Version 6

Reading Guide

If you (Greenlight Guru Clinical Customer) are considered a Processor for a Data Controller, such as in a separate data processing agreement with your own clients, when using Greenlight Guru Clinical services, we (Greenlight Guru Clinical) are considered a sub-processor in the following agreement.

If you (Greenlight Guru Clinical Customer) are considered a Data Controller, when using Greenlight Guru Clinical services, we (Greenlight Guru Clinical) are considered a Processor in the following agreement.

The following document consists of the following two appendices:

Appendix 1 concerns the data processing agreement between Greenlight Guru Clinical Customer acting as controller or processor and Greenlight Guru Clinical acting as processor or sub-processor.

Appendix 2 concerns the transfer agreement in situations where Greenlight Guru Clinical transfers personal data to a Greenlight Guru Clinical Customer established in a third country

Appendix 1 - Data Processor Agreement

SECTION I

Clause 1

Purpose & Scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The controllers and processors **or** processors and sub-processors (individually The Party and together The Parties) listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU)2016/679.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller/processor is subject by virtue of Regulation (EU) 2016/679.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2

Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

a) Where these Clauses use the terms 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 runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller/processor or a processor/sub-processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller/processor or a processor/sub-processor, in accordance with its designation in Annex I.

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

SECTION II OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller/processor, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

a) The processor/sub-processor shall process personal data only on documented instructions from the controller/processor, unless required to do so by Union or Member State law to which the processor/sub-processor is subject. In this case, the processor/sub-processor shall inform the controller/processor of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller/processor throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor/sub-processor shall immediately inform the controller/processor if, in the processor's/sub-processor's opinion, instructions given by the controller/processor infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor/sub-processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller/processor.

7.3. Duration of the processing of personal data

Processing by the processor/sub-processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

a) The processor/sub-processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor/sub-processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor/sub-processor shall ensure that persons authorised to process

the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 and offences ("sensitive data"), the processor/sub-processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor/sub-processor shall deal promptly and adequately with inquiries from the controller/processor about the processing of data in accordance with these Clauses.

c) The processor/sub-processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor/sub-processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors/sub-sub-processors

a) The processor/sub-processor has the controller's/processor's general authorisation for the engagement of sub-processors/sub-sub-processors from an agreed list. The processor/sub-processor shall specifically inform in writing the controller/processor of any intended changes of that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the controller/processor sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s) /sub-sub-processor(s). The processor/sub-processor shall provide the controller/processor with the information necessary to enable the controller/processor to exercise the right to object.

b) Where the processor/sub-processor engages a sub-processor/sub-sub-processor for carrying out specific processing activities (on behalf of the controller/processor), it shall do so by way of a contract which imposes on the sub-processor/sub-sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor/sub-processor in accordance with these Clauses. The processor/sub-processor shall ensure that the sub-processor/sub-sub-processor complies with the

obligations to which the processor/sub-processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

c) At the controller's/processor's request, the processor/sub-processor shall provide a copy of such a sub-processor/sub-sub-processor agreement and any subsequent amendments to the controller/processor. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor/sub-processor may redact the text of the agreement prior to sharing the copy.

d) The processor/sub-processor shall remain fully responsible to the controller/processor for the performance of the sub-processor's/sub-sub-processor's obligations in accordance with its contract with the processor/sub-processor. The processor/sub-processor shall notify the controller/processor of any failure by the sub-processor/sub-sub-processor to fulfil its contractual obligations.

e) The processor/sub-processor shall agree a third party beneficiary clause with the sub-processor/sub-sub-processor whereby - in the event the processor/sub-processor has factually disappeared, ceased to exist in law or has become insolvent - the controller/processor shall have the right to terminate the sub-processor/sub-sub-processor contract and to instruct the sub-processor/sub-sub-processor to erase or return the personal data.

7.8. International transfers

a) Any transfer of data to a third country or an international organisation by the processor/sub-processor shall be done only on the basis of documented instructions from the controller/processor or in order to fulfil a specific requirement under Union or Member State law to which the processor/sub-processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

b) The controller/processor agrees that where the processor/sub-processor engages a sub-processor/sub-sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller/processor) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor/sub-processor and the sub-processor/sub-sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Potential international transfers from the UK to third countries are covered by the standard contractual clauses supplemented with the provisions in Appendix II, Annex II.

In cases where the Parties act as processor and sub-processor respectively, cf. Annex I and the personal data covered by this agreement is transferred from a processor established in a third country to a sub-processor established in the EU, the processor ensures that the controller has approved the use of the Standard Contractual Clauses in Appendix 2 as basis for the transfer of personal data to the EU.

Clause 8

Assistance to the controller/processor

a) The processor/sub-processor shall promptly notify the controller/processor of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller/processor.

b) The processor/sub-processor shall assist the controller/processor in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor/sub-processor shall comply with the controller's/processor's instructions.

c) In addition to the processors/sub-processors obligation to assist the controller/processor pursuant to Clause 8(b), the processor/sub-processor shall furthermore assist the controller/processor in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor/sub-processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller/processor to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller/processor without delay if the processor/sub-processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor/sub-processor is required to assist the controller/processor in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor/sub-processor shall cooperate with and assist the controller/processor for the controller/processor to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor/sub-processor.

9.1 Data breach concerning data processed by the controller /processor

In the event of a personal data breach concerning data processed by the controller/processor, the processor/sub-processor shall assist the controller/processor:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller/processor has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's/processor's notification, and must at least include:

1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed to be taken by the controller/processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor/sub-processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller/processor without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
The Parties shall set out in Annex III all other elements to be provided by the processor/sub-processor when assisting the controller/processor in the compliance with the controller's/processor's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor/sub-processor is in breach of its obligations under these Clauses, the controller/processor may instruct the processor/sub-processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor/sub-processor shall promptly inform the controller/processor in case it is unable to comply with these Clauses, for whatever reason.

b) The controller/processor shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1) the processing of personal data by the processor/sub-processor has been suspended by the controller/processor pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

2) the processor/sub-processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

3) the processor/sub-processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

c) The processor/sub-processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller/processor that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller/processor insists on compliance with the instructions.

d) Following termination of the contract, the processor/sub-processor shall, at the choice of the controller/processor, delete all personal data processed on behalf of the controller/processor and certify to the controller/processor that it has done so, or, return all the personal data to the controller/processor and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor/sub-processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s)/processor(s):

Name: You (the Greenlight Guru Clinical Customer)

Address: The address of your organization (the Greenlight Guru Clinical Customer)

Contact person: the controller/processor is responsible for providing the processor/sub-processor with information on the controller/processor contact person.

Signature and accession date: These Clauses are an integral part of Greenlight Guru Clinical's Online Service Terms & Conditions. As such, the parties agree that their conclusion of the Online Service Terms & Conditions agreement shall constitute the conclusion of these Clauses as well.

Processor(s)/sub-processor(s)

Name: SMART-TRIAL ApS
Address: K. Christensens Vej 2L, 9200 Aalborg SV, Denmark
Contact person: privacy@greenlight.guru

Signature and accession date: These Clauses are an integral part of Greenlight Guru Clinical's Online Service Terms & Conditions. As such, the parties agree that their conclusion of the Online Service Terms & Conditions agreement shall constitute the conclusion of these Clauses as well.

ANNEX II

Description of the processing

Greenlight Guru Clinical Services

The scope of the processing depends on the data controller's/processor's configuration of the Greenlight Guru Clinical services. This Annex II describes the processing related to the standard configuration.

Categories of data subjects whose personal data is processed

- Greenlight Guru Clinical users
- Controller's/processor's customers, clients, subjects and/or patients

Categories of personal data processed

Personal data regarding Greenlight Guru Clinical users:

- Name
- Email address
- Phone number and country code
- IP address
- Initials
- Staff ID
- Organization name
- Department
- Timestamps for user login (date and time)
- All interactions with Greenlight Guru Clinical and on the processor's/sub-processor's servers, including e.g. searches, clicks on links, prints, copying etc.

Personal data regarding controller's/processor's customers, clients, subjects and/or patients:

- Name
- Email address
- Phone number and country code
- IP address
- Initials

- Subject ID
- Date of birth
- Gender
- Address
- Clinical/healthcare data such as physiological variables and laboratory results. A high security level has been established as default. Please refer to our Security and Service Level Statement for further information.

Nature of the processing

Storage and management of clinical data.

Purpose(s) for which the personal data is processed on behalf of the controller/processor

Management of clinical data.

Duration of the processing

The processing shall continue for the duration of the parties' agreement regarding the processor's/sub-processor's services which include processing of personal data.

ANNEX III

Technical and organisational measures to ensure the security of the data

Description of the technical and organisational measures implemented by the processor(s) /sub-processor(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.

A high security level has been established as default. Please refer to our Security and Service Level Statement for information on our technical security measures.

Except the transfers to sub-processors/sub-sub-processors listed in Annex IV below and transfers from controllers/processors in third countries to Greenlight Guru Clinical as processor/sub-processor (Clause 7.8 and Annex 2) Greenlight Guru Clinical stores all personal data covered by this agreement in the EU. Consequently, the personal data is not transferred to or accessed from Greenlight Guru (Soladoc LLC) as parent company to Greenlight Guru Clinical.

For the sake of good order, Greenlight Guru will reject all requests from public authorities in third countries without jurisdiction in Denmark regarding access to personal data – also originating from our parent company.

ANNEX IV

List of sub-processors/sub-sub-processors

The controller/processor authorised sub-processors/sub-sub processors list can be found on Greenlight Guru's Trust Center.

Appendix 2 - International Data Transfers (Standard Contractual Clauses)

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 ProtectionRegulation) 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: 'Transfer Clauses').

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

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

Clause 2

Effect and invariability of the Transfer Clauses

a) These Transfer 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 Transfer Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Transfer Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Transfer 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 Transfer Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b) These Transfer Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c) These Transfer 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 Transfer Clauses and the provisions of related agreements between the Parties, existing at the time these Transfer Clauses are agreed or entered into thereafter, these Transfer 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

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

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

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

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 Transfer Clauses.

8.1 Instructions

a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data , the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data

processed by the data exporter under these Transfer Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

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

8.3 Documentation and compliance
a) The Parties shall be able to demonstrate compliance with these Transfer Clauses.

b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Transfer Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

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 Transfer 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 Transfer 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 Transfer 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

N/A

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

Clause 14

Local laws and practices affecting compliance with the Transfer 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 Transfer 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 Transfer 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 ;
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Transfer 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 Transfer 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 Transfer Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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 Transfer 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 controller or 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 Transfer 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 Transfer 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 Transfer 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 Transfer 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 Transfer Clauses and termination

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

b) In the event that the data importer is in breach of these Transfer Clauses or unable to comply with these Transfer 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 Transfer 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 Transfer 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 Transfer 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 Transfer Clauses. In these cases, it shall inform the competent supervisory authority of such noncompliance. 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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.

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 Transfer 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 Transfer 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 Transfer 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 Transfer 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 Transfer Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

ANNEX I of Appendix II

A. LIST OF PARTIES

Data exporter(s):
Name: SMART-TRIAL ApS
Address: K. Christensens Vej 2L, 9200 Aalborg SV, Denmark
Contact person: privacy@greenlight.guru
Role (controller/processor): Processor

Activities relevant to the data transferred under these Transfer Clauses: SMART TRIAL services

Signature and date: These Transfer Clauses are an integral part of Greenlight Guru Clinical's Online Service Terms & Conditions. As such, the parties agree that their conclusion of the Online Service Terms & Conditions agreement shall constitute the conclusion of these Transfer Clauses as well.

Data importer(s):
Name: You (the Greenlight Guru Clinical Customer)
Address: The address of your organization (the Greenlight Guru Clinical Customer)
Contact person: the controller is responsible for providing the Processor with information on the controller's contact person
Role (controller/processor): Controller

Activities relevant to the data transferred under these Transfer Clauses: SMART TRIAL services

Signature and date: These Transfer Clauses are an integral part of Greenlight Guru Clinical's Online Service Terms & Conditions. As such, the parties agree that their conclusion of the Online Service Terms & Conditions agreement shall constitute the conclusion of these Transfer Clauses as well.

B. DESCRIPTION OF TRANSFER

1. Greenlight Guru Clinical Services
The scope of the transfer depends on the data importer's configuration of the Greenlight Guru Clinical services. This annex II describes the transfer related to the standard configuration.

Categories of data subjects whose personal data is processed

- Greenlight Guru Clinical users
- Controller's customers, clients, subjects and/or patients

Categories of personal data transferred

Personal data regarding Greenlight Guru Clinical users:

- Name
- Email address
- Phone number and country code
- IP address
- Initials
- Staff ID
- Organization name
- Department
- Timestamps for user login (date and time)
- All interactions with Greenlight Guru Clinical and on the processor's servers, including e.g. searches, clicks on links, prints, copying etc.

Personal data regarding controller's customers, clients, subjects and/or patients:

- Name
- Email address
- Phone number and country code
- IP address
- Initials
- Subject ID
- Date of birth
- Gender
- Address
- Clinical/healthcare data such as physiological variables and laboratory results.
  Safeguards: A high security level has been established as default. Please refer to our Security and Service Level Statement for further information.

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

Nature of the processing:
Storage and management of clinical data.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
The processing shall continue for the duration of the parties' agreement regarding the processor's services which include processing of personal data.

C. COMPETENT SUPERVISORY AUTHORITY

N/A

ANNEX II of Appendix II

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES, FOR PERSONAL DATA TRANSFERRED FROM THE UNITED KINGDOM.

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	**The start of this Addendum is hereby, effective upon the commencement of any transfer of Personal Data to countries outside the United Kingdom as set forth in clause 3(b) of the DPA.**
Parties' details	The Parties to this Addendum are the same as specified in the agreement to which this Addendum is attached.
Key Contact	The key contact persons for this Addendum are the same as specified in the agreement to which this Addendum is attached.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	This Addendum applies to the version of the Approved EU SCCs (including the Appendix Information) specified and included in the agreement to which this

	Addendum is attached

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties). That information is included in the agreement to which this Addendum is attached.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: - Importer - Exporter

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 17 of those Mandatory Clauses.

Do you need a signed copy?

Contact us via legal@greenlight.guru and request your copy via pdf.

Older versions

Version 5 From August 18, 2022
Version 4 From March 4, 2022
Version 3 From August 25, 2021
Version 2 From June 23, 2021
Version 1 From February 24, 2021