AZIENDA OSPEDALIERA UNIVERSITARIA

Deliberazione n. 1030 del 20/07/2023

Addendum I alla convenzione stipulata tra l'Azienda Ospedaliera Universitaria Policlinico e per essa l'UOC di Ematologia e la società OPIS S.r.l. per la conduzione della sperimentazione clinica dal titolo "Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresid (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKI" STUDIO MANIFEST 2 Prot. CPI 0610-04– Codice Eudract: 2020-001989-10 - PI: Prof. Marco Santoro.

DIREZIONE GENERALE **Il Responsabile dell'Ufficio atti deliberativi** **Grazia Scalici**	**Area Gestione Economico - Finanziaria** Autorizzazione spesa n. Del Conto di costo _____ NULLA OSTA in quanto conforme alle norme di contabilità **Il Responsabile dell'Area Gestione Economico – Finanziaria**

Ai sensi del DPR n. 445/2000 e ss.mm.ii. e la Legge 241/90 e ss.mm.ii. e L.R. 7/2019, il sottoscritto attesta la regolarità della procedura seguita e la legalità del presente atto, nonché l'esistenza della documentazione citata e la sua rispondenza ai contenuti esposti.

Il Responsabile proponente

Il Commissario Straordinario
Dott. Maurizio Montalbano
nominato con D. A. n. 19/2023 del
09 maggio 2023 prorogato con D.A. n. 28 del 29/06/2023
Con l'intervento, per il parere prescritto dall'art. 3 del D.L.vo n. 502/92
così come modificato dal D.L.vo n. 517/93 e dal D.L.vo n. 229/99
del Direttore Amministrativo Dott. Arturo Caranna
e del Direttore Sanitario Dott. Gaetano Cimò
Svolge le funzioni di segretario verbalizzante
Sig.ra Grazia Scalici

AZIENDA OSPEDALIERA UNIVERSITARIA

Delibera n. 1030 del 20/07/2023

IL COMMISSARIO STRAORDINARIO

VISTO il Decreto dell'08.02.2013, del Ministero della Salute recante misure relative ai criteri per la composizione ed il funzionamento dei Comitati Etici;

VISTO il Decreto dell'Assessorato delle Salute, della Regione Siciliana, n. 1360/2013, con il quale, in ottemperanza alle disposizioni indicate al comma 10, articolo 12, del D.L. 13/09/2012, n. 158, convertito, con modificazioni, dalla L. 8 novembre 2012. N. 189, si è provveduto al riordino dei Comitati Etici della Regione;

VISTA la delibera n. 459 del 03/05/2021 di rinnovo del Comitato Etico Palermo 1.

PREMESSO che con delibera n. 676 del 01/06/2022 è stata sottoscritta la convenzione per lo svolgimento dello Sperimentazione clinica dal titolo ""Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresid (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKI"STUDIO MANIFEST 2 Prot. CPI 0610-04– Codice Eudract: 2020-001989-10 - PI: Prof. Marco Santoro.

PRESO ATTO che con nota del 06/06/2023 la società OPIS s.r.l. per conto di Constellation Pharmaceuticals, Inc., comunicava che in merito alla sperimentazione clinica Prot. CPI0610-04 si è reso necessario integrare nel contratto le clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679, al fine di garantire l'osservanza delle leggi applicabili in materia di protezione dati ;

VISTO L'Addendum I alla Sperimentazione clinica Prot. CPI0610-04 che modifica il contratto originario integrandolo con le clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679.

Per i motivi in premessa citati che qui si intendono ripetuti e trascritti

AZIENDA OSPEDALIERA UNIVERSITARIA

DELIBERA

Di procedere alla sottoscrizione dell'Addendum I alla Convenzione tra l'Azienda Ospedaliera Universitaria Policlinico e per essa l'UOC di Ematologia e la società OPIS S.r.l. per la conduzione della sperimentazione clinica dal titolo "Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresid (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKI" STUDIO MANIFEST 2 Prot. CPI 0610-04- Codice Eudract: 2020-001989-10 - PI: Prof. Marco Santoro.

L 'Addendum I è allegato alla presente per farne parte integrante.

Il Direttore Sanitario
Dott. Gaetano Cimò

Il Direttore Amministrativo
Dott. Arturo Caranna

Il Commissario Straordinario
Dott. Maurizio Montalbano

Il Segretario Verbalizzante
Grazia Scalici

AZIENDA OSPEDALIERA UNIVERSITARIA

PUBBLICAZIONE

Si certifica che la presente deliberazione, per gli effetti dell'art. 53 comma 2 L.R. n. 30 del 03/11/1993, in copia conforme all'originale, è stata pubblicata in formato digitale all'albo informatico dell'Azienda Ospedaliera Universitaria Policlinico a decorrere dal giorno 23/07/2023 e che nei 15 giorni successivi:

- ☐ non sono pervenute opposizioni
- ☐ sono pervenute opposizioni da _____

Il Funzionario Responsabile

Notificata al Collegio Sindacale il _____

DELIBERA NON SOGGETTA AL CONTROLLO

☐ Delibera non soggetta al controllo , ai sensi dell'art. 4, comma 8 della L. n. 412/1991 e divenuta :

ESECUTIVA

☐ Decorso il termine (10 giorni dalla data di pubblicazione ai sensi dell'art. 53, comma 6, L.R. n. 30/93

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4 comma 8, della L. n. 412/1991 e divenuta:

IMMEDIATAMENTE ESECUTIVA

Ai sensi dell'art. 53, comma 7, L.R. 30/93

Il Funzionario Responsabile

ESTREMI RISCONTRO TUTORIO

☐ Delibera trasmessa, ai sensi della L.R. n. 5/09, all'Assessorato Regionale Salute in data _____ prot. n. _____

SI ATTESTA

Che l'Assessorato Regionale Salute, esaminata la presente deliberazione:

☐ Ha pronunciato l'approvazione con atto prot. n. _____ del _____ come da allegato

☐ Ha pronunciato l'annullamento con atto prot. n. _____ del _____ come da allegato

☐ Delibera divenuta esecutiva con decorrenza del termine previsto dall'art. 16 della L. R. n. 5/09 dal _____

Il Funzionario Responsabile

ADDENDUM N. I AL CONTRATTO PER LA CONDUZIONE DELLA SPERIMENTAZIONE CLINICA

"Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresib (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKi"

STUDIO MANIFEST-2

Il presente Emendamento (di seguito "**Emendamento**") alla Convenzione per sperimentazione clinica, Protocollo "Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresib (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKi" - STUDIO MANIFEST-2 - (di seguito la "**Convenzione**") entra in vigore a decorrere dall'ultima sottoscrizione (di seguito la "**Data di efficacia**") ed è stipulato

TRA

AZIENDA OSPEDALIERA UNIVERSITARIA POLICLINICO "PAOLO GIACCONE" DI PALERMO (d'ora innanzi denominato/a "**Ente**"), con sede legale in PALERMO Via del Vespro 129 C.F. e P. IVA n. 05841790826, in persona del Legale Rappresentante, in qualità di Commissario Straordinario Dr. Maurizio Montalbano, munito di idonei poteri di firma del presente atto)

E

ADDENDUM N. I TO THE CLINICAL INVESTIGATION AGREEMENT

"A Phase 3, Randomized, Double-blind, Active-Control Study of Pelabresib (CPI-0610) and Ruxolitinib vs. Placebo and Ruxolitinib in JAKi Treatment Naive MF Patients"

The MANIFEST-2 study

This Amendment **("Amendment")** to the Clinical Trial Agreement, Protocol "A Phase 3, Randomized, Double-blind, Active-Control Study of Pelabresib (CPI-0610) and Ruxolitinib vs. Placebo and Ruxolitinib in JAKi Treatment Naive MF Patients" - **(the "Agreement")** is effective as of the last signature (the "**Effective Date**"), and is entered by

BETWEEN

AZIENDA OSPEDALIERA UNIVERSITARIA POLICLINICO "PAOLO GIACCONE" in PALERMO (hereinafter the "**Entity**"), headquartered in Palermo, Via del Vespro, 129, tax code and VAT no. 05841790826, through its Legal Representative, in the capacity of Extraordinary Commissioner Dr. Maurizio Montalbano, who has been granted with the powers to enter into this Agreement

AND

OPIS S.r.l., con sede legale in G. Matteotti 10 (Palazzo Aliprandi), 20832 Desio (MB), Italia, C.F. e P. IVA n. 12605350151, in persona del Legale Rappresentante Dr.ssa Laura Ambrosoli, in qualità di CEO, (d'ora innanzi denominata la "**CRO**") per conto dello Sponsor Constellation Pharmaceuticals, Inc, con sede legale in 470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA, Tax code: 26-1741721 (d'ora innanzi denominato/a "**Sponsor**")	OPIS S.r.l., with registered office at Via G. Matteotti 10 (Palazzo Aliprandi), 20832 Desio (MB), Italy, Fiscal Code and VAT no. 12605350151, in the person of its Legal Representative Dr.ssa Laura Ambrosoli (hereinafter the "**CRO**"), in his quality as CEO, on behalf of the Sponsor Constellation Pharmaceuticals, Inc, headquartered in 470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA, Tax code: 26-1741721 (hereinafter the **"Sponsor"**)
Lo Sponsor e l'Ente sono di seguito denominati singolarmente "**Parte**" e congiuntamente "**Parti**".	Sponsor and Entity are hereinafter each referred to as a "**Party**" and collectively as the "**Parties**".
PREMESSO CHE:	**WHEREAS:**
• le Parti hanno stipulato la Convenzione per la sperimentazione clinica intitolata "Studio di fase 3, randomizzato, in doppio cieco, con controllo attivo di Pelabresib (CPI-0610) e Ruxolitinib rispetto a placebo e Ruxolitinib nei pazienti con MF naïve al trattamento con JAKi" - STUDIO MANIFEST-2 (di seguito la "**Sperimentazione**");	• the Parties have entered into the Agreement, for the performance of the trial entitled "A Phase 3, Randomized, Double-blind, Active-Control Study of Pelabresib (CPI-0610) and Ruxolitinib vs. Placebo and Ruxolitinib in JAKi Treatment Naive MF Patients" - The MANIFEST-2 study (the "**Trial**";
• mediante accordo separato, lo Sponsor ha OPIS s.r.l., una società con sede operativa principale in [indirizzo della CRO], che opera come organizzazione di ricerca a contratto indipendente insieme alle sue affiliate (di seguito "**CRO**"), (i) di organizzare e monitorare la Sperimentazione per conto dello Sponsor e di rappresentarlo in tutte le attività necessarie alla buona esecuzione della Sperimentazione, come di seguito descritto, e (ii) di sottoscrivere la Convenzione e il presente Emendamento per conto dello Sponsor;	• by separate agreement, Sponsor has engaged OPIS s.r.l, a company with a principal place of business at [CRO address], acting as an independent contract research organization together with its ("**CRO**") (i) to organize and monitor the Trial on behalf of Sponsor and to represent Sponsor for all the activities necessary for the successful performance of the Trial, as described hereunder, and (ii) to sign the Agreement and this Amendment on behalf of Sponsor;

• le Parti ora desiderano modificare alcune condizioni della Convenzione.	• the Parties now wish to amend some terms of the Agreement.
SI CONVIENE E SI STIPULA QUANTO SEGUE:	**NOW, THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:**
Tutti i termini con l'iniziale maiuscola utilizzati nel presente Emendamento avranno il significato attribuitogli nella Convenzione, salvo quanto diversamente ed espressamente indicato nel presente atto.	All capitalized terms used in this Amendment shall have the meaning ascribed to them in the Agreement, except as otherwise expressly stated herein.
1. Trasferimenti internazionali di dati.	**1. International Data Transfers**
Al fine di garantire l'osservanza delle leggi applicabili in materia di protezione dei dati per quanto riguarda il trasferimento dei dati personali dall'Ente allo Sponsor, le Parti convengono che tale trasferimento di dati sarà disciplinato dal	To ensure compliance with applicable data protection laws regarding the transfer of personal data from Entity to Sponsor, the Parties agree that such transfer of data shall be governed by the
"MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento"	"MODULE ONE: Transfer Controller to Controller"
delle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio conformemente alla decisione di esecuzione (UE) 2021/914 della Commissione europea del 4 giugno 2021 (di seguito "**CCT**"), allegate al presente Emendamento come nuovo **Allegato A**.	of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council according to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**SCC**"), attached to this Amendment as **Attachment A**.
Le CCT saranno considerate	The SCC shall be considered duly executed between the Parties upon entering into force of this Amendment, and the Parties agree to observe the terms of the SCC without modification. To the extent not signed separately,

debitamente stipulate tra le Parti al momento dell'entrata in vigore del presente Emendamento e le Parti acconsentono a osservarne le condizioni senza modifiche. Laddove non apposte separatamente, le firme delle Parti sul presente Emendamento saranno ritenute una sottoscrizione appropriata delle CCT. Ai sensi delle CCT, l'Ente sarà considerato "esportatore" e lo Sponsor sarà considerato "importatore".	the Parties' signatures to this Amendment shall be considered an appropriate signature to the SCC. Entity shall be deemed "data exporter" and Sponsor shall be deemed "data importer" under the SCC.
2. Esecuzione ai sensi delle altre condizioni della Convenzione. Salvo quanto espressamente modificato dal presente atto, la Convenzione rimarrà pienamente valida ed efficace. Il presente Emendamento è inserito nella Convenzione tra le Parti e costituisce parte integrante della medesima. In caso di conflitti o incongruenze tra la Convenzione e il presente Emendamento, prevarrà quest'ultimo.	**2. Performance under all other terms of the Agreement.** Except as expressly amended hereby, the Agreement shall continue in full force and effect. This Amendment is incorporated and made a part of the Agreement between the Parties. In the event of any conflict or inconsistency between the Agreement and this Amendment, the latter shall prevail.
3. Copie. L'Emendamento può essere sottoscritto in più copie mediante firma elettronica, che avrà il medesimo valore di una firma autografa su una copia cartacea; ciascuna di tali copie sarà considerata un originale e tutte le copie o i documenti firmati elettronicamente costituiranno congiuntamente un unico e medesimo Emendamento. L'imposta di bollo sull'originale informatico di cui all'art. 2 della	**3. Counterparts.** The Amendment may be executed in counterparts and via electronic signature, which shall have the same effect as a wet signature in a physical counterpart, each of which shall be deemed to be an original, and all such counterparts or electronically signed documents shall together constitute one and the same Amendment. The revenue stamp on the digital original as referred to in Article 2 of

Tabella Allegato A – tariffa parte I del DPR n. 642/1972 è a carico della CRO ed è assolta da quest'ultima in modo virtuale ai sensi dell'art. 15 del D.P.R. n. 642/1972 e successive modificazioni, come da autorizzazione Agenzia delle Entrate n. 642/1972 rilasciata il 17/06/2020 dall'Agenzia delle Entrate Ufficio Territoriale di Desio (MB).

the table in Annex A – tariff part I of Presidential Decree 642/1972 is borne by the CRO and is paid by latter in a virtual manner pursuant to art. 15 of Presidential Decree n. 642/1972 and subsequent amendments, as authorized by the Revenue Agency n. 642/1972 of 17/06/2020 by Agenzia delle Entrate Ufficio Territoriale di Desio (MB).

Il presente Addendum n. 1 è stipulato in lingua italiana ed è tradotto in lingua inglese. In caso di difformità tra la versione italiana e quella inglese, prevale la versione in lingua italiana.

This Amendment is in Italian and translated into English. In case of discrepancies between the Italian version and the English version, the Italian version shall prevail.

Le Parti si danno reciprocamente atto che il presente Contratto è stato accettato in ogni sua parte e che non trovano pertanto applicazione le disposizioni di cui agli artt. 1341, 1342 Codice Civile.

The Parties mutually acknowledge that all parts of the Agreement were negotiated and, therefore, the provisions of Article 1341, 1342 of the Italian Civil Code do not apply.

In fede di che, le Parti, tramite persone debitamente autorizzate, hanno sottoscritto il presente Emendamento.

In Witness Whereof, the Parties have by duly authorized persons, executed this Amendment.

Per la CRO

Il Rappresentante legale

Dott.ssa Laura Ambrosoli

Firma digitale

Laura Ambrosoli 10.07.2023 11:27:58 GMT+01:00

For CRO

Legal Representative

Dr. Laura Ambrosoli

Digital signature

Laura Ambrosoli 10.07.2023 11:27:59 GMT+01:00

Per l'Ente	**For the Entity**
Il Commissario Straordinario Dott. Maurizio Montalbano	Extraordinary Commissioner Dr. Maurizio Montalbano
Firma Firmato digitalmente da: Maurizio Montalbano Data: 20/07/2023 13:23:06	Signature Firmato digitalmente da: Maurizio Montalbano Data: 20/07/2023 13:23:06

Attachment A

EC Standard Contractual Clauses

Standard Contractual Clauses

MODULE 1: Transfer controller to controller

SECTION I

Clause 1
Purpose and scope

(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.

(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').

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

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

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.

[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.

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); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

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.

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.

Clause 7

Docking clause

[*This clause is optional and has been intentionally omitted*].

SECTION II -
OBLIGATIONS OF THE PARTIES

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.

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.

(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.

(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.

(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.

8.3 Accuracy and data minimisation

(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.

(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.

(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.

8.4 Storage limitation

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 anonymisation ([2]) of the data and all back-ups at the end of the retention period.

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.

[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.

(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.

(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.

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.

8.7 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:

(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

[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.

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.

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.

8.9 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.

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

Clause 9

Use of sub-processors

[N/A]

Clause 10

Data subject rights

(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.

(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.

[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.

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

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.

(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.

(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.

Clause 12
Liability

(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.

Clause 13
Supervision

(a) 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.

(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.

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

Clause 14
Local laws and practices affecting compliance with the Clauses

(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.

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

(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;

(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 in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([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.

(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.

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

(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

[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.

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).

(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.

Clause 15

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

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.

(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.

(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.).

(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.

(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.

15.2 Review of legality and data minimisation

(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).

(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.

(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.

SECTION IV -
FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

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

(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).

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

(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;

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

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

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 have agreed otherwise.

(d) 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.

(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.

Clause 17
Governing law

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 Italy.

Clause 18

Choice of forum and jurisdiction

(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 EU Member State in which the data exporter is established.

(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.

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.

ANNEX I

A. LIST OF PARTIES

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]

Name:	AZIENDA OSPEDALIERA UNIVERSITARIA POLICLINICO "PAOLO GIACCONE" in PALERMO
Address:	Palermo, Via del Vespro, 129
Contact person's name, position and contact details:	Dott. Maurizio Montalbano Email: direzione.generale@policlinico.pa.it
Activities relevant to the data transferred under these Clauses:	Conduct of the Trial as outlined in the Agreement and the Protocol as defined the Agreement
Signature and date:	
Role (controller/processor):	Controller

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

Name:	Constellation Pharmaceuticals Inc.
Address:	470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA
Contact person's name, position and contact details:	Sanjaykumar Akhani mail: Sanjaykumar.Akhani@morphosys.com
Activities relevant to the data transferred under these Clauses:	Conduct of the Trial as outlined in the Agreement and the Protocol as defined the Agreement
Signature and date:	DocuSigned by: Sanjaykumar Akhani Signer Name: Sanjaykumar Akhani Signing Reason: I approve this document Signing Time: 07-Jul-2023 | 18:17 CEST 7803F690C79C4412B0959D5FACA04BB5
Role (controller/processor):	Controller

Name:	Constellation Pharmaceuticals Inc.
Address:	470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA
Contact person's name, position and contact details:	Regina Bönsch mail: Regina.Boensch@morphosys.com
Activities relevant to the data transferred under these Clauses:	Conduct of the Study/Trial as outlined in the Clinical Trial Agreement and the Protocol as defined the Clinical Trial Agreement
Signature and date:	DocuSigned by: Regina Bönsch Signer Name: Regina Bönsch Signing Reason: I approve this document Signing Time: 03-Jul-2023 | 10:23 CEST 455EC9363E64446A898A7BDBF37AFF36
Role (controller/processor):	Controller

Firmato digitalmente da:
Maurizio Montalbano
Data: 20/07/2023 13:23:06

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The personal data transferred concern the following categories of data subjects:

- Trial subjects and/or their relatives (in case of pregnancy of the Study Subject) ("**Study Subjects**")
- Entity staff ("**Institution Personnel**")

Categories of personal data transferred:

The personal data transferred concern the following categories of data:

For Study Subjects:
1. Health data and other sensitive data [see below for details]
2. Subject identification number assigned for research participation
3. Physical description and other personal characteristics (such as gender, childbearing potential, weight, height)

All personal data relating to Study Subjects is pseudonymized data.

For Institution Personnel:
1. Personal identification data (such as name, surname)
2. Contact information (such as telephone number, fax number, email address, address, practice / hospital / clinic location)
3. Professional and academic experience and qualifications
4. Financial information

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:

The personal data transferred concern the following special categories of data:

Any health, genetic and other sensitive data of Study Subjects included in the Study Data as required by the Protocol, including the following:

1. Racial or ethnic origin, in accordance with the Clinical Trial Agreement, the Protocol and informed consent form and in compliance with local applicable laws
2. Data related to health, such as without limitation:
- Prior therapy, concomitant medication, sub-sequent therapy
- Current medical conditions
- Relevant medical history
- Results of physical examination
- Testing results, images and tissue samples/slides (e.g. laboratory testing / radiology testing / assessment of samples or slides derived from bone marrow biopsy)
3. Genetic data derived from Biological Samples

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

On a continuous basis, as required for the performance of the Study and as set forth in the Clinical

Trial Agreement, Protocol and informed consent form and any written instructions issued by data importer.

Nature of the processing:

The processing involves for example collection, recording, organisation, filing, storage, adaptation or alteration, retrieval, disclosure by transmission, disclosure or any other form of provision, comparison or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing:

The personal data is processed in the scope of executing the Study as set out in the Clinical Trial Agreement, the Protocol, the informed consent form, and this Annex.

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

For a period of at least 25 years after completion or termination of the clinical trial, or longer if required by law.

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

Nature of the processing: The processing involves for example collection, recording, organisation, filing, storage, adaptation or alteration, retrieval, disclosure by transmission, disclosure or any other form of provision, comparison or combination, restriction, erasure or destruction. Subject matter: All services related to the conduct of the Study including: - Clinical trial application and reporting to health authorities and ethics committees as per local requirements - Testing of biological samples incl. samples derived from bone marrow biopsy - Radiology testing and assessment of images - Analysis of data - Publishing of results - Retention of trial information and data Duration: For a period of at least 25 years after completion or termination of the Study or longer if required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

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

Italian Data Protection Authority Email account: protocollo@gpdp.it

ANNEX II

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

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.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and organisational measures
according to Art. 32 Para. 1 GDPR
of
CONSTELLATION PHARMACEUTICALS INC

1 Measures to ensure confidentiality

2 **Entrance control** Is intended to prevent unauthorised persons from gaining physical access to data processing systems. Measures for building and room security.	Applicable (if yes, please tick)
Locking system	☒
Burglar-resistant windows/ Special glazing	☒
External security service	☒
Alarm system	☒
CCTV surveillance	☒
Access control concept	☒
Person verification at gatekeeper/reception desk	☒
Logging of visitor accesses / visitor book /visitor badges	☒
ID badges	☒
Electronic access code cards/ access transponders	☒
Security zones (visitor meeting, server rooms, workplaces, research)	☒
Existence of an authorisation overview for the security zones	☒
Self-closing doors are used when zones are crossed	☒
Authorisation cards (for individual zones)	☒
Key regulations	☒
Separately secured access to the server room	☒
Work instructions/guidelines regarding the locking of rooms when leaving/finishing work	☒
Careful choice of cleaning staff	☒

3 Access Control Intended to prevent unauthorised access to and use of data processing systems. System security.	Applicable (if yes, please tick)
Role-based security concept/ assignment of user rights	☒
Creation of user profiles	☒
Authorisation management	☒
Avoidance of group identifiers	☒
Documented process for assigning rights when new employees join the organisation	☒
Documented process for withdrawing rights when employees change departments	☒
Documented process for withdrawing rights when employees leave the company	☒
Functional and/or time-limited assignment of user authorisations	☒
Use of individual passwords	☒
Login with user name and password	☒
Automatic password-secured locking of the screen after inactivity (screen saver)	☒
Password policy with minimum password complexity requirements:	☒
• Minimum of 13 characters	☒
• Minimum of 13 characters for local admin passwords	☒
• Upper and lower case, special characters, number (of which at least 3 criteria)	☒
• Prevention of trivial passwords (e.g. password1, password2, 123456, qwerty)	☒
• Password history (no re-use of last passwords)	☒
• Input restriction of certain special characters to prevent SQL injections	☒
• Appropriately secure PW reset procedure	☒
Change cycle for passwords	☒
Failed login attempts are displayed to users	☒
Automatic blocking of user accounts after multiple incorrect PW entries	☒
Blocking passwords after security incident and reassignment	☒
Blocking passwords in case of suspected infringement	☒
Largely automatic (technical) implementation of the password policy	☒
Two- or multi-factor authentication for high-risk processes	☒
Hashing of stored passwords	☒
Encryption of networks	☒
Locking of data processing equipment (e.g. locked cage for servers).	☒
Deactivation of autostart of external media	☒
Programme check and release procedures for new installations	☒
Preventing the execution of downloaded software whose sources are marked as insecure	☒
Preventing automatic execution of programmes from temporary downloads	☒
Use of intrusion prevention systems	☒
Use of VPN technology	☒
Use of anti-virus software: server	☒
Use of anti-virus software: clients	☒
Use of a software firewall	☒
Use of a hardware firewall	☒

Default authentication information changed after software installation/first login	☒
Central device management	☒
Mobile device management	☒
For smartphones: access only after authentication	☒
For smartphone: Secure sources for apps, apps are tested and approved	☒
Storage of personal data/data carriers in lockable security cabinets or in separately secured rooms	☒
Policy on home office / teleworking	☒
Policy on private use of equipment or exclusion of private use	☒

4 Access control Shall prevent unauthorized activities in data processing systems outside granted authorizations.	Applicable (if yes, please tick)
Use of an authorization concept	☒
Minimal use of administrator accounts	☒
Different administrative roles according to least privilege concept (users, firewall, backups etc.)	☒
Separation of authorization approval (organizational) and authorization assignment (technical)	☒
Regulation for restoring data from backups (who, when, on whose request)	☒
Storage of data backups (e.g., tapes, CDs) in an access-protected safe	☒
Regular review of roles and permissions	☒
Partial access to databases and functions (read, write, execute)	☒
Time limitation of access possibilities	☒
Deactivation of unused standard server services	☒
Logging at firewall level to detect unauthorized access between networks	☒
Automatic notifications when unauthorized processing is suspected	☒
Logging of remote maintenance accesses	☒
Logging of file accesses	☒
Logging of file deletions	☒
Logging of file changes	☒
SPAM filter	☒
Intrusion detection (IDS)	☒
Instrusion Prevention (IPS)	☒
Restricted access to log files (Log Admin only)	☒
SSL certificates only from trusted sources	☒
Controlled destruction of data:	
• Data media disposal - secure deletion of data media (DIN 66399)	☒
• Sealed metal containers (so-called data protection garbage cans), disposal by service provider	☒
Connection of branch offices or home offices only via VPN connections with client certificate authentication	☒
Use of WLAN only on current routers with effective access mechanisms	☒
WLAN guest access without access to internal network	☒
Clean desk policy	☒

Checking incoming e-mails using anti-malware	☒
Security concept for handling printers, copiers, etc.	☒

5 Measures to ensure integrity

6 **Transfer Control** Shall ensure the security of data during electronic transmission and data transport and the auditability of the transfer.	Applicable (if yes, please tick)
How is data transmitted between the controller and third parties?	
• VPN connection	☒
• Secure File Transfer Protocol (sftp)	☒
E-mail encryption	
• SMIME	☒
• Sending e-mails with encrypted ZIP files	☒
Other transmission method: Share Point	☒
Use of signature procedure	☒
Documented management of data media, inventory control	☒
Encryption of mobile data carriers (e.g. laptop hard drives, external hard drives, USB sticks)	☒
Regulation on making copies of data records	☒
Making backup copies of data media that must be transported	☒
Direct collection, courier service, transport escort	☒

7 **Input control** The purpose is to ensure that it can be traced whether, who, and when personal data has been entered into data processing systems, changed or deleted.	Applicable (if yes, please tick)
Technical logging of the entry, modification and deletion of data	☒
Individual user names, no user groups	☒
Assignment of rights to enter, change and delete data based on an authorisation concept	☒
Organisational definition of input responsibilities	☒
Commitment to data secrecy	☒
Regulation on retention periods for auditing/evidence purposes	☒

8 Measures to ensure availability & resilience

9 **Availability control** Designed to protect data against accidental destruction or loss.	Applicable (if yes, please tick)
Fire alarm systems in server rooms	☒
Smoke detectors in server rooms	☒
Fire doors	☒
Waterless fire suppression systems in server rooms	☒
Lightning / overvoltage protection	☒
Air-conditioned server rooms	☒
Storage of backup systems in separate rooms and in separate fire compartment	☒

Server rooms not under or next to sanitary facilities	☒
Access to server rooms limited to necessary personnel only	☒
Alarm signal in case of unauthorised access to server rooms	☒
Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)	☒
CO2 fire extinguishers in the immediate vicinity of the server rooms	☒
UPS system (uninterruptible power supply)	☒
Documented data protection and backup concept	☒
Execution of data backups and creation of backups according to the 3-2-1 principle	☒
Emergency archive (outsourcing of data)	☒
Regular tests for data recovery	☒
At least one backup system cannot be encrypted by malicious code	☒
Separate partitions for operating system and data	☒
Emergency plan in place (BSI standard 200-4)	☒
Ensure long-term technical readability of backup storage media.	☒

10 Resilience (resilience and failure control) Shall enable systems to cope with risk-related changes and to demonstrate tolerance and compensatory capacity in the face of disruptions.	Applicable (if yes, please tick))
Redundant power supply	☒
Redundant data connection	☒
Redundant air conditioning	☒
Backup data centres available	☒
Computer Emergency Response Team (CERT)	☒
Carrying out penetration tests	☒
Immediate and regular activation of available software and firmware updates	☒
Regularly checking the configuration of the firewalls	☒
Regular sensitisation of employees (at least annually)	☒
Process for immediate reporting of incidents to IT is known to all employees	☒
Conclusion of a cyber insurance policy	☒

11 Measures for regular review, assessment and evaluation

12 Control procedures Shall ensure the effectiveness of data security measures.	Applicable (if yes, please tick)
Processing directories (Art. 30 I and II GDPR) are updated regularly	☒
Notification of new/modified data processing procedures to the data protection officer	☒
Processes for reporting new/changed procedures are documented	☒
Concepts and documentation are regularly reviewed (PDCA cycle)	☒
Review of the effectiveness of security measures taken at least annually	☒
Conduct security tests on web applications according to good practice procedures (e.g. OWASP Testing Guide)	☒
If findings are made during the aforementioned review, the security measures are adjusted in line with the risk.	☒
Process exists for responding to security breaches (attacks) and system malfunctions (incident response management)	☒

Documentation of security incidents	☒

13 Order control Shall ensure that data processed on behalf by service providers (subcontractors) are only processed in accordance with the principal's instructions.	Applicable (if yes, please tick)
Contract design in accordance with legal requirements (Art. 28 GDPR)	☒
Pre-contract checks at the contractor's premises before the start of the contract	☒
Regular checks at the contractor's premises after the start of the contract (during the term of the contract)	☒
Review of the contractor's data security concept	☒
Review of existing IT security certificates of the contractor	☒
Contractor has appointed data protection officer	☒

14 Separation control Data collected for different purposes shall also be processed separately.	Applicable (if yes, please tick)
Logical data separation (e.g. based on customer or client numbers)	☒
Separation of development, test and production systems	☒
For pseudonymised data: Separation of the assignment file & storage on a different system	☒

15 Other data protection or security management	Applicable (if yes, please tick)
Appropriate organisational structure for information security with clearly defined roles	☒
IT security officer appointed	☒
Use of data protection management software	☒
Data protection officer appointed	☒
Documented process for handling IT security incidents	☒
Documented process for handling data protection incidents	☒
Clear responsibilities for handling data protection and security incidents	☒
Documented process for ensuring data subject rights	☒
Central storage of policies/processes/procedural instructions accessible to all employees	☒
Guidelines/processes/procedural instructions are communicated within the company and known to all employees.	☒
External service providers are bound to secrecy, if necessary.	☒
Arrangements for effective data deletion on hardware that is taken back by the manufacturer or service provider	☒
Regular training on the guidelines and security processes	☒

Allegato A

Clausole contrattuali tipo della Commissione europea

CLAUSOLE CONTRATTUALI TIPO

MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento

SEZIONE I

Clausola 1
Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo è garantire il rispetto dei requisiti del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati) ([6]) per il trasferimento di dati personali verso un paese terzo.

b) Le parti:

   i) la o le persone fisiche o giuridiche, la o le autorità pubbliche, la o le agenzie o altri organismi (in seguito la o le "entità") che trasferiscono i dati personali, elencati nell'allegato I.A (di seguito "esportatore"), e

   ii) la o le entità di un paese terzo che ricevono i dati personali dall'esportatore, direttamente o indirettamente tramite un'altra entità anch'essa parte delle presenti clausole, elencate nell'allegato I.A (di seguito "importatore")

   hanno accettato le presenti clausole contrattuali tipo (di seguito: "clausole").

c) Le presenti clausole si applicano al trasferimento di dati personali come specificato nell'allegato I.B.

d) L'appendice alle presenti clausole contenente gli allegati ivi menzionati costituisce parte integrante delle presenti clausole.

Clausola 2
Effetto e invariabilità delle clausole

a) Le presenti clausole stabiliscono garanzie adeguate, compresi diritti azionabili degli interessati e mezzi di ricorso effettivi, in conformità dell'articolo 46, paragrafo 1, e dell'articolo 46, paragrafo 2, lettera c), del regolamento (UE) 2016/679 e, per quanto riguarda i trasferimenti di dati da titolari del trattamento a responsabili del trattamento e/o da responsabili del trattamento a responsabili del trattamento, clausole contrattuali tipo in conformità dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679, purché non siano modificate, tranne per selezionare il modulo o i moduli appropriati o per aggiungere o aggiornare informazioni nell'appendice. Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio e/o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

---

[6] Qualora l'esportatore sia un responsabile del trattamento soggetto al regolamento (UE) 2016/679 che agisce per conto di un'istituzione o di un organo dell'Unione in qualità di titolare del trattamento, l'utilizzo delle presenti clausole quando è fatto ricorso a un altro responsabile del trattamento (sub-trattamento) non soggetto al regolamento (UE) 2016/679 garantisce anche il rispetto dell'articolo 29, paragrafo (4), del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39), nella misura in cui le presenti clausole e gli obblighi in materia di protezione dei dati stabiliti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento in conformità dell'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725 sono allineati. Si tratta, in particolare, del caso in cui il titolare del trattamento e il responsabile del trattamento si basano sulle clausole contrattuali tipo incluse nella decisione 2021/915.

b) Le presenti clausole non pregiudicano gli obblighi cui è soggetto l'esportatore a norma del regolamento (UE) 2016/679.

Clausola 3
Terzi beneficiari

a) Gli interessati possono invocare e far valere le presenti clausole, in qualità di terzi beneficiari, nei confronti dell'esportatore e/o dell'importatore, con le seguenti eccezioni:

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

   ii) clausola 8 - modulo uno: clausola 8.5 e) e clausola 8.9 b); modulo due: clausola 8.1 b), 8.9 a), c), d) ed e); modulo tre: clausola 8.1 a), c) e d) e clausola 8.9 a), c), d), e), f) e g); modulo quattro: clausola 8.1 b) e clausola 8.3 b);

   iii) clausola 9 - modulo due: clausola 9 a), c), d) ed e); modulo tre: clausola 9 a), c), d) ed e);

   iv) clausola 12 - modulo uno: clausola 12 a) e d); moduli due e tre: clausola 12 a), d) e f);

   v) clausola 13;

   vi) clausola 15.1 c), d) ed e);

   vii) clausola 16 e);

   viii) clausola 18 - moduli uno, due e tre: clausola 18 a) e b); modulo quattro: clausola 18.

b) La lettera a) lascia impregiudicati i diritti degli interessati a norma del regolamento (UE) 2016/679.

Clausola 4
Interpretazione

a) Quando le presenti clausole utilizzano termini che sono definiti nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui a detto regolamento.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679.

Clausola 5
Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 6
Descrizione dei trasferimenti

I dettagli dei trasferimenti, in particolare le categorie di dati personali trasferiti e le finalità per le quali i dati sono trasferiti, sono specificati nell'allegato I.B.

Clausola 7

Clausola di adesione successiva

[*La presente clausola è facoltativa ed è stata intenzionalmente omessa*].

SEZIONE II -
OBBLIGHI DELLE PARTI

Clausola 8
Garanzie in materia di protezione dei dati

L'esportatore garantisce di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore, grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole.

8.1 Limitazione delle finalità

L'importatore tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'allegato I.B. Può trattare i dati personali per un'altra finalità soltanto:

i) se ha ottenuto il consenso preliminare dell'interessato;

ii) se il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o

iii) se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

8.2 Trasparenza

a) Per consentire agli interessati di esercitare effettivamente i propri diritti in conformità della clausola 10, l'importatore li informa, direttamente o tramite l'esportatore, circa:

   i) la sua identità e i suoi dati di contatto;

   ii) le categorie di dati personali trattati;

   iii) il diritto di ottenere una copia delle presenti clausole;

   iv) qualora intenda trasferire successivamente i dati personali a terzi, il destinatario o le categorie di destinatari (ove opportuno al fine di fornire informazioni significative), la finalità del trasferimento successivo e il motivo dello stesso in conformità della clausola 8.7.

b) La lettera a) non si applica se l'interessato dispone già delle informazioni, anche quando tali informazioni sono già state fornite dall'esportatore, o se la comunicazione delle informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato per l'importatore. In quest'ultimo caso l'importatore, per quanto possibile, rende pubbliche le informazioni.

c) Su richiesta, le parti mettono gratuitamente a disposizione dell'interessato una copia delle presenti clausole, compresa l'appendice da loro compilata. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, le parti possono espungere informazioni dall'appendice prima di trasmetterne una copia, fornendo tuttavia una sintesi significativa qualora l'interessato non sia altrimenti in grado di comprenderne il contenuto o di esercitare i propri diritti. Su richiesta, le parti comunicano all'interessato le ragioni delle espunzioni, per quanto possibile senza rivelare le informazioni espunte.

d) Le lettere da a) a c) lasciano impregiudicati gli obblighi incombenti all'esportatore a norma degli articoli 13 e 14 del regolamento (UE) 2016/679.

8.3 Esattezza e minimizzazione dei dati

a) Ciascuna parte provvede affinché i dati personali siano esatti e, se necessario, aggiornati. L'importatore adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

b) Se una parte viene a conoscenza del fatto che i dati personali che ha trasferito o ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo l'altra parte.

c) L'importatore provvede affinché i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

8.4 Limitazione della conservazione

L'importatore conserva i dati personali per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati. Mette in atto misure tecniche o organizzative adeguate per garantire il rispetto di tale obbligo, compresa la cancellazione o l'anonimizzazione ([7]) dei dati e di tutti i backup alla fine del periodo di conservazione.

8.5 Sicurezza del trattamento

a) L'importatore e, durante la trasmissione, anche l'esportatore mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali, compresa la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito «violazione dei dati personali»). Nel valutare l'adeguato livello di sicurezza, essi tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati. Le parti prendono in considerazione in particolare la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo.

b) Le parti concordano le misure tecniche e organizzative di cui all'allegato II. L'importatore effettua controlli regolari per garantire che tali misure continuino a offrire un adeguato livello di sicurezza.

c) L'importatore garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

d) In caso di una violazione dei dati personali trattati dall'importatore a norma delle presenti clausole, l'importatore adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

e) In caso di una violazione dei dati personali che possa presentare un rischio per i diritti e le libertà delle persone fisiche, l'importatore informa l'esportatore e l'autorità di controllo competente in conformità della clausola 13 senza ingiustificato ritardo. Tale notifica contiene i) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), ii) le sue

[7] Questo richiede di rendere anonimi i dati in modo tale che la persona non sia più identificabile da nessuno, in linea con il considerando 26 del regolamento (UE) 2016/679, e che tale processo sia irreversibile.

probabili conseguenze, iii) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e iv) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni. Nella misura in cui non gli sia possibile fornire le informazioni contestualmente, l'importatore può fornirle in fasi successive senza ulteriore ingiustificato ritardo.

f) In caso di una violazione dei dati personali che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'importatore informa senza ingiustificato ritardo gli interessati della violazione dei dati personali e della sua natura, se necessario in cooperazione con l'esportatore, unitamente alle informazioni di cui alla lettera e), punti da ii) a iv), a meno che l'importatore abbia attuato misure volte a ridurre in modo significativo il rischio per i diritti o le libertà delle persone fisiche o che la notifica implichi uno sforzo sproporzionato. In quest'ultimo caso, l'importatore effettua una comunicazione pubblica o adotta misure analoghe per informare il pubblico della violazione dei dati personali.

g) L'importatore documenta tutte le circostanze pertinenti relative alla violazione dei dati personali, comprese le sue conseguenze e i provvedimenti adottati per porvi rimedio, e ne tiene un registro.

8.6 Dati sensibili

Qualora il trasferimento riguardi dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (in prosieguo «dati sensibili»), l'importatore applica limitazioni specifiche e/o garanzie supplementari adeguate alla natura specifica dei dati e ai rischi connessi. Ciò può includere limitazioni del personale autorizzato ad accedere ai dati personali, misure di sicurezza supplementari (quali la pseudonimizzazione) e/o limitazioni aggiuntive all'ulteriore divulgazione.

8.7 Trasferimenti successivi

L'importatore non comunica i dati personali a terzi situati al di fuori dell'Unione europea ([8]) (nel suo stesso paese o in un altro paese terzo - di seguito: «trasferimento successivo»), a meno che il terzo sia o accetti di essere vincolato dalle presenti clausole, secondo il modulo appropriato. Altrimenti, il trasferimento successivo da parte dell'importatore può aver luogo solo se:

i) è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del regolamento (UE) 2016/679 che copre il trasferimento successivo;

ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del regolamento (UE) 2016/679 in relazione al trattamento in questione;

iii) il terzo stipula uno strumento vincolante con l'importatore che garantisce lo stesso livello di protezione dei dati previsto dalle presenti clausole e l'importatore fornisce una copia di tali garanzie all'esportatore;

iv) il trasferimento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari;

[8] L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La legislazione dell'Unione sulla protezione dei dati, regolamento (UE) 2016/679 compreso, è materia contemplata dall'accordo SEE, nel cui allegato XI è stata integrata. Pertanto, qualunque comunicazione da parte dell'importatore a terzi situati nel SEE non può essere considerata un trasferimento successivo ai fini delle presenti clausole.

v) il trasferimento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, o

vi) qualora non ricorra nessuna delle altre condizioni, l'importatore ha ottenuto il consenso esplicito dell'interessato al trasferimento successivo in una situazione specifica, dopo averlo informato delle sue finalità, dell'identità del destinatario e dei possibili rischi di siffatto trasferimento per l'interessato dovuti alla mancanza di garanzie adeguate in materia di protezione dei dati. In tal caso, l'importatore informa l'esportatore e, su richiesta di quest'ultimo, gli trasmette copia delle informazioni fornite all'interessato.

Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti clausole, in particolare la limitazione delle finalità.

8.8 Trattamento sotto l'autorità dell'importatore

L'importatore provvede affinché chiunque agisca sotto la sua autorità, compreso un responsabile del trattamento, tratti i dati soltanto su sua istruzione.

8.9 Documentazione e rispetto

a) Ciascuna parte deve essere in grado di dimostrare il rispetto degli obblighi che le incombono a norma delle presenti clausole. In particolare, l'importatore conserva documentazione adeguata delle attività di trattamento effettuate sotto la sua responsabilità.

b) Su richiesta, l'importatore mette tale documentazione a disposizione dell'autorità di controllo competente.

Clausola 9
Ricorso a sub-responsabili del trattamento

[Non applicabile]

Clausola 10
Diritti dell'interessato

a) L'importatore, se del caso con l'assistenza dell'esportatore, tratta qualunque richiesta di informazioni e richiesta ricevute da un interessato in relazione al trattamento dei suoi dati personali e all'esercizio dei suoi diritti in virtù delle presenti clausole senza ingiustificato ritardo, al più tardi entro un mese dal ricevimento della richiesta di informazioni o richiesta. ([9]) L'importatore adotta misure adeguate per agevolare tali richieste di informazioni, richieste e l'esercizio dei diritti dell'interessato. Tutte le informazioni fornite all'interessato sono in forma intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

b) In particolare, su richiesta dell'interessato, e gratuitamente, l'importatore:

   i) conferma all'interessato se i dati personali che lo riguardano sono o meno oggetto di trattamento e, in caso affermativo, fornisce una copia di tali dati e le informazioni di cui all'allegato I; se i dati personali sono stati o saranno oggetto di un trasferimento successivo, fornisce informazioni circa i destinatari o le categorie di destinatari (se del caso al fine di fornire informazioni significative) a cui i dati personali sono stati o saranno trasferiti, la finalità di tali trasferimenti successivi e il loro motivo in conformità della clausola 8.7; e fornisce informazioni sul diritto di proporre reclamo a un'autorità di controllo conformemente alla clausola 12, lettera c), punto i);

   ii) rettifica i dati inesatti o incompleti dell'interessato;

   iii) cancella i dati personali dell'interessato se tali dati sono o sono stati trattati in violazione di una delle presenti clausole, garantendo i diritti del terzo beneficiario, o se l'interessato revoca il consenso su cui si basa il trattamento.

c) Qualora l'importatore tratti i dati personali per finalità di marketing diretto, cessa il trattamento per tali finalità se l'interessato vi si oppone.

d) L'importatore non prende alcuna decisione basata unicamente sul trattamento automatizzato dei dati personali trasferiti (di seguito «decisione automatizzata»), che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, salvo con il consenso esplicito dell'interessato o se autorizzato in tal senso dalla legislazione del paese di destinazione, a condizione che tale legislazione preveda misure adeguate a tutela dei diritti e dei legittimi interessi dell'interessato. In tal caso l'importatore, se necessario in cooperazione con l'esportatore:

   i) informa l'interessato della prevista decisione automatizzata, delle conseguenze previste e della logica utilizzata; e

   ii) attua garanzie adeguate, consentendo almeno all'interessato di contestare la decisione, esprimere la propria opinione e ottenere il riesame da parte di un essere umano.

[9] Tale termine può essere prorogato al massimo di due mesi, se necessario, tenuto conto della complessità e del numero di richieste. L'importatore informa debitamente e prontamente l'interessato di tale proroga.

e) Qualora le richieste dell'interessato siano eccessive, in particolare per il carattere ripetitivo, l'importatore può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi dell'accoglimento della richiesta o rifiutarsi di soddisfare la richiesta.

f) L'importatore può rifiutare la richiesta dell'interessato se tale rifiuto è consentito dalla legislazione del paese di destinazione ed è necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679.

g) Se l'importatore intende rifiutare la richiesta dell'interessato, informa quest'ultimo dei motivi del rifiuto e della possibilità di proporre reclamo all'autorità di controllo competente e/o di proporre ricorso giurisdizionale.

Clausola 11
Ricorso

a) L'importatore informa gli interessati, in forma trasparente e facilmente accessibile, mediante avviso individuale o sul suo sito web, di un punto di contatto autorizzato a trattare i reclami. Tratta prontamente qualunque reclamo ricevuto da un interessato.

b) In caso di controversia tra un interessato e una delle parti sul rispetto delle presenti clausole, la parte in questione fa tutto il possibile per risolvere la questione in via amichevole in modo tempestivo. Le parti si tengono reciprocamente informate di tali controversie e, se del caso, cooperano per risolverle.

c) Qualora l'interessato invochi un diritto del terzo beneficiario in conformità della clausola 3, l'importatore accetta la decisione dell'interessato di:

   i) proporre reclamo all'autorità di controllo dello Stato membro di residenza abituale o del luogo di lavoro o all'autorità di controllo competente in conformità della clausola 13;

   ii) deferire la controversia agli organi giurisdizionali competenti ai sensi della clausola 18.

d) Le parti accettano che l'interessato possa essere rappresentato da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni di cui all'articolo 80, paragrafo 1, del regolamento (UE) 2016/679.

e) L'importatore si attiene a qualunque decisione vincolante a norma della legislazione applicabile dell'UE o degli Stati membri.

f) L'importatore dichiara che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla legislazione applicabile.

Clausola 12
Responsabilità

a) Ciascuna parte è responsabile nei confronti delle altre parti per i danni che essa ha causato loro violando le presenti clausole.

b) Ciascuna parte è responsabile nei confronti dell'interessato per i danni materiali o immateriali che essa gli ha causato violando i diritti del terzo beneficiario previsti dalle presenti clausole, e

l'interessato ha il diritto di ottenere il risarcimento. Ciò lascia impregiudicata la responsabilità dell'esportatore a norma del regolamento (UE) 2016/679.

c) Qualora più di una parte sia responsabile per un danno causato all'interessato a seguito di una violazione delle presenti clausole, tutte le parti responsabili sono responsabili in solido e l'interessato ha il diritto di agire in giudizio contro una qualunque di loro.

d) Le parti convengono che, se una delle parti è ritenuta responsabile a norma della lettera (c), essa ha il diritto di reclamare dalle altre parti la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

e) L'importatore non può invocare il comportamento di un responsabile del trattamento o un sub-responsabile del trattamento per sottrarsi alla propria responsabilità.

Clausola 13
Controllo

a) L'autorità di controllo responsabile di garantire che l'esportatore rispetti il regolamento (UE) 2016/679 per quanto riguarda il trasferimento dei dati, quale indicata all'allegato I.C, agisce in qualità di autorità di controllo competente.

b) L'importatore accetta di sottoporsi alla giurisdizione dell'autorità di controllo competente e di cooperare con la stessa nell'ambito di qualunque procedura volta a garantire il rispetto delle presenti clausole. In particolare, l'importatore accetta di rispondere alle richieste di informazioni, sottoporsi ad attività di revisione e rispettare le misure adottate dall'autorità di controllo, comprese le misure di riparazione e risarcimento. Fornisce all'autorità di controllo conferma scritta che sono state adottate le misure necessarie.

SEZIONE III - LEGISLAZIONE E OBBLIGHI LOCALI IN CASO DI ACCESSO DA PARTE DI AUTORITÀ PUBBLICHE

Clausola 14

Legislazione e prassi locali che incidono sul rispetto delle clausole

a) Le parti garantiscono di non avere motivo di ritenere che la legislazione e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore, compresi eventuali requisiti di comunicazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscano all'importatore di rispettare gli obblighi che gli incombono a norma delle presenti clausole. Ciò si basa sul presupposto che la legislazione e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del regolamento (UE) 2016/679 non sono in contraddizione con le presenti clausole.

b) Le parti dichiarano che nel fornire la garanzia di cui alla lettera a), hanno tenuto conto in particolare dei seguenti elementi:

   i) le circostanze specifiche del trasferimento, tra cui la lunghezza della catena di trattamento, il numero di attori coinvolti e i canali di trasmissione utilizzati; i trasferimenti successivi previsti; il tipo di destinatario; la finalità del trattamento; le categorie e il formato dei dati personali trasferiti; il settore economico in cui ha luogo il trasferimento; il luogo di conservazione dei dati trasferiti;

   ii) la legislazione e le prassi del paese terzo di destinazione – comprese quelle che impongono la comunicazione di dati alle autorità pubbliche o che le autorizzano ad accedere ai dati – pertinenti alla luce delle circostanze specifiche del trasferimento, nonché le limitazioni e le garanzie applicabili ([10]);

   iii) qualunque garanzia contrattuale, tecnica o organizzativa pertinente predisposta per integrare le garanzie di cui alle presenti clausole, comprese le misure applicate durante la trasmissione e il trattamento dei dati personali nel paese di destinazione.

c) L'importatore garantisce che, nell'effettuare la valutazione di cui alla lettera b), ha fatto tutto il possibile per fornire all'esportatore le informazioni pertinenti e dichiara che continuerà a cooperare con l'esportatore per garantire il rispetto delle presenti clausole.

d) Le parti accettano di documentare la valutazione di cui alla lettera b) e di metterla a disposizione dell'autorità di controllo competente su richiesta.

e) L'importatore accetta di informare prontamente l'esportatore se, dopo aver accettato le presenti clausole e per la durata del contratto, ha motivo di ritenere di essere, o essere

[10] Per quanto riguarda l'impatto della legislazione e delle prassi sul rispetto delle presenti clausole, possono essere presi in considerazione diversi elementi nell'ambito di una valutazione globale. Tali elementi possono includere un'esperienza pratica pertinente e documentata in casi precedenti di richieste di comunicazione da parte di autorità pubbliche, o l'assenza di tali richieste, per un periodo di tempo sufficientemente rappresentativo. Si tratta in particolare di registri interni o altra documentazione, elaborati su base continuativa conformemente alla dovuta diligenza e certificati a livello di alta dirigenza, sempre che tali informazioni possano essere lecitamente condivise con terzi. Qualora per concludere che all'importatore non sarà impedito di rispettare le presenti clausole si faccia affidamento su questa esperienza pratica, essa deve essere sostenuta da altri elementi pertinenti e oggettivi, e spetta alle parti valutare attentamente se tali elementi, congiuntamente, abbiano un peso sufficiente in termini di affidabilità e rappresentatività per sostenere tale conclusione. In particolare, le parti devono considerare se la loro esperienza pratica è corroborata e non contraddetta da informazioni disponibili al pubblico, o altrimenti accessibili, e affidabili sull'esistenza o sull'assenza di richieste nello stesso settore e/o sull'applicazione pratica della legislazione, come la giurisprudenza e le relazioni di organi di vigilanza indipendenti.

diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla lettera a), anche a seguito di una modifica della legislazione del paese terzo o di una misura (ad esempio una richiesta di comunicazione) che indichi un'applicazione pratica di tale legislazione che non è conforme ai requisiti di cui alla lettera a).

f) A seguito di una notifica in conformità della lettera e), o se ha altrimenti motivo di ritenere che l'importatore non sia più in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole, l'esportatore individua prontamente le misure adeguate (ad esempio, misure tecniche o organizzative per garantire la sicurezza e la riservatezza) che egli stesso e/o l'importatore devono adottare per far fronte alla situazione. L'esportatore sospende il trasferimento dei dati se ritiene che non possano essere assicurate garanzie adeguate per tale trasferimento, o su istruzione dell'autorità di controllo competente. In tal caso l'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole. Se le parti del contratto sono più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della parte interessata, salvo diversamente concordato dalle parti. In caso di risoluzione del contratto in conformità della presente clausola, si applica la clausola 16, lettere d) ed e).

Clausola 15

Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche

15.1 Notifica

a) L'importatore accetta di informare prontamente l'esportatore e, ove possibile, l'interessato (se necessario con l'aiuto dell'esportatore) se:

   i) riceve una richiesta giuridicamente vincolante di un'autorità pubblica, comprese le autorità giudiziarie, a norma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende informazioni sui dati personali richiesti, sull'autorità richiedente, sulla base giuridica della richiesta e sulla risposta fornita; o

   ii) viene a conoscenza di qualunque accesso diretto effettuato, conformemente alla legislazione del paese terzo di destinazione, da autorità pubbliche ai dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende tutte le informazioni disponibili all'importatore.

b) Se la legislazione del paese di destinazione vieta all'importatore di informare l'esportatore e/o l'interessato, l'importatore accetta di fare tutto il possibile per ottenere un'esenzione dal divieto, al fine di comunicare al più presto quante più informazioni possibili. Per poterlo dimostrare su richiesta dell'esportatore, l'importatore accetta di documentare di aver fatto tutto il possibile.

c) Laddove consentito dalla legislazione del paese di destinazione, l'importatore accetta di fornire periodicamente all'esportatore, per la durata del contratto, quante più informazioni pertinenti possibili sulle richieste ricevute (in particolare, il numero di richieste, il tipo di dati richiesti, la o le autorità richiedenti, se le richieste sono state contestate e l'esito di tali contestazioni ecc.).

d) L'importatore accetta di conservare le informazioni di cui alle lettere da a) a c) per la durata del contratto e di metterle a disposizione dell'autorità di controllo competente su richiesta.

e) Le lettere da a) a c) lasciano impregiudicato l'obbligo dell'importatore in conformità della clausola 14, lettera e), e della clausola 16 di informare prontamente l'esportatore qualora non sia in grado di rispettare le presenti clausole.

15.2 Riesame della legittimità e minimizzazione dei dati

a) L'importatore accetta di riesaminare la legittimità della richiesta di comunicazione, in particolare il fatto che essa rientri o meno nei poteri conferiti all'autorità pubblica richiedente, e di contestarla qualora, dopo un'attenta valutazione, concluda che sussistono fondati motivi per ritenere che essa sia illegittima a norma della legislazione del paese di destinazione, compresi gli obblighi applicabili a norma del diritto internazionale e dei principi di cortesia internazionale. L'importatore, alle stesse condizioni, si avvale delle possibilità di ricorso. Quando contesta una richiesta, l'importatore chiede l'adozione di provvedimenti provvisori affinché gli effetti della richiesta siano sospesi fintantoché l'autorità giudiziaria competente non abbia deciso nel merito. Non comunica i dati personali richiesti fino a quando non sia tenuto a farlo ai sensi delle norme procedurali applicabili. Tali requisiti lasciano impregiudicati gli obblighi dell'importatore a norma della clausola 14, lettera (e).

b) L'importatore accetta di documentare la propria valutazione giuridica e qualunque contestazione della richiesta di comunicazione e, nella misura consentita dalla legislazione del paese di destinazione, mette tale documentazione a disposizione dell'esportatore. Su richiesta, la mette a disposizione anche dell'autorità di controllo competente.

c) Quando risponde a una richiesta di comunicazione l'importatore accetta di fornire la quantità minima di informazioni consentite, sulla base di un'interpretazione ragionevole della richiesta.

SEZIONE IV - DISPOSIZIONI FINALI

Clausola 16
Inosservanza delle clausole e risoluzione

a) L'importatore informa prontamente l'esportatore qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Qualora l'importatore violi le presenti clausole o non sia in grado di rispettarle, l'esportatore sospende il trasferimento dei dati personali all'importatore fino a che il rispetto non sia nuovamente garantito o il contratto non sia risolto. Ciò lascia impregiudicata la clausola 14, lettera f).

c) L'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora:

   i) l'esportatore abbia sospeso il trasferimento dei dati personali all'importatore in conformità della lettera (b) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

   ii) l'importatore violi in modo sostanziale o persistente le presenti clausole; o

   iii) l'importatore non si conformi a una decisione vincolante di un organo giurisdizionale competente o di un'autorità di controllo competente in merito agli obblighi che gli incombono a norma delle presenti clausole.

   In tali casi, informa l'autorità di controllo competente di tale inosservanza. Qualora le parti del contratto siano più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della parte interessata, salvo diversamente concordato dalle parti.

d) I dati personali che sono stati trasferiti prima della risoluzione del contratto in conformità della lettera c) sono, a scelta dell'esportatore, restituiti immediatamente all'esportatore o cancellati integralmente. Lo stesso vale per qualunque copia dei dati. L'importatore certifica all'esportatore la cancellazione dei dati. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali trasferiti, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale.

e) Ciascuna parte può revocare il proprio accordo a essere vincolata dalle presenti clausole qualora i) la Commissione europea adotti una decisione in conformità dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 riguardante il trasferimento di dati personali cui si applicano le presenti clausole; o ii) il regolamento (UE) 2016/679 diventi parte del quadro giuridico del paese verso il quale i dati personali sono trasferiti. Ciò lascia impregiudicati gli altri obblighi che si applicano al trattamento in questione a norma del regolamento (UE) 2016/679.

Clausola 17
Legge applicabile

Le presenti clausole sono disciplinate dalla legge di uno degli Stati membri dell'UE, purché essa riconosca i diritti del terzo beneficiario. Le parti convengono che tale legge è quella italiana.

Clausola 18
Scelta del foro e giurisdizione

a) Qualunque controversia derivante dalle presenti clausole è risolta dagli organi giurisdizionali di uno Stato membro dell'UE.

b) Le Parti concordano che tali tribunali saranno quelli dello Stato membro dell'UE in cui è stabilito l'esportatore di dati stabilito.

c) L'interessato può agire in giudizio contro l'esportatore e/o l'importatore anche dinanzi agli organi giurisdizionali dello Stato membro in cui ha la propria residenza abituale.

d) Le parti accettano di sottoporsi alla giurisdizione di tali organi giurisdizionali.

APPENDICE

NOTA ESPLICATIVA:
Deve essere possibile distinguere chiaramente le informazioni applicabili a ciascun trasferimento o a ciascuna categoria di trasferimenti e, a tale riguardo, determinare i ruoli rispettivi delle parti quali esportatori e/o importatori. Non occorre per forza compilare e firmare appendici distinte per ciascun trasferimento/categoria di trasferimenti e/o rapporto contrattuale laddove tale trasparenza possa essere garantita con un'unica appendice. Tuttavia, ove necessario per assicurare una sufficiente chiarezza, dovrebbero essere utilizzate appendici distinte.

ALLEGATO I

A. ELENCO DELLE PARTI

Esportatore/i:
[Identità e dati di contatto del o degli esportatori e, se del caso, del suo/loro responsabile della protezione dei dati e/o rappresentante nell'Unione europea]

Nome:	AZIENDA OSPEDALIERA UNIVERSITARIA POLICLINICO "PAOLO GIACCONE" in PALERMO
Indirizzo:	Palermo, Via del Vespro, 129
Nome, qualifica e dati di contatto del referente:	Dott. Maurizio Montalbano direzione.generale@policlinico.pa.it
Attività pertinenti ai dati trasferiti a norma delle presenti clausole:	Conduzione della Sperimentazione di cui al Contratto per la conduzione della sperimentazione clinica su medicinali "CPI-0610" ("Contratto") e al Protocollo, come definito nel Contratto
Firma e data:	
Ruolo (titolare del trattamento/responsabile del trattamento):	Titolare del trattamento

Importatore/i:
[Identità e dati di contatto del o degli importatori, compreso qualsiasi referente con responsabilità in materia di protezione dei dati]

Nome:	Constellation Pharmaceuticals Inc.
Indirizzo:	470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA
Nome, qualifica e dati di contatto del referente:	Sanjaykumar Akhani mail: Sanjaykumar.Akhani@morphosys.com
Attività pertinenti ai dati trasferiti a norma delle presenti clausole:	Conduzione della Sperimentazione di cui al Contratto e al Protocollo, come definito nel Contratto
Firma e data:	DocuSigned by: Sanjaykumar Akhani Signer Name: Sanjaykumar Akhani Signing Time: 07-Jul-2023 | 18:17 CEST 7803F690C79C4412B0959D5FACA04BB5
Ruolo (titolare del trattamento/responsabile del trattamento):	Titolare del trattamento Firmato digitalmente da: Maurizio Montalbano Data: 20/07/2023 13:23:07

Nome:	Constellation Pharmaceuticals Inc.
Indirizzo:	470 Atlantic Ave, Ste. 1401, Boston, MA 02110-2264 USA
Nome, qualifica e dati di contatto del referente:	Regina Bönsch Regina.Boensch@morphosys.com
Attività pertinenti ai dati trasferiti a norma delle presenti clausole:	Conduzione della Sperimentazione di cui al Contratto e al Protocollo, come definito nel Contratto
Firma e data:	DocuSigned by: Regina Bönsch Signer Name: Regina Bönsch Signing Time: 03-Jul-2023 | 10:23 CEST 455EC9363E64446A898A7BDBF37AFF36
Ruolo (titolare del trattamento/responsabile del trattamento):	Titolare del trattamento

B. DESCRIZIONE DEL TRASFERIMENTO

Categorie di interessati i cui dati personali sono trasferiti:

I dati personali trasferiti riguardano le seguenti categorie di interessati:

- Interessati partecipanti alla sperimentazione, come definiti nel Contratto, e/o i loro parenti (in caso di gravidanza dell'interessato partecipante alla sperimentazione clinica) (**"Soggetti dello studio"**)
- Staff e personale dell'Ente e dell'Università (**"Personale dell'Istituto"**)

Categorie di dati personali trasferiti

I dati personali trasferiti riguardano le seguenti categorie di dati:

Per i Soggetti dello studio:
1. Dati sanitari e altri dati sensibili [per maggiori informazioni, fare riferimento a quanto segue]
2. Numero identificativo assegnato al soggetto per la partecipazione allo studio
3. Descrizione fisica e altre caratteristiche personali (quali sesso, fertilità, peso, altezza)
Tutti i dati personali relativi ai Soggetti dello studio sono pseudonimizzati.

Per il Personale dell'istituto:
1. Dati di identificazione personale (quali nome, cognome)
2. Recapiti (quali numero di telefono, numero di fax, indirizzo e-mail, indirizzo postale, sede dello studio/dell'ospedale/dell'ambulatorio)
3. Esperienza e qualifiche professionali e accademiche
4. Informazioni finanziarie

Dati sensibili trasferiti (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari:

I dati personali trasferiti riguardano le seguenti categorie particolari di dati:

Tutti i dati sanitari, genetici e altri dati sensibili dei Soggetti dello studio, come richiesto dal Protocollo, quali:

1. Origine razziale o etnica, in conformità al Contratto, al Protocollo e al modulo di consenso informato e ai sensi della legislazione locale applicabile
2. Dati sanitari, quali ad esempio:
- Terapia precedente, concomitante e successiva
- Attuali condizioni cliniche
- Informazioni anamnestiche pertinenti
- Risultati dell'esame obiettivo
- Risultati degli esami, immagini e campioni/vetrini istologici (ad es. esami di laboratorio esami radiologici, valutazione di campioni o vetrini derivanti da biopsia osteomidollare)
3. Dati genetici derivanti da campioni biologici

La frequenza del trasferimento (ad esempio se i dati sono trasferiti come evento singolo o su base continua):

Su base continua, come richiesto per l'esecuzione della Sperimentazione e come stabilito nel Contratto, nel Protocollo e nel modulo di consenso informato, nonché in qualsiasi

istruzione scritta fornita dall'importatore.

Natura del trattamento:

Il trattamento comporta, ad esempio, la raccolta, la registrazione, l'organizzazione, l'archiviazione, la conservazione, l'adattamento o la modifica, l'estrazione, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Finalità del trasferimento dei dati e dell'ulteriore trattamento:

I dati personali sono trattati nell'ambito dell'esecuzione della Sperimentazione, come descritto nel Contratto, nel Protocollo, nel modulo di consenso informato e nel presente Allegato.

Periodo di conservazione dei dati personali oppure, se non è possibile, criteri utilizzati per determinare tale periodo:

Per un periodo di almeno 25 anni dopo il completamento o il termine della sperimentazione clinica oppure per un periodo più lungo se richiesto dalla legge.

Per i trasferimenti a (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento:

Natura del trattamento: Il trattamento comporta, ad esempio, la raccolta, la registrazione, l'organizzazione, l'archiviazione, la conservazione, l'adattamento o la modifica, l'estrazione, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Materia disciplinata: Tutti i servizi relativi alla conduzione della Sperimentazione, tra cui:
- Domanda di sperimentazione clinica e comunicazione alle autorità sanitarie e ai comitati etici in conformità alla normativa locale
- Analisi di campioni biologici, compresi i campioni derivanti da biopsia osteomidollare
- Esami radiologici e valutazione delle immagini
- Analisi dei dati
- Pubblicazione dei risultati
- Conservazione delle informazioni e dei dati relativi alla sperimentazione

Durata: Per un periodo di almeno 25 anni dopo il completamento o il termine della sperimentazione clinica oppure per un periodo più lungo se richiesto dalla legislazione applicabile.

C. AUTORITÀ DI CONTROLLO COMPETENTE

Identificare la o le autorità di controllo competenti conformemente alla clausola 13:

Italian Data Protection Authority Email account: protocollo@gpdp.it

ALLEGATO II
MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in termini specifici (e non generici). Si veda anche la nota esplicativa nella prima pagina dell'appendice, in particolare riguardo alla necessità di indicare chiaramente quali misure si applicano a ciascun trasferimento/insieme di trasferimenti.

Descrizione delle misure tecniche e organizzative messe in atto dal o dagli importatori (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

Misure tecniche e organizzative ai sensi dell'art. 32, paragrafo 1, del regolamento generale sulla protezione dei dati di

CONSTELLATION PHARMACEUTICALS INC

Misure per garantire la riservatezza

Controllo degli ingressi Ha lo scopo di impedire alle persone non autorizzate l'accesso fisico ai sistemi per il trattamento dei dati. Misure per la sicurezza degli edifici e dei locali.	Applicabile (se sì, barrare)
Sistema di chiusura	☒
Finestre antieffrazione/Vetri speciali	☒
Servizio di sicurezza esterno	☒
Impianto di allarme	☒
Sorveglianza con telecamere a circuito chiuso	☒
Piano di controllo degli accessi	☒
Verifica delle persone presso la portineria/la reception	☒
Registrazione degli accessi dei visitatori/registro dei visitatori/badge per i visitatori	☒
Badge identificativi	☒
Schede elettroniche con codice di accesso/transponder di accesso	☒
Aree di sicurezza (area riunioni ospiti, sale server, aree di lavoro, ricerca)	☒
Panoramica delle autorizzazioni per le aree di sicurezza	☒
Il passaggio da un'area all'altra avviene attraverso porte munite di chiudiporta	☒
Tessere di autorizzazione (per singole aree)	☒
Norme riguardo alle chiavi	☒
Accesso alla sala server protetto e indipendente	☒
Istruzioni/linee guida relative alla chiusura dei locali all'uscita/al termine del lavoro	☒
Selezione accurata del personale addetto alle pulizie	☒

Controllo degli accessi Ha lo scopo di impedire l'accesso e l'utilizzo non autorizzati dei sistemi per il trattamento dei dati. Sicurezza del sistema.	Applicabile (se sì, barrare)
Piano di sicurezza basato su ruoli/assegnazione di diritti degli utenti	☒
Creazione di profili utente	☒
Gestione delle autorizzazioni	☒
Utilizzo degli identificativi di gruppo non consentito	☒
Processo documentato di assegnazione dei diritti qualora nuovi dipendenti entrino a far parte dell'organizzazione	☒
Processo documentato di revoca dei diritti qualora i dipendenti cambino reparto	☒
Processo documentato di revoca dei diritti qualora i dipendenti lascino la società	☒
Assegnazione funzionale e/o limitata nel tempo delle autorizzazioni concesse agli utenti	☒
Utilizzo di password individuali	☒
Login mediante nome utente e password	☒
Blocco automatico dello schermo protetto da password dopo un determinato periodo di inattività (screen saver)	☒
Politica sulle password con requisiti minimi di complessità:	☒

• Minimo 13 caratteri	☒
• Minimo 13 caratteri per le password degli amministratori locali	☒
• Maiuscole e minuscole, caratteri speciali, numeri (almeno 3 criteri)	☒
• Esclusione di password banali (ad es. password1, password2, 123456, qwerty)	☒
• Cronologia delle password (impossibilità di riutilizzo delle ultime password)	☒
• Limitazione dell'inserimento di alcuni caratteri speciali per prevenire le SQL injection	☒
• Procedura di reimpostazione delle password adeguatamente protetta	☒
Cambio ciclico delle password	☒
Visualizzazione dei tentativi di accesso non andati a buon fine	☒
Blocco automatico dell'account utente dopo più inserimenti errati della password	☒
Blocco delle password dopo eventuali incidenti di sicurezza e riassegnazione	☒
Blocco delle password in caso di sospetta violazione	☒
Implementazione prevalentemente automatica (tecnica) della politica sulle password	☒
Autenticazione a due o più fattori per i processi ad alto rischio	☒
Hashing delle password memorizzate	☒
Crittografia delle reti	☒
Conservazione sotto chiave delle apparecchiature di elaborazione dati (ad es. gabbie chiuse per i server)	☒
Disattivazione dell'avvio automatico dei supporti esterni	☒
Procedure di verifica e rilascio dei programmi di nuova installazione	☒
Impossibilità di esecuzione di software scaricato i cui sorgenti siano contrassegnati come non sicuri	☒
Impossibilità di esecuzione automatica di programmi da download temporanei	☒
Utilizzo di sistemi di prevenzione delle intrusioni	☒
Utilizzo della tecnologia VPN	☒
Utilizzo di software antivirus: server	☒
Utilizzo di software antivirus: client	☒
Utilizzo di un firewall software	☒
Utilizzo di un firewall hardware	☒
Modifica delle informazioni di autenticazione predefinite dopo l'installazione del software/il primo accesso	☒
Gestione centralizzata dei dispositivi	☒
Gestione dei dispositivi mobili	☒
Per gli smartphone: accesso solo previa autenticazione	☒
Per gli smartphone: app da fonti sicure, verificate e approvate	☒
Conservazione dei dati/supporti dei dati personali in armadi di sicurezza dotati di serratura o in locali protetti e separati	☒
Politica in materia di lavoro da casa/telelavoro	☒
Politica in materia di uso privato delle apparecchiature o esclusione dell'uso privato	☒

Controllo degli accessi Impedisce le attività non autorizzate nei sistemi per il trattamento dei dati, al di fuori delle autorizzazioni concesse.	Applicabile (se sì, barrare)
Utilizzo di un sistema di autorizzazione	☒
Uso minimo di account amministratore	☒
Diversificazione dei ruoli amministrativi secondo il principio del minor privilegio (utenti, firewall, backup ecc.)	☒
Separazione tra approvazione dell'autorizzazione (organizzativa) e assegnazione dell'autorizzazione (tecnica)	☒
Regolamento per il ripristino dei dati dai backup (chi, quando, su richiesta di chi)	☒
Conservazione dei backup dei dati (ad es. nastri, CD) in una cassaforte	☒
Riesame periodico dei ruoli e delle autorizzazioni	☒
Accesso parziale a database e funzioni (lettura, scrittura, esecuzione)	☒
Limitazione temporale delle possibilità di accesso	☒
Disattivazione dei servizi standard del server non utilizzati	☒
Registrazione a livello di firewall per rilevare gli accessi non autorizzati tra le reti	☒
Notifiche automatiche in caso di sospetto trattamento non autorizzato	☒
Registrazione degli accessi per la manutenzione a distanza	☒
Registrazione degli accessi ai file	☒
Registrazione delle cancellazioni di file	☒
Registrazione delle modifiche ai file	☒
Filtro posta indesiderata	☒
Rilevamento delle intrusioni (IDS)	☒
Prevenzione delle intrusioni (IPS)	☒
Limitazione dell'accesso ai file di registro (solo Log Admin)	☒
Certificati SSL solo da fonti affidabili	☒
Distruzione controllata dei dati:	
• Smaltimento dei supporti dei dati - cancellazione sicura dei supporti dei dati (DIN 66399)	☒
• Contenitori metallici sigillati (contenitori di sicurezza per lo smaltimento di dati riservati), smaltimento da parte del fornitore di servizi	☒
Connessione di filiali o postazioni domestiche solo tramite VPN con autenticazione del certificato client	☒
Utilizzo di WLAN solo su router attuali con meccanismi di accesso efficaci	☒
Accesso guest alla WLAN senza accesso alla rete interna	☒
Politica della scrivania pulita	☒
Controllo della posta elettronica in arrivo tramite anti-malware	☒
Piano di sicurezza per la gestione di stampanti, fotocopiatrici ecc.	☒

Misure per garantire l'integrità

Controllo dei trasferimenti Garantisce la sicurezza dei dati durante la trasmissione elettronica e il trasporto dei dati, nonché la verificabilità del trasferimento.	Applicabile (se sì, barrare)
Come vengono trasmessi i dati tra titolare del trattamento e terzi?	
• Connessione VPN	☒
• Secure File Transfer Protocol (SFTP)	☒
Crittografia delle e-mail	
• S/MIME	☒
• Invio di e-mail con file ZIP crittografati	☒
Altri metodi di trasmissione: Punto di condivisione	☒
Utilizzo di una procedura di firma	☒
Gestione documentata dei supporti dei dati, controllo dell'inventario	☒
Crittografia dei supporti dei dati mobili (ad es. dischi rigidi di computer portatili, dischi rigidi esterni, chiavette USB)	☒
Regolamento sulla realizzazione di copie di record di dati	☒
Esecuzione di copie di backup di supporti di dati che devono essere trasportati	☒
Raccolta diretta, servizio di corriere, scorta per il trasporto	☒

Controllo degli inserimenti Ha lo scopo di garantire che si possa stabilire se, da chi e quando i dati personali sono stati inseriti, modificati o cancellati nei sistemi per il trattamento dei dati.	Applicabile (se sì, barrare)
Registrazione tecnica dell'inserimento, della modifica e della cancellazione dei dati	☒
Nomi utente individuali, esclusione dei gruppi di utenti	☒
Assegnazione dei diritti di inserimento, modifica e cancellazione dei dati in base a un sistema di autorizzazione	☒
Definizione organizzativa delle responsabilità di inserimento	☒
Impegno alla segretezza dei dati	☒
Regolamentazione dei periodi di conservazione a fini di verifica/prova	☒

Misure per garantire la disponibilità e la resilienza

Controllo della disponibilità Studiato per proteggere i dati dalla distruzione o dalla perdita accidentali.	Applicabile (se sì, barrare)
Sistemi di allarme antincendio nelle sale server	☒
Rilevatori di fumo nelle sale server	☒
Porte antincendio	☒
Sistemi di spegnimento incendi senza acqua nelle sale server	☒
Protezione da fulmini/sovratensioni	☒
Climatizzazione delle sale server	☒
Stoccaggio dei sistemi di backup in locali separati e in un compartimento antincendio separato	☒
Le sale server non si trovano sotto o accanto ai servizi igienici	☒
Accesso alle sale server limitato al solo personale necessario	☒
Segnale di allarme in caso di accesso non autorizzato alle sale server	☒
Conservazione dei supporti di archiviazione nelle opportune condizioni di	☒

conservazione (climatizzazione, requisiti di protezione ecc.)	
Estintori a CO2 nelle immediate vicinanze delle sale server	☒
Sistema UPS (gruppo di continuità)	☒
Piano documentato di backup e protezione dei dati	☒
Esecuzione di backup dei dati e creazione di copie secondo il principio 3-2-1	☒
Archivio di emergenza (outsourcing dei dati)	☒
Test periodici per il recupero dei dati	☒
Almeno un sistema di backup non può essere crittografato da codice maligno	☒
Partizioni separate per sistema operativo e dati	☒
Piano di emergenza implementato (standard BSI 200-4)	☒
Assicurazione della leggibilità tecnica a lungo termine dei supporti di archiviazione backup.	☒

Resilienza (controllo della resilienza e dei malfunzionamenti) Consente ai sistemi di far fronte ai cambiamenti connessi ai rischi e di dimostrare tolleranza e capacità di compensazione in caso di interruzioni.	Applicabile (se sì, barrare)
Alimentazione ridondante	☒
Connessione dati ridondante	☒
Climatizzazione ridondante	☒
Disponibilità di data center di backup	☒
Computer Emergency Response Team (CERT)	☒
Esecuzione di test di penetrazione	☒
Attivazione immediata e regolare degli aggiornamenti software e firmware disponibili	☒
Controllo periodico della configurazione dei firewall	☒
Sensibilizzazione periodica dei dipendenti (almeno una volta all'anno)	☒
Il processo di segnalazione immediata degli incidenti all'IT è noto a tutti i dipendenti	☒
Stipula di una polizza di assicurazione informatica	☒

Misure per il riesame, la verifica e la valutazione periodici

Procedure di controllo Garantiscono l'efficacia delle misure per la sicurezza dei dati.	Applicabile (se sì, barrare)
Aggiornamento periodico dei registri delle attività di trattamento (art. 30, paragrafi 1 e 2, GDPR)	☒
Notifica delle procedure di trattamento dei dati nuove/modificate al responsabile della protezione dei dati	☒
Processi documentati per la segnalazione di procedure nuove/modificate	☒
Riesame periodico dei piani e della documentazione (ciclo PDCA)	☒
Riesame dell'efficacia delle misure di sicurezza con cadenza almeno annuale	☒
Esecuzione di test di sicurezza sulle applicazioni web secondo le procedure di buona pratica (ad es. OWASP Testing Guide)	☒
Qualora dal suddetto riesame emergano vulnerabilità, le misure di sicurezza vengono adeguate in funzione del rischio	☒
Processo di risposta alle violazioni della protezione (attacchi) e ai malfunzionamenti del sistema (gestione della risposta agli incidenti)	☒
Documentazione degli incidenti di sicurezza	☒

Controllo delle istruzioni Garantisce che i dati trattati dai fornitori di servizi (subappaltatori) siano trattati solo in conformità alle istruzioni del responsabile del trattamento.	Applicabile (se sì, barrare)
Elaborazione del contratto in conformità ai requisiti di legge (art. 28, GDPR)	☒
Controlli precontrattuali presso la sede dell'appaltatore prima dell'entrata in vigore del contratto	☒
Controlli periodici presso la sede dell'appaltatore dopo l'entrata in vigore del contratto (durante il periodo di validità del contratto)	☒
Riesame del piano di sicurezza dei dati dell'appaltatore	☒
Riesame dei certificati di sicurezza informatica validi dell'appaltatore	☒
Nomina di un responsabile della protezione dei dati da parte dell'appaltatore	☒

Controllo della separazione I dati raccolti per scopi diversi devono anche essere trattati separatamente.	Applicabile (se sì, barrare)
Separazione logica dei dati (ad es. in base agli identificativi dei clienti)	☒
Separazione dei sistemi di sviluppo, verifica e produzione	☒
Per i dati pseudonimizzati: Separazione dei file di assegnazione e archiviazione su un sistema diverso	☒

Altra gestione della protezione dei dati o della sicurezza	Applicabile (se sì, barrare)
Struttura organizzativa adeguata per la sicurezza delle informazioni con ruoli ben definiti	☒
Nomina di un responsabile della sicurezza informatica	☒
Utilizzo di un software per la gestione della protezione dei dati	☒
Nomina di un responsabile della protezione dei dati	☒
Processo documentato per la gestione degli incidenti di sicurezza informatica	☒
Processo documentato per la gestione degli incidenti relativi alla protezione dei dati	☒
Responsabilità chiare per la gestione degli incidenti relativi alla protezione dei dati e alla sicurezza	☒
Processo documentato per garantire i diritti degli interessati	☒
Archiviazione centrale di politiche/processi/istruzioni procedurali accessibili a tutti i dipendenti	☒
Linee guida/processi/istruzioni procedurali sono comunicati all'interno della società e conosciuti da tutti i dipendenti	☒
I fornitori di servizi esterni sono tenuti alla segretezza, se necessario	☒
Disposizioni per la cancellazione effettiva dei dati presenti sull'hardware ritirato dal produttore o dal fornitore di servizi	☒
Formazione periodica sulle linee guida e sui processi di sicurezza	☒

DocuSign

Certificate Of Completion

Envelope Id: 960EC2181A4C44C58E67161B6B284B16
Status: Completed
Subject: Complete with DocuSign: CPI0610-04_Template_CTA_Amendment_Constellation_SCC_site 3521_Final_30....
Source Envelope:
Document Pages: 60
Signatures: 4
Certificate Pages: 5
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Envelope Originator:
OPIS Medical Department
Via Matteotti, 10
Desio, MB 20832
medicaldep@opisresearch.com
IP Address: 93.145.18.18

Record Tracking

Status: Original
30-Jun-2023 | 12:30

Holder: OPIS Medical Department
medicaldep@opisresearch.com

Location: DocuSign

Signer Events	Signature	Timestamp
Regina Bönsch Regina.Boensch@morphosys.com CTL MorphoSys AG Security Level: Email, Account Authentication (Required)	Regina Bönsch Signature Adoption: Pre-selected Style Signature ID: 455EC936-3E64-446A-898A-7BDBF37AFF36 Using IP Address: 212.14.81.203 With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I approve this document I approve this document	Sent: 30-Jun-2023 | 12:32 Viewed: 03-Jul-2023 | 10:22 Signed: 03-Jul-2023 | 10:23
Electronic Record and Signature Disclosure: Accepted: 08-Aug-2022 | 11:52 ID: 346782ff-9e64-4727-82bd-4e38fac741ed		
Sanjaykumar Akhani Sanjaykumar.Akhani@morphosys.com Clinical Trial Lead MorphoSys AG Security Level: Email, Account Authentication (Required)	Sanjaykumar Akhani Signature Adoption: Pre-selected Style Signature ID: 7803F690-C79C-4412-B095-9D5FACA04BB5 Using IP Address: 212.14.81.203 With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I approve this document I approve this document	Sent: 30-Jun-2023 | 12:32 Viewed: 07-Jul-2023 | 18:16 Signed: 07-Jul-2023 | 18:17
Electronic Record and Signature Disclosure: Accepted: 04-Apr-2022 | 16:57 ID: 9e41b36f-ea50-496a-adb5-e091187a8ab2		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp
Carbon Copy Events	**Status**	**Timestamp**
Witness Events	**Signature**	**Timestamp**
Notary Events	**Signature**	**Timestamp**
Envelope Summary Events	**Status**	**Timestamps**
Envelope Sent	Hashed/Encrypted	30-Jun-2023 | 12:32
Certified Delivered	Security Checked	07-Jul-2023 | 18:16
Signing Complete	Security Checked	07-Jul-2023 | 18:17
Completed	Security Checked	07-Jul-2023 | 18:17
Payment Events	**Status**	**Timestamps**
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, OPIS s.r.l. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact OPIS s.r.l.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: dpo@opisresearch.com

To advise OPIS s.r.l. of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at info@opisresearch.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from OPIS s.r.l.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to info@opisresearch.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with OPIS s.r.l.

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to dpo@opisresearch.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify OPIS s.r.l. as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by OPIS s.r.l. during the course of your relationship with OPIS s.r.l..