**JOINT CONTROLLER AGREEMENT  
\_\_\_\_\_\_\_\_\_\_**

This Joint Controller Data Processing Agreement (the “**JCA**”) has been entered into by

1. **KAROLINSKA INSTITUTET**, Department of Global Public Health, org.nr 202100-2973, with registered address at SE-171 77 Stockholm, Sweden, (“**KI**”); and
2. **The George Institute for Global health** [please insert full address. TGI has several branches. We need to identify the legal entity that will sign this agreement], [address], (“**TGI**”),

hereinafter jointly referred to as “**Parties**” and separately as “**Party**”.

**WHEREAS**

1. The Parties are currently engaged in a collaboration within the study entitled “Effects of Advanced Trauma Life Support® Training Compared to Standard Care on Adult Trauma Patient Outcomes: A Cluster Randomised Trial” and have entered into a research collaboration agreement (the “**Collaboration Agreement**”) which further describes the research to be conducted by the Parties (the “**Research**) in a research plan (“the “**Research Plan**”) and specifies the rights and obligations of each Party concerning inter alia intellectual property rights.
2. TGI will collect certain study data in India and is willing to use such data (the “Dataset”) for the purpose of conducting the Research with KI. In performing the Research, both Parties will process personal data for the purposes and with means that they have decided on jointly, subject to the terms and conditions of the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller to Controller Transfers) pursuant to Regulation (EU) 2016/679 (also referred to as “**GDPR**”), hereinafter referred to as the “**SCC**”, included in the Addendum, which constitute an integral part of this JCA.
3. Annex B of the SCC describes the data being transferred (“**the Personal Data**”) as well as the purpose for the transfer (“**the Research**”).

**IT IS AGREED** as follows:

1. SCOPE and purpose

The JCA including its Addendum is an additional agreement to the Collaboration Agreement, fully executed by the Parties on [insert date], which further details the Research and, which together with this JCA, determine the purpose of the processing of personal data (the “**Purpose**”).

The personal data in the Dataset will be collected by TGI under a protocol approved by relevant Ethical Review Boards in accordance with local laws, under the supervision of [insert name] as principal investigator.

The personal data in the Dataset will be processed by KI under a protocol that has been approved by [the Swedish Ethical Review Board in xxx insert dr.nr.] with [insert name] as principal investigator.

The Parties agree that they together determine the purposes and the means of the processing with regards to the Research described in the Collaboration Agreement and the Parties therefore agree that they are both **joint controllers**.

The JCA including the Addendum governs the Parties’ processing of Personal Data in connection with the conduct of the Research under the Collaboration Agreement.

This JCA duly reflects the respective roles and responsibilities of the Parties as joint controllers towards the data subjects in accordance with Article 26 of the GDPR and ensures that data subjects can exercise their rights in relation to the Parties’ processing of Personal Data.

For the sake of clarity, the joint controllership does not extend to any processing undertaken by either Party outside the scope of the Collaboration Agreement. It also excludes the Personal Data pertaining to each joint controllers’respective employees exchanged between the Parties for the administrative management of this contractual relationship and for which each Party remains an independent controller. This JCA only applies to the processing activities specific to the Personal Data analysis which are performed jointly by the Parties as part of the Research and for which KI acts as the “Data Exporter” giving access to the Personal Data through KI’s server to TGI who acts as “Data Importer”.

The Parties agree that in relation to the processing of personal data, this JCA shall take priority over any other agreement between the Parties.

To ensure appropriate safeguards for the transfer, the SCC in the **Addendum**, constitute an integral part of this JCA and **must be executed by the Parties**.

This JCA does not intend to amend or modify any clauses of the SCC as they, according to Clause 2 (a) of the SCC, may not be modified, except to add or update information in the Appendix. In case any provision of this JCA is in conflict with any provision of the SCC, the provision of the latter shall prevail.

Where this JCA uses terms that are defined in in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

1. COMPLIANCE WITH APPLICABLE LAWS

Each Party shall comply with all applicable provisions of EU and Member State privacy and data protection laws and regulations, as amended from time to time, to which the Party is subject with respect to the performance of its obligations under this JCA.

Each Party shall bear sole responsibility for ensuring that its processing of Personal Data within the Research Project complies with all laws and regulations on data protection applicable to that Party.

The Parties agree that their respective responsibilities for compliance with the obligations under the GDPR shall be allocated in accordance with the provisions of this JCA.

1. Obligations of the parties

The Party collecting Personal Data directly from data subjects (“TGI”) is a controller of the Personal Data. TGI shall be solely responsible for ensuring that Personal Data is collected for specific, explicit and legitimate purposes, which are described in the Research Plan (hereinafter the “Purpose”).

TGI further undertakes to ensure that only Personal Data that may be processed for the Purpose is stored in REDCap.

The Parties shall ensure that the processing of the Personal Data by the Parties is in accordance with GDPR Article 6 (processing is necessary for the performance of a task carried out in the public interest) and/or Article 9, (processing is necessary for conducting scientific research and statistical analysis).as applicable i.e. that there is a legal basis for the processing of Personal Data.

The Parties shall only process the Personal Data for the specific Purpose.

When Parties process the Personal Data under this JCA, Parties are joint controllers of Personal Data. As joint controllers of Personal Data, Parties agree to meet all the obligations of a joint controller as specified in the GDPR and all other mandatory laws and regulations on data protection applicable to that Party.

1. ACCESS TO PERSONAL DATA – METHOD OF TRANSFER

Data will be collected by TGI through Clinical Research Coordinators at each Study Site. Initial data collection will be done using a paper based Case Record Form (CRF), which is then transferred to an electronic CRF (eCRF) using REDCap hosted on TGI servers.

Any Personal Data shall be pseudonymized (as that term is defined under GDPR) by TGI so that KI cannot attribute the Personal Data to a specific data subject without the use of a link that is retained separately by TGI i.e. in a coded and encrypted format which protects data subject identities. The key code will be kept separately by TGI, subject to technical and organizational measures.

KI shall store the Personal Data and make it accessible to TGI by means of access to a KI server over a Virtual Private Network (VPN) with multi-factor authentication (MFA) based on an affiliation agreement of the TGI investigator.

1. PERSONAL DATA PROTECTION – RECIPIENT OBLIGATIONS

TGI shall securely safeguard, encrypt and appropriately protect the Personal Data from unauthorized access, use and theft. TGI shall comply with any reasonable instructions from KI**.**

TGI agrees not to use the Personal Data to identify the data subjects nor to contact them under any circumstances. TGI shall refrain from analyzing and/or using Personal Data in a way that has the potential to (i) lead to the re-identification of any data subject, (ii) compromise the anonymity of any data subject in any way, or (iii) where the legal basis for the processing is consent, result in use of Personal Data outside the strict scope of any data subject’s consent.

Any audit or review under the JCA will be subject to conditions that the TGI (Data Importer) reasonably requests to protect the confidentiality of its data files, documentation and/or other information of a confidential or proprietary nature.

1. intellectual property

Any rights and title to any intellectual property generated under the Research Plan will be subject to the terms agreed by the Parties in the Collaboration Agreement.

1. PUBLICATION

All publications shall be made in accordance with the terms agreed by the Parties in the Collaboration Agreement.

1. SUBCONTRACTORS

TGI may not transfer any Personal Data to any third party under this JCA unless specifically designated in the Research Plan or approved in writing by KI in each case. If a third party or subcontractor has been designated in the attached Research Plan and/or if KI has approved in writing the transfer of Personal Data to a third party or subcontractor, TGI undertakes to ensure that the terms of the JCA are extended to any such third party or subcontractor prior to any such transfer. TGI will, however, remain responsible for any third party or subcontractor’s compliance with the provisions of the JCA, the GDPR and all other laws and regulations on data protection applicable to TGI.

1. RIGHTS OF DATA SUBJECTS

The Parties are Joint Controllers of Personal Data under the GDPR and as such, both Parties are responsible for compliance with the GDPR with regard to the exercise of Data Subjects’ rights.

On request of a data subject, the Parties are obliged to provide information about the processing of the data subject’s Personal Data or to correct, provide access to, restrict or erase Personal Data regarding that data subject pursuant to the request and in compliance with the GDPR. The Parties will maintain appropriate technical and organizational measures needed to enable them to respond to requests from data subjects exercising the Data Subjects’ rights in Chapter III of the GDPR with respect to any relevant Personal Data held by the Parties (“Request”). The Parties will cooperate to the extent reasonably necessary in connection with a Request.

The Parties undertake to take appropriate technical and organizational measures in respect of Personal Data, including (but not limited to) to (i) restrict processing of, erase or anonymize Personal Data, (ii) provide information about the processing activities, (iii) facilitate the data subjects’ access to Personal Data, (iv) rectify incorrect Personal Data, and (v) provide Personal Data in a structured, commonly used and machine-readable format.

A Party receiving a request will promptly inform the other Party if it is unable to fulfill the Request. The Parties will work in good faith to resolve the Request within the deadlines specified by the GDPR and to determine whether there exist any derogations to a data subject’s right set forth in Chapter III of the GDPR. The Parties acknowledge that the Party who has collected the Personal Data from the data subjects is best placed to manage the contacts with the data subjects. TGI therefore undertakes to, when possible, inform the data subjects of the processing activities and to provide data subjects with all other relevant information regarding the processing of Personal Data under this JCC, as required by the GDPR.

Where processing of a Data Subject’s Personal Data is based on consent, at the point of obtaining consent, TGI will provide data subjects access to information that identifies the joint controllers and includes a description of the Parties’ respective roles with respect to the processing of Personal Data. TGI shall further make the essence of this JCA available to the relevant data subjects.

1. BREACH NOTIFICATION

TGI is under a strict obligation to notify KI of any potential or actual Personal Data breaches without undue delay. If TGI becomes aware of any unauthorized access to or use or disclosure of Personal Data, it will promptly notify KI. The TGI will promptly provide KI such other information as KI may reasonably request, including, but not limited to documentation of its investigation.

Unless otherwise agreed, KI shall, regardless of which Party is responsible for the Personal Data breach, be responsible for submitting the notifications required by the GDPR to the supervisory authority, provided that the TGI is given the opportunity to review any breach notification that mentions the TGI, under the specified time limit for such notification. If the TGI is responsible for the Personal Data breach, it shall compensate KI for any costs related to the notification procedure. To the extent the Parties are jointly responsible for a Personal Data breach, the Parties agree to work collaboratively to determine the manner of such notification and an equitable apportionment of notification costs, taking into account any proportion of fault and/or breach of the Parties.

The Parties agree that when a Personal Data breach is noted and any of the Parties have become aware of it, the Personal Data breach shall, without undue delay and, where feasible, not later than seventy-two (72) hours be reported by KI to the supervisory authority competent in accordance with Articles 33 and 55 of the GDPR, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. For KI to be able to meet such deadline, the TGI, when responsible for the Personal Data breach or otherwise when the TGI have become aware of such breach, shall notify the KI within forty-eight (48) hours. Where the notification to the supervisory authority is not made within seventy-two (72) hours, it shall be accompanied by reasons for the delay.

Notifications of Personal Data breaches to the supervisory authority shall at least include the information as described in Article 33 of the GDPR, and notifications of Personal Data breaches to affected Data Subjects shall at least include the information as described in Article 34 of the GDPR.

1. COOPERATION OBLIGATION

Upon a request issued by a supervisory authority to either Party for records regarding Personal Data, the Party receiving the request will respond to the supervisory authority and the other Party will cooperate and provide the responding Party with records related to processing activities performed, including information on the categories of Personal Data processed and the purposes of the processing, the use of processors with respect to such processing, any disclosures of Personal Data to third parties, transfers of Personal Data to third countries and documentation on suitable safeguards to protect such Personal Data, and a general description of technical and organizational measures to protect the security of Personal Data.

1. TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

To the extent that the processing of Personal Data under this JCA including its Addendum involves a transfer of Personal Data originating from either Party’s systems in the EU/EEA to either Party’s systems located in countries outside the EU/EEA that have not received a binding adequacy decision by the Commission, such transfers are subject to applicable data transfer mechanisms in the GDPR and the prior written approval of KI. The Parties agree that with respect to transfers of Personal Data in compliance with GDPR the JCA and the SCC in the Addendum shall serve as the applicable data transfer mechanism.

1. RETENTION OF PERSONAL DATA

Personal Data received by TGI in connection with this JCA including its Addendum will be retained only for so long as may be reasonably required in connection with the Parties’ performance of the Research described in the Research Plan.

1. SURVIVAL

The JCA will be effective on the date of its last signature date by the Parties.

TGI’s obligation to protect the Personal Data is continuous and survives any termination, cancellation, expiration, or other conclusion of the JCA including its Addendum and of the Collaboration Agreement.

1. AMENDMENTS

No provision of this JCA may be amended, modified or otherwise changed, other than by an instrument in writing duly executed on behalf of the Parties.

The Parties acknowledge and agree that to the extent required, this JCA shall be amended to achieve compliance with future changes to data protection laws.

1. Authorized users

The Personal Data transferred may be disclosed to the following personnel or categories of personnel:

Investigators and research staff involved with the project at TGI

Researchers and research staff involved with the project at KI

1. **LIABILITY**

In no event shall KI be liable to TGI for any loss, claim, damage or liability which may arise from the use, handling or storage of the Data by TGI. TGI shall indemnify and hold harmless KI and any of its employees from and against any loss, claim, damage or liability arising out of the performance of this JCA including its Addendum, but only in proportion to and to the extent such loss, claim, damage or liability are caused by or result from the negligent or intentional acts or omissions of TGI.

1. **APPLICABLE LAW AND DISPUTES**

This JCA shall be governed by the laws of Sweden and any dispute arising out of or in connection with this JCA, which cannot be solved amicably, shall be settled by the courts of Sweden with the District Court of Stockholm as the court of first instance.

20 Signatures

This JCA has been drawn up in two (2) originals of which the Parties have taken one (1) each.

|  |  |
| --- | --- |
| **KAROLINSKA INSTITUTET** | **THE GEORGE INSTITUTE OF GLOBAL HEALTH** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | |  | | Name | | | Head of Department of …. | | | Date: | | | |  | | --- | |  | | xxx | | |  | | | Date: | | |

|  |
| --- |
| Read and approved |
| Name | |
| Principal Investigator | |
| Date: | |

**ADDENDUM TO JOINT CONTROLLER AGREEMENT**

### **STANDARD CONTRACTUAL CLAUSES**

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]](#endnote-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.

**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 8.5 (e) and Clause 8.9(b);

(iii) N/A

(iv) Clause 12(a) and (d);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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**

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

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

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

**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]](#endnote-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.

(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]](#endnote-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 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]](#endnote-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.

(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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([[5]](#endnote-5)) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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**

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

(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 ([[6]](#endnote-6));

(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 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 Sweden**.

**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 Sweden**.

(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**

**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: KAROLINSKA INSTITUTET

Address: 171 77 Stockholm, Sweden

**Contact person’s name, position and contact details:**

Insert name of PI

Principal Investigator, Department of…

Insert contact details

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data Protection Officer

Name: Mats Gustavsson

Address: Legal Office, Nobels väg 6, 1717 77 Stockholm, Sweden

E-mail: dataskyddsombud@ki.se

**Activities relevant to the data transferred under these Clauses:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature and date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role (controller): Head of Department of ….

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

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Contact person’s name, position and contact details**:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Activities relevant to the data transferred under these Clauses:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature and date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role (controller):

**ANNEX I. B**

**DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

insert

*Categories of personal data transferred*

insert

*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.*

insert

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

insert

*Nature of the processing*

insert

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

insert

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

insert

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

insert

**ANNEX I. C.**

**COMPETENT SUPERVISORY AUTHORITY**

*The competent supervisory authority/ies in Sweden in accordance with Clause 13 is*

**The Swedish Authority for Privacy Protection** (sw. Integritesskyddsmyndigheten)

Org. no: 202100-0050

Address: Box 8114, 104 20 Stockholm, Sweden

E-mail: [imy@imy.se](mailto:imy@imy.se)

Phone no: +46 (0) 8 657 61 00

Website: <https://www.imy-se>

**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.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also* *describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 8.5:

The data exporter understands and agrees that these measures are subject to technical progress and development and the data importer is therefore expressly allowed to implement alternative measures provided that they maintain or exceed the general security level described below.

1. Any computer equipment and portable storage media that is not supervised must be securely locked up in order to protect against unauthorized access, manipulation and theft. Premises containing such equipment shall always be protected with such physical security measures deemed necessary to ensure that only authorized personnel is granted access.
2. Personal data shall regularly be backed up. Backup copies shall be kept separate and protected as to allow restoration in case of a disruption. The data importer shall implement routine testing of readback capability.
3. Access to personal data shall be controlled with a technical solution for authentication. Authorization shall be limited to only those in need of the data for their work. User identity and passwords shall be personal and may not be transferred to someone else. The data importer shall implement routines for the granting and revoking of rights.
4. Access to personal data shall be traceable through the use of logs or similar solutions that allows the data importer to verify access and report back to the data exporter.
5. Any external connection for communication of data must be protected by a technical solution that ensures that the connection is authorized.
6. Access to sensitive personal data (special categories) shall require two-factor authentication.
7. The transfer of personal data by technical means outside of the data importer’s control and supervision shall employ encryption.
8. Systems and components shall carry active security measures configured in such a way that they provide adequate levels of protection for the personal data.
9. Whenever mounted or portable storage media containing personal data are taken out of use, all personal data shall be deleted in such a way that it cannot be recovered. This may necessitate the destruction of hardware.
10. Written agreements ensuring security and confidentiality must be executed between the data importer and any third party carrying out repairs or service of equipment used for the storage of personal data.
11. On-site visits by third parties for repairs and service must be supervised by the data importer. If that is not possible, any storage media containing personal data must be removed prior to any such visit.
12. Service by remote communication is only allowed provided it can be done through a secure connection and a reliable electronic identification of the person performing the service. Access shall only be given for the time required to perform the service. Any separate access way for service shall be closed whenever service is not actively being performed.
13. The data exporter, or any third party hired by the data exporter for the purpose, has a right to investigate unauthorized access at the data importer.

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](https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2018:295:TOC)), 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. [↑](#endnote-ref-1)
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. [↑](#endnote-ref-2)
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. [↑](#endnote-ref-3)
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. [↑](#endnote-ref-4)
5. The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards. [↑](#endnote-ref-5)
6. 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. [↑](#endnote-ref-6)