller for Module 1

PŘÍLOHA I

A. **SEZNAM SMLUVNÍCH STRAN**

MODUL 1: Předání od správce správci

Vývozce (vývozci) údajů: *[Totožnost a kontaktní údaje vývozce/vývozců údajů a v příslušném případě jeho/jejich pověřence pro ochranu osobních údajů a/nebo zástupce v Evropské unii]*

1. Jméno/název: Vojenská nemocnice Brno, p.o.

   Adresa: Zábrdovická 3, 615 00 Brno, Česká republika

   Jméno, funkce a kontaktní údaje kontaktní osoby: [redacted]

   Činnosti relevantní pro předávání údajů na základě těchto doložek: Předávání osobních údajů dovozci údajů, pokud je to nezbytné pro dovozce údajů k provádění klinického výzkumu.

   Podpis: . . . . . .

   Jméno: plk. gšt. MUDr. Václav Masopust, Ph.D., MBA, LL.M, DBA

   Funkce: ředitel

   Datum: . . . . . .

   Úloha: Správce pro modul 1

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Akros Pharma Inc.

   Address: 302 Carnegie Center, Suite 300, Princeton, NJ 08540, USA

   Contact person's name, position and contact details: [redacted]

   Activities relevant to the data transferred under these Clauses: To conduct and manage clinical trials, perform analysis and reporting of the results, ensure safety monitoring, fulfill regulatory requirements, and any other activities necessary for the successful conduct and analysis of the clinical trials and research and development thereafter of the drugs and compounds used in the clinical trials.

   ICON Clinical Research Limited signs on behalf of AKROS by virtue of Power of Attorney

   Signature: .....

   Name: [redacted]

   Title: [redacted]

   Date: .....

   Role: controller

Dovozce nebo dovozci údajů: *[Totožnost a kontaktní údaje dovozce/dovozců údajů, včetně jakékoli kontaktní osoby, která je odpovědná za ochranu údajů]*

1. Jméno/název: Akros Pharma Inc.

   Adresa: 302 Carnegie Center, Suite 300, Princeton, NJ 08540, USA

   Jméno, funkce a kontaktní údaje kontaktní osoby: [redacted]

   Činnosti relevantní pro předávání údajů na základě těchto doložek: Provádění a řízení klinických hodnocení, provádění analýz a podávání zpráv o výsledcích, zajištění monitorování bezpečnosti, plnění regulačních požadavků a jakékoli další činnosti nezbytných pro úspěšné provádění a analýzu klinických hodnocení a následný výzkum a vývoj léčiv a sloučenin používaných v klinických hodnoceních.

   ICON Clinical Research Limited podepisuje jménem AKROS na základě plné moci

   Podpis: .....

   Jméno: [redacted]

   Funkce: [redacted]

   Datum: .....

   Úloha: Správce

B. **DESCRIPTION OF TRANSFER**

MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred

Healthcare professionals
Patients
Patients' babies (in case of pregnant patient or pregnant partner of a patient)

Categories of personal data transferred

B. **POPIS PŘEDÁNÍ**

MODUL 1: Předání od správce správci

Kategorie subjektů údajů, jejichž osobní údaje se předávají

Zdravotničtí pracovníci
Pacienti
Děti pacientů (v případě těhotné pacientky nebo těhotné partnerky pacienta)

Kategorie předávaných osobních údajů

For healthcare professionals:

- Name, work contact details (address, telephone number and email address);
- CV including work experience, qualifications, registrations and memberships;
- Bank account details for payment processing (if the professional is paid by Sponsor or Icon); and
- Periodic financial disclosure forms if the professional meets the criteria to complete the US Food and Drug Administration (FDA) Form 1572 reporting requirements or equivalent local law requirements.

For patients (including patients' babies):

- Subject ID number;
- Gender (if authorized by local laws);
- Year of birth/age;
- Laboratory and echocardiography imaging data; and
- Outcome of the pregnancy, body weight and height of the patient's baby.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

For patients (including patients' babies):

- Health data; and
- Racial or ethnic origins (if authorized by local laws).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer is expected to take place on a continuous basis, unless agreements or instructions establish otherwise.

Nature of the processing

The personal data transferred (or otherwise made available) by the Data Exporter to the Data Importer may be subject to the following processing activities: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pro zdravotnické pracovníky:

- jméno, pracovní kontaktní údaje (adresa, telefonní číslo a e-mailová adresa);
- životopis, který bude obsahovat pracovní zkušenosti, kvalifikaci, registrace a členství;
- bankovní údaje pro zpracování plateb (pokud je odborník placen zadavatelem nebo společností Icon); a
- formuláře pro pravidelné zveřejňování finančních údajů, pokud odborník splňuje kritéria pro vyplnění formuláře 1572 amerického Úřadu pro kontrolu potravin a léčiv (FDA) nebo rovnocenné požadavky místních právních předpisů.

Pro pacienty (včetně dětí pacientů):

- identifikační číslo subjektu;
- pohlaví (pokud je povoleno místními právními předpisy);
- rok narození/věk;
- laboratorní údaje a údaje ze zobrazovacího echokardiografického vyšetření; a
- výsledek těhotenství, tělesná hmotnost a výška dítěte pacienta.

Citlivé údaje, které se předávají (v příslušných případech), a uplatněná omezení nebo záruky, jež plně zohledňují povahu údajů a související rizika, například přísné účelové omezení, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamu o přístupu k údajům, omezení pro další předávání nebo dodatečná bezpečnostní opatření.

Pro pacienty (včetně dětí pacientů):

- zdravotní údaje; a
- rasový nebo etnický původ (pokud je povoleno místními právními předpisy).

Četnost předávání (např. zda jsou údaje předávány jednorázově nebo průběžně).

Očekává se, že předávání bude probíhat průběžně, pokud smlouvy nebo pokyny nestanoví jinak.

Povaha zpracování

Osobní údaje, které vývozce údajů předává (nebo jinak zpřístupní) dovozci údajů, mohou podléhat těmto činnostem zpracování: shromažďování, zaznamenávání, organizace, strukturování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, používání, zpřístupnění přenosem, šíření nebo jiné zpřístupnění, seřazování nebo kombinování, omezení, výmaz nebo zničení.

Purpose(s) of the data transfer and further processing

- For healthcare professionals: management and administration of the relationship with the healthcare professional (including confirming their qualifications and experience, communicating about the clinical study, complying with financial reporting requirements under applicable local laws in respect of the payments made for the services provided and conducting training where applicable);
- For patients: processing of patients data in the context of the research study for the product JTT-861 as described in the Informed Consent Form (ICF), including conducting and overseeing the study, checking the patient's suitability to take part in the study, monitoring the treatment, analyzing the treatment results and monitoring and reporting adverse events.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data transferred (or otherwise made available) by the Data Exporter to the Data Importer will be retained for as long as necessary to perform the study and this may be up to 25 years once the study has finished depending on country regulations, as specifically agreed between the Parties, and in compliance with applicable legal obligations.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of the processing are the same as listed above.

Účel nebo účely předání údajů a další zpracování

- Pro zdravotnické pracovníky: Řízení a správa vztahu se zdravotnickým pracovníkem (včetně potvrzení jeho kvalifikace a zkušeností, komunikace týkající se klinické studie, dodržování požadavků na podávání finančních informací podle platných místních právních předpisů, pokud jde o platby provedené za poskytnuté služby a případně za provádění školení).
- Pro pacienty: Zpracování údajů pacientů v kontextu výzkumné studie pro přípravek JTT-861, jak je popsáno ve formuláři informovaného souhlasu (FIS), včetně provádění studie a dohledu nad studií, kontroly vhodnosti pacienta k účasti ve studii, sledování léčby, analýzy výsledků léčby a sledování a hlášení nežádoucích účinků.

Doba, po kterou budou osobní údaje uchovávány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby

Osobní údaje, které vývozce údajů předává (nebo jinak zpřístupní) dovozci údajů, budou uchovány po dobu nezbytnou k provedení studie, a to až 25 let po ukončení studie v závislosti na předpisech příslušné země, jak je výslovně dohodnuto mezi stranami, a v souladu s platnými zákonnými povinnostmi.

Pokud jde o předávání (dílčím) zpracovatelům, rovněž uveďte předmět, povahu a trvání zpracování

Předmět, povaha a doba zpracovávání jsou stejné jako ty, jež jsou uvedeny výše.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

Identify the competent supervisory authority/ies in accordance with Clause 13

Office for Personal Data Protection

Úřad pro ochranu osobních údajů (The office for personal data protection)
Pplk. Sochora 27
170 00 Praha 7
Czech Republic

Tel. +420 234 665 111
ID datové schránky: qkbaa2n

E-mail: posta@uoou.cz

Czech Republic

C. PŘÍSLUŠNÝ DOZOROVÝ ÚŘAD

MODUL 1: Předání od správce správci

V souladu s doložkou 13 určete příslušný dozorový úřad nebo příslušné dozorové úřady.

Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
Česká republika

Tel. +420 234 665 111
ID datové schránky: qkbaa2n

E-mail: posta@uoou.cz

Česká republika

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

For personal data of data subjects in all categories

- Role-Based Access Control (RBAC): Implement role-based access control within the organization to restrict access to data, including personal data, based on the roles and responsibilities of users. Grant permissions ensuring that users can only access data they are authorized to see, and specifically limit access to personal data to those who require it for legitimate purposes.
- Network Split: There is firewall between internal LAN and Clinical development LAN, so that general user doesn't have access to clinical file server and other clinical systems.
- User Access Control and Access Control Reviews: Implement strict user access controls to ensure that only authorized individuals have access to sensitive information. Regularly review and evaluate the effectiveness of these controls to ensure that access is restricted to authorized personnel. Consistently review user accounts to confirm that only appropriate personnel have access and deactivate accounts that are no longer needed.
- Regular Data Backups: Perform regular backups of data, including personal data, and ensure that they are securely stored in a different location from the primary data. Keep a copy of the system at an off-site data center. Schedule the backups to ensure that data can be restored after an incident. Retain the backup sets on the file server for 60 days.
- Off-site Backup Storage: Store backup data in a different location to protect against physical damage.
- Disaster Recovery and Incident Response Plan: Develop a comprehensive disaster recovery plan that includes procedures for restoring personal data. Develop and maintain an incident response plan to ensure a quick and effective response to any data breaches or security incidents. Have a dedicated incident response team that can act quickly to restore data availability in case of an incident.

PŘÍLOHA II

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ BEZPEČNOSTI ÚDAJŮ

MODUL 1: Předání od správce správci

VYSVĚTLIVKY:

Technická a organizační opatření musí být popsána konkrétně (nikoli obecně). Viz také obecnou poznámku na první stránce dodatku, týkající se zejména potřeby jasně uvést, která opatření se vztahují na každé jednorázové nebo souborné předání.

Pro osobní údaje subjektů údajů ve všech kategoriích

- Řízení přístupu na základě rolí (RBAC): Zavedení řízení přístupu na základě rolí v rámci organizace s cílem omezit přístup k údajům, včetně osobních údajů, na základě úloh a povinností uživatelů. Udělit povolení, která zajistí, že uživatelé budou mít přístup pouze k údajům, pro které mají oprávnění, a konkrétně omezit přístup k osobním údajům na osoby, které je potřebují pro legitimní účely.
- Rozdělení sítí: Mezi interní LAN a LAN klinického vývoje je firewall, takže běžný uživatel nemá přístup k serveru klinických souborů a dalším klinickým systémům.
- Řízení přístupu uživatelů a přezkoumání řízení přístupu: Zavedení přísné kontroly přístupu uživatelů, aby bylo zajištěno, že k citlivým informacím budou mít přístup pouze oprávněné osoby. Pravidelná kontrola a vyhodnocování účinnosti těchto kontrol, aby bylo zajištěno, že je přístup omezen na oprávněné osoby. Soustavná kontrola uživatelských účtů, aby bylo potvrzeno, že přístup mají pouze příslušní pracovníci, a deaktivace účtů, které již nejsou potřeba.
- Pravidelné zálohování dat: Provádění pravidelného zálohování dat, včetně osobních dat, a zajištění, aby byla bezpečně uložena na jiném místě než primární data. Uchovávání kopie systému v datovém centru mimo pracoviště. Plánované zálohování, aby bylo zajištěna možnost obnovení dat po incidentu. Uchovávání sad záloh na souborovém serveru po dobu 60 dnů.
- Záložní úložiště mimo pracoviště: Uložení zálohovaných údajů na jiném místě, aby byly chráněny před fyzickým poškozením.
- Plán obnovení dat po havárii a odezvy na incidenty: Vypracování komplexního plánu obnovení dat po havárii, který zahrnuje postupy pro obnovení osobních údajů. Vytvoření a udržování plánu odezvy na incidenty, aby byla zajištěna rychlá a efektivní odezva na jakékoli porušení zabezpečení údajů nebo bezpečnostní incidenty. Ustanovení vyhrazeného týmu pro odezvu na incidenty, který je schopen rychle jednat a obnovit dostupnost údajů v případě incidentu.

- Regular Testing of Recovery Procedures: Periodically test the recovery procedures to ensure they are effective in restoring data.	- Pravidelné testování postupů obnovení: Pravidelné testování postupů obnovení, aby bylo zajištěno, že jsou účinné při obnovení dat.
- Fault Tolerant Hardware: Employ fault-tolerant hardware to minimize downtime and maintain data availability during a physical or technical incident.	- Hardware odolný vůči chybám: Používání hardwaru odolného proti chybám pro minimalizaci prostojů a zachování dostupnosti údajů během fyzického nebo technického incidentu.
- Data Recovery Tools: Invest in data recovery tools and services that can assist in retrieving lost or corrupted data.	- Nástroje pro obnovení dat: Investice do nástrojů a služeb pro obnovení dat, které mohou pomoci při získání ztracených nebo poškozených dat.
- Penetration Testing: Regularly conduct penetration testing, at least every 3 to 5 years, to evaluate the resilience and effectiveness of security systems and the security of the network by simulating cyberattacks.	- Penetrační testy: Pravidelné provádění penetračních testů alespoň jednou za 3 až 5 let pro vyhodnocení odolnosti a efektivity bezpečnostních systémů a zabezpečení sítě pomocí simulace kybernetických útoků.
- User Activity Monitoring and Logs with LAN ScopeCAT: Use LAN ScopeCAT to monitor and record user activity. In addition, maintain logs of these user activities for reviewing and auditing purposes.	- Monitorování aktivity a přihlašování uživatele pomocí LAN ScopeCAT: Použití LAN ScopeCAT k monitorování a zaznamenávání aktivity uživatelů. Dále uchovávání záznamů o těchto uživatelských aktivitách pro účely kontroly a auditu.
- Power-on Password and Windows User Account Security:For laptop PCs, require a password when powering on to ensure unauthorized users cannot access the system. Additionally, for Windows PCs, require users to have unique usernames and passwords that are at least 8 characters long for identification and authorization purposes. Passwords must be changed every 90 days, and the last three passwords cannot be reused.	- Heslo pro zapnutí a zabezpečení uživatelského účtu systému Windows: U notebooků bude při zapnutí vyžadováno heslo, aby bylo zajištěno, že k systému nebudou mít přístup neoprávnění uživatelé. U počítačů se systémem Windows bude dále vyžadováno, aby uživatelé měli jedinečná uživatelská jména a hesla pro účely identifikace a oprávnění, která budou mít nejméně 8 znaků. Hesla musí být měněna každých 90 dní a poslední tři hesla nesmí být použita znovu.
- Virtual Private Networks (VPNs) Security and Usage: Utilize Virtual Private Networks (VPNs) to establish secure and encrypted communication channels over the internet for remote access such as working from home. Require users to have unique usernames and passwords that are at least 8 characters long for identification and authorization purposes when connecting via VPN. Passwords must be changed every 30 days, and the last password cannot be reused. We use Fortinet's FortiGate 100F for our New Jersey location and FortiGate 100E for our California data center, both with maintenance contracts for firmware and hardware replacement. To further ensure security, PCs must be registered in Fortinet's Endpoint Management System (EMS), and only registered PCs are allowed to connect to the VPN. Additionally, use Secure Sockets Layer (SSL) encryption to secure data during transmission over the VPN.	- Zabezpečení a použití virtuálních privátních sítí (VPN): Pro vzdálený přístup přes internet, jako je práce z domova, budou využívány virtuální privátní sítě (VPN) k vytvoření bezpečných a šifrovaných komunikačních kanálů. Bude vyžadováno, aby uživatelé měli při připojení přes VPN jedinečná uživatelská jména a hesla pro účely identifikace a oprávnění, která budou mít nejméně 8 znaků. Hesla musí být měněna každých 30 dní a poslední heslo nesmí být použito znovu. Pro naše sídlo v New Jersey používáme Fortinet FortiGate 100F a pro naše datové centrum v Kalifornii používáme FortiGate 100E, a to se smlouvami o údržbě pro firmware i výměnu hardwaru. Pro další zajištění bezpečnosti musí být osobní počítače zaregistrovány v systému správy koncových bodů (EMS) společnosti Fortinet a k VPN se mohou připojit pouze registrované počítače. K zabezpečení dat během přenosu přes VPN bude dále používáno šifrování SSL (Secure Sockets Layer).
- BitLocker Encryption at laptop PC: Encrypt whole internal hard drive on physical laptop by Windows BitLocker to ensure that it is unreadable without the appropriate Recovery keys.	- Šifrování BitLocker na notebooku: Šifrování celého interního pevného disku na notebooku pomocí nástroje Windows BitLocker, aby bylo zajištěno, že bude bez příslušných klíčů pro obnovení nečitelný.
- Restricted Access Zones: Limit access to areas where personal data is processed to authorized	- Zóny s omezeným přístupem: Omezení přístupu do prostor, kde jsou osobní údaje zpracovávány,

personnel only.	pouze na oprávněné pracovníky.
- Security Surveillance: Deploy security surveillance cameras at key locations to monitor and secure the premises.	- Bezpečnostní dohled: Rozmístění bezpečnostních kamer na klíčových místech pro monitorování a zabezpečení prostor.
- Machine Room Physical Security: Ensure physical security measures such as secure locks and restricted machine room access to protect data storage devices.	- Fyzické zabezpečení strojovny: Zajištění fyzických bezpečnostních opatření pro ochranu zařízení pro ukládání dat, jako jsou bezpečné zámky a omezený přístup do strojovny.
- Visitor Logging and Identification: Maintain a log of all visitors and ensure they wear identification badges while on the premises.	- Zaznamenávání a identifikace návštěvníků: Vedení záznamů o všech návštěvnících a zajištění, aby během pobytu v prostorách nosili identifikační štítky.
- Secure Disposal: Ensure the secure disposal of both physical and digital media containing personal data when they are no longer needed. Implement strict procedures where paper documents containing personal information are shredded before disposal. Additionally, make sure that electronic storage devices are securely erased to prevent unauthorized access to sensitive information.	- Bezpečná likvidace: Zajištění bezpečné likvidace fyzických i digitálních médií obsahujících osobní údaje, pokud již nejsou potřeba. Zavedení přísných postupů před likvidací papírových dokumentů tam, kde jsou papírové dokumenty skartovávány. Dále bude zajištěno bezpečné vymazání elektronických paměťových zařízení, aby bylo zabráněno neoprávněnému přístupu k citlivým informacím.
- Mobile Device Management: Implement policies for the use of company smart phone that access email. Personal mobile device is not allowed to access any data.	- Správa mobilních zařízení: Zavedení zásad pro používání firemního chytrého telefonu, který umožňuje přístup do e-mailu. Přístup k údajům pomocí osobního mobilního zařízení není povolen.
- Integrated Security Monitoring and Response: Employ specialized log management tools for collecting, storing, analyzing, and visualizing log data, enhancing security and compliance. Implement a Security Operation Center (SOC) to monitor logs from Firewalls at NJ and CA data centers. SOC analyzes the logs and detects any attacks from outside, with Akros IT taking necessary actions such as registering the source IP in block lists for future attacks. Additionally, for behavior monitoring, install CrowdStrike's Falcon agent on all PCs and servers. The SOC will monitor alerts and take necessary actions if any alerts are triggered, ensuring a comprehensive and proactive approach to security.	- Integrované sledování zabezpečení a odezvy: Používání specializovaných nástrojů pro správu protokolů pro shromažďování, uchovávání, analýzu a zobrazování dat protokolů, zvyšování zabezpečení a dodržování předpisů. Vytvoření bezpečnostního dohledového centra (SOC) pro monitorování protokolů z firewallů v datových centrech v New Jersey a Kalifornii. SOC analyzuje protokoly a detekuje jakékoli externí útoky; společnost Akros IT přijme nezbytná opatření, jako je registrace zdrojové IP adresy v seznamech blokovaných adres, pro budoucí útoky. Dále instalace platformy Falcon společnosti CrowdStrike na všechny počítače a servery pro monitorování chování. SOC bude monitorovat výstrahy a přijímat nezbytná opatření, pokud budou spuštěny nějaké výstrahy, což zajistí komplexní a proaktivní přístup k zabezpečení.
- "Implementing Security Patches: Regularly apply security patches to fix vulnerabilities in system configurations and software. Maintain the record.	- Implementace bezpečnostních oprav: Pravidelné používání bezpečnostních oprav k odstranění zranitelných míst v konfiguracích systému a softwaru. Vedení záznamů.
- Least Privilege Principle in Configuration: Configure systems so that users and processes have the minimum levels of access necessary to perform their tasks.	- Princip nejmenších privilegií v konfiguraci: Konfigurace systémů tak, aby uživatelé a procesy měli minimální úrovně přístupu nezbytné k plnění úkolů.
- Configuration Backups: Regularly back up system configurations to facilitate recovery in case of system failure or corruption.	- Zálohy konfigurace: Pravidelné zálohování konfigurace systému, což usnadní obnovení v případě selhání nebo poškození systému.
- Data Protection Governance and Compliance: Appoint a Data Protection Officer (DPO) responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. Additionally, conduct Data	- Správa ochrany údajů a dodržování předpisů: Jmenování pověřence pro ochranu osobních údajů (DPO) odpovědného za dohled nad strategií a implementací ochrany osobních údajů s cílem zajistit dodržování požadavků GDPR. Dále se bude

Protection Impact Assessments (DPIAs) to identify and minimize data protection risks in new projects or processes as necessary. Have in place a GDPR policy and enter into Data Protection Agreements (DPAs) as necessary to ensure that data handling practices are compliant with data protection laws and regulations.	podle potřeby provádět posouzení vlivu na ochranu osobních údajů (DPIA) s cílem zjistit a minimalizovat rizika spojená s ochranou osobních údajů v nových projektech nebo postupech. Podle potřeby budou zavedeny zásady GDPR a uzavřeny smlouvy o ochraně osobních údajů (DPA), aby bylo zajištěno, že postupy nakládání s údaji budou v souladu se zákony a předpisy o ochraně osobních údajů.
- Establishing Data Breach Response Protocols: Create and implement procedures for identifying, reporting, and managing data breaches.	- Zavedení protokolů odezvy na porušení zabezpečení osobních údajů: Vytvoření a implementace postupů pro identifikaci, hlášení a řízení narušení zabezpečení údajů.
- Data Retention Policy: Establish and enforce a data retention policy specifying the duration for which personal data can be stored and the conditions for its deletion.	- Zásady uchovávání údajů: Zavedení a prosazování zásad uchovávání údajů, které stanoví dobu, po kterou mohou být osobní údaje uchovávány, a podmínky jejich vymazání.
<u>For personal data of patients and patients' babies (in addition to the above measures)</u>	<u>Pro osobní údaje pacientů a dětí pacientů (kromě výše uvedených opatření)</u>
- Identifiable information such as names, addresses, social security numbers, or any other directly identifying details are not collected in our clinical database. Instead, each subject is assigned with an unique identifiers (subject ID). These identifiers allow us to analyze the data while maintaining a level of anonymity for the subject.	- V naší klinické databázi nejsou shromažďovány informace, z nichž by bylo možné zjistit totožnost, jako jsou jména, adresy, čísla sociálního pojištění, ani žádné jiné údaje, z nichž by bylo možné zjistit totožnost přímo. Místo toho je každému subjektu přidělen jedinečný identifikační údaj (ID subjektu). Tyto identifikační údaje nám umožňují analyzovat data při zachování úrovně anonymity subjektu.
- Data Minimisation: Akros Clinical Team ensures that only the minimum necessary information required for study result analysis and interpretation is collected and stored in the clinical database. This approach reduces the amount of sensitive data being processed, minimizing the risk of data breaches and enhancing data protection.	- Minimalizace dat: Klinický tým společnosti Akros zajišťuje, že v klinické databázi budou shromažďovány a ukládány pouze minimální informace nezbytné pro analýzu a interpretaci výsledků studie. Tento přístup snižuje množství zpracovávaných citlivých údajů, minimalizuje riziko narušení zabezpečení údajů a zvyšuje ochranu údajů.
- The primary processing of personal data of patients and patient' babies is carried out in Rave EDC (Electronic Data Capture) system provided by Medidata Solutions Inc. ○ Confidentiality: Medidata ensures confidentiality by implementing robust measures such as role-based access controls and user authentication mechanisms. These measures effectively restrict access to the clinical database (Medidata Rave), ensuring that only authorized individuals can gain entry. ○ Integrity: To maintain data integrity, Medidata implements validation checks that verify the accuracy and consistency of the data collected within the clinical database. Medidata maintains detailed logs of system activities, including data modifications. This logging enables the tracking and monitoring of any unauthorized changes or tampering, ensuring data integrity. Medidata manages and tracks different versions of	- Primární zpracování osobních údajů pacientů a dětí pacientů se provádí v systému Rave EDC (elektronický systém pro zaznamenávání údajů) poskytovaném společností Medidata Solutions Inc. ○ Důvěrnost informací: Společnost Medidata zajišťuje důvěrnost informací zavedením robustních opatření, jako jsou kontroly přístupu založené na rolích a mechanismy ověřování uživatelů. Tato opatření účinně omezují přístup do klinické databáze (Medidata Rave) a zajišťují, že do databáze mohou vstoupit pouze oprávněné osoby. ○ Integrita: V zájmu zachování integrity zavádí společnost Medidata validační kontroly pro zachování integrity dat, které ověřují přesnost a konzistentnost údajů shromážděných v klinické databázi. Společnost Medidata vede podrobné záznamy o činnostech systému, včetně modifikací údajů. Vedení těchto záznamů umožňuje sledování a monitorování neoprávněných změn nebo manipulace, což zajišťuje integritu údajů. Společnost

data and system configurations. This approach helps maintain data integrity over time by ensuring that changes are properly documented and controlled.	Medidata spravuje a sleduje různé verze údajů a konfigurací systému. Tento přístup pomáhá udržovat integritu údajů v průběhu času tím, že zajišťuje řádné zdokumentování a kontrolování změn.
○ Availability: Medidata ensures system availability by deploying redundant hardware, network infrastructure, and data centers. These redundancies safeguard against hardware or software failures, minimizing disruptions in service. Additionally, Medidata implements backup and recovery procedures, enabling the timely restoration of data and services in the event of a major disruption or disaster.	○ Dostupnost: Společnost Medidata zajišťuje dostupnost systému nasazením duplicitního hardwaru, síťové infrastruktury a datových center. Tato duplicitní zařízení jsou pojistkou proti selhání hardwaru nebo softwaru a minimalizují přerušení provozu. Společnost Medidata dále implementuje postupy zálohování a obnovy, které umožňují včasné obnovení údajů a služeb v případě závažného narušení provozu nebo havárie.
○ Resilience: To enhance resilience, Medidata performs routine backups of data and system configurations. These backups facilitate recovery and minimize the risk of data loss in case of unforeseen incidents. Furthermore, Medidata utilizes real-time monitoring tools and alerts to proactively identify potential issues or abnormalities in the system.	○ Odolnost: Pro zvýšení odolnosti provádí společnost Medidata pravidelné zálohování údajů a konfigurací systému. Tyto zálohy usnadňují obnovení a minimalizují riziko ztráty údajů v případě nepředvídaných incidentů. Společnost Medidata dále využívá monitorovací nástroje a výstrahy v reálném čase pro proaktivní identifikaci potenciálních problémů nebo abnormalit v systému.
○ Backup and recovery: Medidata implements robust backup mechanisms to create regular copies of the data stored in their systems. Medidata performs traditional backup as well as site-to-site electronic replication of data to protect client data in the event of a disaster. There is a dedicated disaster recovery site distant from the production data centers.	○ Zálohování a obnovení: Společnost Medidata zavádí robustní mechanismy zálohování pro vytváření pravidelných kopií údajů, které má uloženy ve svých systémech. Společnost Medidata provádí tradiční zálohování i elektronickou replikaci údajů z jednoho pracoviště na druhé s cílem chránit údaje klientů v případě havárie. Společnost má vyhrazené pracoviště pro obnovení po havárii, které je vzdálené od produkčních datových center.
○ Disaster recovery planning: Medidata has comprehensive disaster recovery plans in place, which outline the steps and procedures to be followed in the event of a major incident. The plan covers: alert lists, team responsibilities, recovery and notification procedures, resumption plans, installation tasks, work area checklists and preparedness procedures. Medidata's support, product and account management teams would notify all customers of unscheduled downtime via email initially, via phone if the situation escalates.	○ Plánování obnovení po havárii: Společnost Medidata má zavedeny komplexní plány na obnovení po havárii, jež stanovují kroky a postupy, které je nutné dodržovat v případě závažného incidentu. Tento plán zahrnuje: seznamy výstrah, povinnosti týmu, postupy obnovení a oznamování, plány obnovení činnosti, instalační úkoly, kontrolní seznamy pro pracovní oblast a postupy připravenosti. Týmy podpory a správy produktů a účtů společnosti Medidata by nejdříve upozornily všechny zákazníky na neplánovaný výpadek e-mailem, a pokud by situace eskalovala, upozornily by je telefonicky.
○ Redundancy: Medidata deploys redundant infrastructure and data centers, distributing data and services across multiple data centers. This helps ensure uninterrupted availability and access to personal data.	○ Duplicita: Společnost Medidata využívá duplicitní infrastrukturu a datová centra a distribuuje údaje a služby přes více datových center. Pomáhá to zajistit nepřetržitou dostupnost a přístup k osobním údajům.

- Testing and validation: Medidata performs regular testing and validation of their backup and recovery processes to ensure their effectiveness.
- Medidata's processes include the following:
  - Conduct regular security audits and assessments to evaluate the effectiveness of technical and organizational measures.
  - Perform periodic penetration tests to simulate real-world attacks and identify potential weaknesses in the systems. This helps assess the resilience of the infrastructure and application security controls.
  - Implement systematic approach to identify and address vulnerabilities in a timely manner. This includes infrastructure vulnerability scans, peer code reviews, static source code analysis and dynamic scanning of URLs.
  - Establish a well-defined incident response program to handle security incidents effectively. This plan should outline the steps to be taken, roles and responsibilities of the incident response team, communication protocols, and strategies for containment, investigation, and recovery.
  - Implement real-time and continuous monitoring systems to detect and respond to security events promptly.
  - Adhere to relevant regulatory requirements and industry standards for data security and privacy. This includes regularly reviewing and updating security measures to align with changing regulations and standards.
- User Access Control: Medidata Rave enforces the use of unique usernames and strong passwords for user identification and authorization. To enhance security, passwords are rotated every 90 days. Additionally, Multi-Factor Authentication (MFA) is adopted, providing an extra layer

- Testování a validace: Společnost Medidata provádí pravidelné testování a validaci svých procesů zálohování a obnovení, aby byla zajištěna jejich účinnost.
- Procesy společnosti Medidata zahrnují:
  - provádění pravidelných auditů a hodnocení zabezpečení pro vyhodnocení účinnosti technických a organizačních opatření.
  - provádění pravidelných penetračních testů pro simulaci útoků v reálném světě a identifikaci potenciálních slabých míst v systémech. To pomáhá vyhodnotit odolnost infrastruktury a kontroly zabezpečení aplikací.
  - zavedení systematického přístupu k včasnému zjištění a řešení zranitelných míst. Tento postup zahrnuje skenování zranitelnosti infrastruktury, vzájemné hodnocení kódu, statickou analýzu zdrojových kódů a dynamické skenování adres URL.
  - vytvoření dobře definovaného programu odezvy na incidenty pro efektivní řešení bezpečnostních incidentů. Tento plán by měl stanovit kroky, které je nutné učinit, role a odpovědnosti týmu pro odezvy na incidenty, komunikační protokoly a strategie pro zamezení šíření, prošetření a obnovení.
  - zavedení systémů soustavného monitorování v reálném čase pro rychlé detekování bezpečnostních události a reakce na tyto události.
  - dodržování příslušných regulačních požadavků a oborových standardů pro zabezpečení údajů a soukromí. Zahrnuje to pravidelnou kontrolu a aktualizaci bezpečnostních opatření, aby byly v souladu s měnícími se předpisy a standardy.
- Kontrola uživatelského přístupu: Medidata Rave prosazuje používání jedinečných uživatelských jmen a silných hesel pro identifikaci a autorizaci uživatelů. Pro zvýšení zabezpečení se hesla mění každých 90 dní. Dále je zavedeno vícefaktorové ověřování (MFA),

of security to user authentication. Moreover, the system automatically logs users out after a period of inactivity, protecting against unauthorized access.	které poskytuje další vrstvu zabezpečení ověřování uživatele. Systém kromě toho uživatele po určité době nečinnosti automaticky odhlásí, čímž zajišťuje ochranu před neoprávněným přístupem.
○ Transmission Security: All data transmission in Medidata, whether internal or external, is encrypted using Transport Layer Security (TLS). Encryption ensures that the data is protected from unauthorized interception or tampering.	○ Zabezpečení předávání údajů: Veškeré externí i interní předávání údajů ve společnosti Medidata je šifrováno pomocí protokolu TLS (Transport Layer Security). Šifrování zajišťuje ochranu údajů před neoprávněným zachycením nebo manipulací.
○ Data Encryption: Encryption is enabled at the storage unit level and is affected through hardware. For the Rave EDC data stores, the Storage Area Network uses 256-bit Advanced Encryption Standard (AES) keys, using a proprietary key management system.	○ Šifrování údajů: Šifrování je povoleno na úrovni úložiště a je ovlivňováno hardwarem. Síť SAN (Storage Area Network) používá pro úložiště údajů Rave EDC 256bitové šifrovací klíče AES (Advanced Encryption Standard), a to pomocí patentově chráněného systému správy šifrovacích klíčů.
○ Regular data backup: Medidata also follows regular data backup processes to create copies of the stored data. This helps to safeguard against data loss and ensures data availability in case of unexpected incidents. To further enhance data availability and resilience, Medidata implements redundant storage systems to ensure data availability and minimize the risk of data loss.	○ Pravidelné zálohování údajů: Společnost Medidata také provádí pravidelné zálohování údajů, a vytváří tak kopie uložených údajů. Zálohování napomáhá při ochraně před ztrátou údajů a zajišťuje jejich dostupnost v případě neočekávaných incidentů. Pro další zlepšení dostupnosti a odolnosti údajů společnost Medidata zavádí duplicitní úložné systémy, které zajišťují dostupnost údajů a minimalizují riziko jejich ztráty.
○ All Medidata data and systems are housed in TIA Level 3+ data centers in order to provide state-of-the-art protections at the front door. All data centers are unmarked with unpublished addresses, cameras with digital recorders, 24x7 uniformed guards, biometrics, mandatory photo-id smart cards, environmental sensors and more. Medidata's corporate sites are similar, with tight access control uniformly throughout the entire environment.	○ Všechny údaje a systémy společnosti Medidata jsou umístěny v datových centrech úrovně hodnocení 3+ dle TIA, která poskytují nejmodernější vstupní ochranu. Všechna datová centra jsou neoznačená a mají nepublikované adresy, jsou vybavena kamerami s digitálním záznamem, nepřetržitě chráněna uniformovanou ostrahou, využívají biometrické údaje a povinné čipové karty s identifikační fotografií, čidla v prostředí atd. Pracoviště společnosti Medidata jsou podobná, a to s přísnou jednotnou kontrolou přístupu na celém pracovišti.
○ Within Data Center Suite, access is restricted to authorized personnel by means of a card reader on the Cage door, using the internal access card.	○ V datovém centru je přístup omezen na oprávněný personál používající interní přístupovou kartou, která je kontrolována pomocí čtečky karet na dveřích.
○ Medidata implements a centralized logging system to collect and store logs from various sources in one place, enabling better monitoring and analysis. Additionally, they utilize specialized log management tools for collect and analyze operating systems and application logs for security events.	○ Společnost Medidata zavádí centralizovaný systém protokolování pro shromažďování a uchovávání protokolů z různých zdrojů na jednom místě, což umožňuje lepší sledování a analýzu. Společnost dále využívá specializované nástroje pro správu protokolů pro shromažďování a analýzu operačních systémů a záznamů z aplikací pro účely bezpečnostních událostí.
○ Medidata uses centralized configuration	○ Společnost Medidata používá nástroje pro

management tools to maintain consistent system configurations across systems. In addition, Medidata follows a regular patch management process to apply security patches and updates to their systems and software. Medidata maintains proper documentation for all new releases, including a log of changes. This documentation helps track and communicate the modifications made during each release, providing transparency and accountability for any configuration changes.	centralizovanou správu konfigurací k zachování konzistentních konfigurací systému ve všech systémech. Společnost Medidata dále dodržuje postup pravidelných bezpečnostních oprav, kterým provádí bezpečnostní opravy a aktualizace svých systémů a softwaru. Společnost Medidata vede řádnou dokumentaci pro všechny nové verze, včetně protokolu změn. Tato dokumentace pomáhá sledovat a sdělovat změny provedené v každé verzi, čímž zajišťuje transparentnost a odpovědnost za jakékoli změny konfigurace.
○ Data Audit Trails: Medidata Rave maintains comprehensive audit trails that track and document any changes or modifications made to the data. This practice ensures transparency, traceability, and accountability in data management processes, allowing for thorough monitoring and auditing of data activities.	○ Datové auditní stopy: Medidata Rave zachovává komplexní auditní stopy, které sledují a dokládají veškeré změny nebo úpravy provedené v údajích. Tato praxe zajišťuje transparentnost, sledovatelnost a odpovědnost v procesech správy údajů, což umožňuje důkladné sledování a audit aktivit v údajích.
○ Data Validation: In Medidata Rave, Akros implements programed edit checks to validate the accuracy and completeness of entered data. This includes range checks, format validations, and logical consistency checks. These validation measures ensure the integrity and reliability of the collected data.	○ Validace údajů: Akros provádí v Medidata Rave naprogramované kontroly úprav pro ověření přesnosti a úplnosti zadaných údajů. Zahrnuje to kontroly rozsahu, validaci formátu a logické kontroly konzistentnosti. Tato validační opatření zajišťují integritu a spolehlivost shromážděných údajů.
- RBAC: RBAC is implemented in Medidata Rave. Specific users are granted role-based access to the clinical database for a particular study within the Electronic Data Capture system, as required. User accounts are set up in the EDC system through Medidata, which allows users to authenticate with a single set of credentials and gain access to multiple related systems. The roles and user list for the study are maintained by the Akros clinical data management team.	- RBAC: V Medidata Rave je zavedeno RBAC. Určitým uživatelům je v rámci systému EDC podle potřeby udělen přístup do klinické databáze pro konkrétní studii. Uživatelské účty jsou v systému EDC nastaveny prostřednictvím společnosti Medidata, což uživatelům umožňuje provést ověření pomocí jedné sady přihlašovacích údajů a získat přístup do několika souvisejících systémů. Seznam rolí a uživatelů pro studii spravuje tým společnosti Akros pro správu klinických údajů.
- Once the study is concluded and the database lock has been confirmed, Akros clinical data management team revoke EDC access for all non-Akros users, ensuring that only authorized individuals retain access to the system.	- Po dokončení studie a potvrzení uzamčení databáze zruší tým společnosti Akros pro správu klinických údajů přístup do EDC všem uživatelům, kteří nejsou ze společnosti Akros, a zajistí tak, že do systému budou mít přístup pouze oprávněné osoby.
- SOP Review, Training, and User Education: Akros regularly reviews and updates its Standard Operating Procedures (SOPs) to align with best practices and regulatory requirements. Comprehensive training is provided to all employees, including data entry personnel, focusing on data collection standards, protocols, SOPs, and role-specific data quality standards. Periodic training sessions ensure employees' understanding of and adherence to data quality and security protocols, promoting consistent, accurate, and compliant processes while fostering accountability throughout the organization.	- Přezkoumání SOP, školení a edukace uživatelů: Společnost Akros pravidelně přezkoumává a aktualizuje své standardní provozní postupy (SOP), aby byly v souladu s nejlepší praxí a požadavky právních předpisů. Všem zaměstnancům, včetně pracovníků zadávajících údaje, je poskytováno komplexní zaškolení zaměřené na standardy shromažďování údajů, protokoly, SOP a standardy kvality údajů pro konkrétní role. Pravidelná školení zajišťují, že zaměstnanci porozumí protokolům pro zajištění kvality údajů a jejich zabezpečení a budou je dodržovat, a podporují konzistentní a přesné procesy splňující příslušné požadavky a odpovědnost v celé organizaci.

- Database Standards: Akros adheres to industry-recognized CDISC standards when building the clinical database. This approach ensures consistency and high-quality data collection while minimizing errors.
- User Acceptance Testing: Prior to system release, Akros data management team perform thorough user acceptance testing to ensure that the system functions as expected. This testing phase verifies the system's performance, functionality, and usability to guarantee its effectiveness and reliability.
- Data Reconciliation: Akros' data management team conducts data reconciliations to ensure consistency and accuracy between different data sources or systems. This process involves comparing and aligning data from various sources to eliminate discrepancies and maintain data integrity.
- Data Review and Query Resolution: Study clinical research associates (CRAs) periodically review and compare data entered in the clinical database with source data to ensure accuracy. Akros' data management team conducts regular data reviews, identifying discrepancies or missing information and raising queries to researchers or data providers for resolution. These measures contribute to maintaining data integrity, completeness, and accuracy. The clinical team also performs data reviews to identify data errors, inconsistencies, and outliers.

- Standardy pro databáze: Společnost Akros dodržuje při budování klinické databáze oborově uznávané standardy CDISC. Tento přístup zajišťuje konzistentnost, vysoce kvalitní shromažďování údajů a minimalizaci chyb.
- Testování přijetí uživateli: Před uvolněním systému provádí tým společnosti Akros pro správu údajů důkladné testování přijetí uživateli s cílem zjistit, zda systém funguje podle očekávání. Tato fáze testování ověřuje výkonnost, funkčnost a použitelnost systému, aby byla zaručena jeho účinnost a spolehlivost.
- Rekonciliace údajů: Tým společnosti Akros pro správu údajů provádí rekonciliace údajů, aby byly zajištěny konzistentnost a přesnost mezi různými zdroji údajů nebo systémy. Tento proces zahrnuje srovnávání a sladění údajů z různých zdrojů, aby byly odstraněny nesrovnalosti a byla zachována integrita údajů.
- Přezkoumání údajů a řešení dotazů: Pracovníci klinického výzkumu (CRA), kteří se podílejí na studii, pravidelně kontrolují a porovnávají údaje zadané do klinické databáze se zdrojovými údaji, aby byla zajištěna přesnost. Tým společnosti Akros pro správu údajů provádí pravidelné kontroly údajů, identifikuje nesrovnalosti nebo chybějící informace a vznáší dotazy či připomínky vůči výzkumným pracovníkům nebo poskytovatelům údajů k vyřešení. Tato opatření přispívají k zachování integrity, úplnosti a přesnosti údajů. Klinický tým také provádí přezkoumání údajů pro zjištění chyb v údajích, nesrovnalostí a odlehlých hodnot.

FINAL PROVISION

Counterparts. These SCC may be executed in two or more counterparts, each of which shall be deemed an original, but both of which together shall constitute one and the same instrument. Each of the contracting parties will receive one signed copy of these SCCs.

IN WITNESS WHEREOF, the parties hereto, each by a duly authorized representative, have executed these SCC as of the SCC Effective Date.

THE SIGNATURES APPEAR ON THE FOLLOWING PAGE

ZÁVĚREČNÉ USTANOVENÍ

Stejnopisy. Tyto SCC mohou být vyhotoveny ve dvou a více stejnopisech, z nichž je každý považován za originál a všechny společně představují jednu a tutéž listinu. Každá ze smluvních stran obdrží jeden podepsaný stejnopis těchto SCC.

NA DŮKAZ ČEHOŽ podepsaly smluvní strany prostřednictvím svých řádně oprávněných zástupců tyto SCC ke dni účinnosti SCC.

PODPISY JSOU UVEDENY NA NÁSLEDUJÍCÍ STRANĚ

ICON Clinical Research Limited, on behalf of Akros Pharma Inc. /ICON Clinical Research Limited, jménem Akros Pharma Inc.

[redacted]

INSTITUTION / ZDRAVOTNICKÉ ZAŘÍZENÍ

[redacted]

READ AND ACKNOWLEDGED / ČETL JSEM A POROZUMĚL

[redacted]