DATA PROTECTION ADDENDUM

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 Protection Regulation) 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

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

(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

(Intentionally left blank)

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 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "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 purpose(s) of processing and the risks involved in the processing for the data subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data

importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(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 that the related underlying main agreement is subject to and if applicable law of the related underlying main agreement is not the law of an EU Member State, German law shall apply.

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 that are competent to resolve a dispute that arises based on or in connection with the related underlying main agreement. If such court is not a court of a Member State, German courts will resolve.

(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

ANNEX I

A. LIST OF PARTIES

If an agreed final version of this DPA is incorporated as an Exhibit at the time the underlying main agreement is signed by the parties, the DPA is deemed to be signed and a separate signature below is not required. This data processing agreement replaces any previous agreement on the subject matter. The underlying main agreement means the [Icertis SaaS Subscription Agreement and Services Agreement] to which the document is an Exhibit.

Data exporter(s):

Name: as set out in the underlying main agreement

Address: as set out in the underlying main agreement

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

Activities relevant to the data transferred under these Clauses: as set out in the underlying main agreement

Data Exporter acts as a Controller according to Art. 4(7) GDPR with respect to the personal data of its own Authorized Users and (if applicable) on behalf of and in the name of Affiliates acting as data controllers of Authorized Users under the terms of the underlying main agreement from time to time.

Signature on behalf of Data Exporter and its Affiliates (if applicable) that from time-to-time use the Icertis Contract Intelligence solution (ICI) under the terms of the underlying main agreement.

Date: [include]

Name: [include]

Function: [include]

_____

Signature

Role (controller/processor): Controller

Data importer(s):

Name: Icertis Inc.

Address: 14711 NE 29th Place, Suite 100 Bellevue WA 98007 USA

Contact person's name, position and contact details: Global Data Protection Officer, GlobalDPA@icertis.com Tel. +91 20 6608 8400; representative in the European Union: Icertis GmbH, Taunusanlage 1 in 60329 Frankfurt, Germany, DSB@icertis.com

Activities relevant to the data transferred under these Clauses: as set out in the underlying main agreement.

Signature on behalf of Icertis Inc. and date:

Date: [include]

Name: [include]

Function: [include]

_____
Signature

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

Employees of Data Exporter and its clients, business partners (e.g. supplier, vendor) and any other category of Data Subjects that the Data Exporter may process from time to time as part of the Service.

2. Categories of personal data transferred

(*1) Categories of data*: Name, sex, job function, email address, User Data (i.e. user ID, user logs, ICI system user activities and user product support ticket data) and any other categories of data contained in documents uploaded by or on behalf of the Exporter to the Importers contract intelligence solution. "ICI" means the Icertis Contract Intelligence SaaS Solution.

(2) 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.

☐ Racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Genetic data

☐ Biometric data

☐ Data concerning health

☐ Data concerning a natural person's sex life or sexual orientation

☐ Other: [include]

If none of the above boxes are marked, no sensitive data will be processed.

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

Continuous basis.

4. Nature of the processing

(1) As part of implementing (where applicable), operating (hosting, backing up data), maintaining and supporting (including Processing log files) the Services, Data Importer will process Personal Data contained in documents managed by the Services.

Data Importer will not request Data Exporter to send and herby request Data Exporter to refrain from sending (e.g. via email, teams or alike) to Data Importer or any of its subprocessor any files (documents uploaded to ICI that include personal data) for the purpose of providing the Services.

(2) Data Importer will aggregate User Data to generate an internal management dashboard. For this, a computer program of Data Importer will access User Data filed in ICI and in the support application. Data Importer will not transfer User Data to the Dashboard. To aggregate User Data for the Dashboard, the user ID of the Authorised User will be processed in a Microsoft Azure data centre of Icertis located in the European Union.

(3) As an unintended consequence of the Icertis computer algorithm "reading" content / documents Data Exporter has uploaded to ICI, Data Importer processes Personal Data contained therein. Data Importer will ignore such personal data and will never share it with third parties.

5. Purpose(s) of the data transfer and further processing

Implementation (if and to the applicable) including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services; product support including troubleshooting (preventing, detecting, repairing, investigating, mitigating, and repairing problems, including Security Incidents); (Management Dashboard) use of ICI which includes delivering functional capabilities based on aggregated data as licensed, configured, and used by Subscriber and its Authorised Users; keeping the ICI solution up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.

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

Duration of the related underlying main agreement.

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

See **Annex III**

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority is located in the following EEA:

[include name of the Member State of the EEA*]

The name, the address and the contact details of the supervisory authority located in the Member State of the EEA mentioned above can be identified by referring to the following website:

https://edpb.europa.eu/about-edpb/about-edpb/members_en

***Note to data exporter when located outside the EEA**: If the data exporter has appointed a representative: the authority in the EEA of the representative. If no representative is appointed: The supervisory authority of one of the EEA in which the data subjects whose personal data is transferred.*

** The competent supervisory authority for Germany and Belgium is split amongst different supervisory authorities in the respective country. You can identify the competent supervisory authorities by referring to the link to the website mentioned above. Please include the name of the so identified supervisory authority after the Member State name (Germany or Belgium) into the field highlighted in yellow above.*

EEA includes all member states of the European Union as well as Iceland, Liechtenstein and Norway.

The name and the details of the supervisory authority for the United Kingdom and Switzerland are mentioned in the relevant Annex below. In this case, you can leave the field highlighted in yellow above as is.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A. Icertis Technical and Organizational Measures (including Microsoft Azure)

To ensure an appropriate level of data security, Icertis has implemented the following technical and organizational measures (TOM) to protect Personal Data. The TOM include the Icertis Contract Intelligence (ICI) Platform that is hosted on the Microsoft Azure cloud which provides certain technical and organisational measures specified herein.

Accordingly, security of processing is achieved through Microsoft Azure and Icertis security measures.

1. Organizational controls

1.1. Policies

- Internal regulations are in place on the operation and procedures of data processing as well as on the various data security measures.

1.2. Personnel

- To keep personal data confidential, all Icertis employees are subject to confidentiality obligations signed before onboarding (see also point 1.5 below).
- Icertis has appointed a Global Data Protection Officer (DPO) and Chief Information Security Officer (CISO). The Information Security Management systems and the Data Protection Systems are integrated to provide the DPO with a robust clarity into the relevant operational systems and performance. The CISO is also responsible for the approval of policies and procedures after the review by the respective department heads, which is conducted annually.
- Microsoft has appointed a European Union Data Protection Officer (DPO). The DPO advises Microsoft's engineering and business groups.

1.3. Contracts

- Icertis transfers personal data based on the European Commission standard contractual clauses for international transfers to which this document is incorporated.
- Microsoft facilitates the transfer of personal data outside of the EU on basis of the Standard Contractual Clauses (SCC) that are incorporated into the Online data protection addendum terms and conditions https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
- Microsoft complies with the EU Cloud Code of Conduct: https://eucoc.cloud/en/public-register/list-of-adherent-services.html

1.4. Training

- Information Security and Data Privacy training is mandatory for all Icertis employees. All employees need to undergo regular training. New Joiners have to finish their training within a specified timeframe of joining.
- Product training is provided to all the Icertis employee depending upon the job role requirement. There are various training and certification-based program take place based upon the nominations and requirement for a role.

1.5. Employee Onboarding and Offboarding

- Before onboarding the employees, thorough background verification is performed.
- To keep personal data confidential, all Icertis employees are subject to confidentiality obligations signed before onboarding.
- Access rights are granted on an individual basis according to the need-to-know principle. Requested changes to permissions will only be made in accordance with existing security policies.
- After the initiation of the offboarding process, all the access granted to the employees are revoked, on the last actual working day of the employee.
- Icertis' IT collects all the devices provided and informs the HR of the same.

1.6. Internal and External Audit

- Icertis' internal audit is conducted once every 6 months and external audits are conducted annually. The audits are conducted by external parties and supported by CISO and the Compliance Manager and the compliance team. The departments covered are Top Management, CISO, Cloud Operations, IT, Human Resources, Admin, Production and Engineering, Delivery Team and Customer Success Team.

Microsoft Azure:

- Microsoft fulfils several international and national security standards. Internal and external audits are conducted regularly by internal and third-party auditors. Information on Azure compliance can be found here: https://servicetrust.microsoft.com/

1.7. Certifications

- Icertis is an ISO 27001, ISO 27017, and 27018 certified organization. Icertis also complies with ITAR and has SOC1 and SOC2 (type2) certifications.

Microsoft Azure:

- Information on Azure compliance can be found here: https://servicetrust.microsoft.com/

2. Confidentiality

2.1. Physical Access Control

2.1.1. Access to Data Centres and Office Premises

- Access to Icertis and Microsoft Azure data centres and office premises are strictly restricted, monitored and logged.
- Access the Icertis data centre and office premises are provided only to the authorized personnel.
- In case a guest requires entry to the Icertis data centre or office premises, an employee of Icertis shall always accompany the guest.
- Access to Microsoft's data centres is managed by Microsoft and accordance with its strict access requirements.
- Procedures have been established by the Cloud Service Provider to restrict physical access to their datacentre to authorized employees, vendors, contractors, and visitors.
- Physical access mechanisms (e.g., access card readers, biometric devices, man traps/ portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals by Microsoft at its datacentres.

2.1.2. Monitoring

- Electronic surveillance and video monitoring of all the office entrances and exits including but not limited to security door interlocking systems and server rooms.
- Use of electronic physical access control systems with log generation and retention.

2.2. Logical Access Control

2.2.1. ICI Application

- Strict role-based access control is implemented in the ICI Platform. Icertis understands that the management of authentication (the user's identity) and authorization (the user's permissions) is critical to an application's overall security posture. The ICI Platform supports various kinds of authentication mechanisms. Authorization is generally implemented using various authorization features provided by within the ICI Platform. User authentication is logged.
- The ICI Platform recommends integration with customer's Identity Provider, which allows only customer users to have access to the ICI Platform. The ICI Platform has its own fine-grained authorization model, which is based on roles and security groups assigned to the user in ICI Platform. Customer user will have access to the data if he has valid account in Identity Provider and role and permissions are assigned in ICI Platform.

2.2.2. Cloud Operation

- The ICI Platform hosted on the Microsoft Azure platform is locked down using several digital certificates and passwords.
- Icertis ensures that access to Cloud Production subscription must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access Cloud instances.
- The ICI Platform is hosted on Microsoft Azure cloud and offered as a SaaS to end customer. The environment is managed by Icertis and only named FTEs from Icertis Ops team has access to environment for Ops related activities like deployments and troubleshooting. Customer will not have access to the cloud environment.
- Microsoft Azure's personnel administrating the Azure production environment use secure admin workstations (SAW). Access to the Azure production environment is granted on a just-in-time basis. Only Azure data centre engineers have persistent access to the environment, in this case it is ensured that no access to customer data is possible.
- Microsoft ensures Tenant level isolation on different layers, like compute isolation, storage isolation etc. Logical segregation is implemented to restrict unauthorized access to other customer tenants.
- Administrative access to the Azure service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e. read, write) are restricted to authorized personnel through designated channels based on job responsibilities.

2.2.3. IT

- Users from IT need privileged access to IT systems like Active Directory, Microsoft Offices 365, Network Devices, etc. All such privileged access is governed through special processes are reviewed once a quarter.
- Access to IT Hub rooms and server rooms is reviewed on a periodic basis and approval process requires the user to get an approval from the IT manager.
- IT uses Centralized Syslog Server to capture Active Directory, VPN and Network Logs. These logs are retained for minimum 1 year.
- IT has implemented an Endpoint Privilege Manager, Privileged Identity management solution to restrict the use of privileged accounts based on the principle of least privilege to ensure that no user can be assigned administrative access unless required and authorised, and those with a need for administrator accounts should only use them when necessary.
- Icertis has implemented the BitLocker encryption solution to encrypt the hard drives of laptops. BitLocker uses the AES 265-bit encryption method.
- Icertis has deployed Windows Defender anti-virus software on its workstations and servers for protection against viruses and intrusion attempts. The anti-virus software is configured to download latest virus definition updates automatically from the vendor's cloud server as and when the latest definitions are available.

2.3. ICI Platform Encryption

- All data at rest is encrypted using AES 256-bit encryption, which is provided by underlying Azure services. Encryption keys are managed by Microsoft Azure. If required, Icertis can manage the encryption keys in the Azure Key Vault.
- For data in transit, data encryption is done using TLS1.2 or IPSec standards. Internal Azure components communication is protected with TLS encryption.

- Icertis uses Transparent Data Encryption (TDE) service provided by Azure for encrypting the Azure SQL databases using AES 256-bit encryption
- Customer traffic moving between Azure datacentres are secured with a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec).

Microsoft Azure:

- Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption
- Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures
- Data at rest is encrypted using AES 256-bit encryption, which is provided by underlying Azure services.

2.4. Personal Data Transfers

- The ICI Platform treats data as highly confidential\sensitive data and does not disclose any data including personal information (if it is used for contract management process) without an authorisation.

Microsoft Azure:

- Procedures have been established by Microsoft for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes.

3. Integrity

3.1. Data Transfer Control

- All the Icertis employees are trained to handle personal data that is in accordance with the data protection laws and compliant with the GDPR rules.
- Deletion of customer data is in accordance with the data protection regulations and the contract signed, after the termination of contract.
- ICI Platform Rest APIs can be used for data transfer. Data will always remain in the cloud throughout the lifecycle of a contract.
- Microsoft network segregates customer traffic from management traffic. A monitoring system has been implemented to monitor the platform for potential malicious activity and intrusion past service trust boundaries.

3.2. Data Retention

- Data Icertis process on behalf of Customers is not stored on Icertis laptops or desktops.
- Icertis IT maintains an inventory of the assets to be disposed. These assets can be (not limited to the examples provided) desktops, laptops, servers, network devices, printers, monitors, TV Screen, projectors, loose storage media like USB drives, SD Cards, SSD, Tapes and HDD etc. The HDDs of these assets must be wiped before they are sent out from Icertis premises and there should not be any traces of Icertis logins and data.
- Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires or is terminated.

- Once the customer exit formalities are completed Icertis removes the Microsoft Azure subscription and deletes the data (including back up data) it processes on behalf of customers within 48 hours.
- Icertis provides data destruction confirmation/certificate upon request. The data is deleted permanently

Microsoft Azure:

- Microsoft (single tenant) wipes hardware according to best practices. Hardware that cannot be wiped will be destroyed following a defined procedure

3.3. Data Entry Control

- Icertis does not make any changes to customer data filed on the ICI Platform and only acts on the data as agreed by the customer
- The ICI Platform has its own Object Relational Mapping (ORM) framework, which is responsible managing transactions in the ICI Platform. The ICI Platform ORM layer also maintains the integrity of the data by applying appropriate locking mechanism during concurrent operations on the data.
- The ICI Platform has a validation engine that takes care of data validations at the time of data entry.

3.4. Mobile computing and Teleworking

- Microsoft Intune Mobile Device Management (MDM) solution is used for managing the mobile devices of all the employees for accessing Icertis applications and data on mobile devices.
- All the data stored on portable devices are encrypted.
- Prior to reuse or disposal of mobile devices such as laptops, all the data is purged.
- In case of remote work, use of VPN to connect to customer instances on the cloud is mandatory and IT provides the access to the employees in line with the principle of the least privileges.
- The Azure production environment is accessed through SAWs.
- In Microsoft Azure, access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection.

4. Availability and Resilience

4.1. Availability Control

- Business continuity planning and disaster recovery process are developed and exercised.
- Deployment of backup techniques.
- Constant monitoring of all the devices, networks, servers, and systems to ensure availability to customer instances.
- Emergency backup generators in place to ensure the normal operation of critical systems and components.
- Permanently active DDoS protection.

Microsoft Azure:

- Microsoft Azure reviews portal performance monthly to evaluate compliance with customer SLA requirements.
- Critical Azure components have been designed by Microsoft with redundancy to sustain isolated faults and minimize disruptions to customer services.
- Microsoft's Datacentre Management team maintains datacentre - managed environmental equipment within the facility according to documented policy and maintenance procedures.

4.2. Logs and Backups

- User Activity and Audit Log data (together the "Log(s)") are retained by default for 30 days from the date of Log generation.
- Audit Logs include Application Audit Logs and Application Access Logs. These logs include user identity data (i.e. person who is accessing e.g. the application, source IP address).
- User Activity Logs capture all pages accessed in ICI on an Authorised User basis.
- All Logs are read-only.
- Icertis has well automated scheduled backup of the customer data.
- Data at rest is encrypted using AES256 standards , including backups. Transparent Data Encryption (TDE) enabled on all DB storage During restores, they are restored in controlled production staging environment
- BCP/DR is performed as per the customer requirements.
- The ICI Platform data backup process:
  - All backups are stored in Azure BLOB storage with a separate and secured storage account.
  - The Storage is geo replicated, so backup copy is maintained at paired data centres, which are hundreds of miles away from primary data centre.
- Incremental backup is performed every 24 hours
- Full back up is performed once a week during a pre-defined maintenance window
- Backups (including Logs) are retained by default for 30 days from the date of log generation.
- Backups of key Azure service components and secrets are performed regularly by Microsoft and stored in fault tolerant (isolated) facilities.

Microsoft Azure:

- Microsoft Azure's Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.

5. Procedures for Regular Testing, Assessment, and Evaluation

5.1. Testing Assessment and Evaluation

- Icertis has vulnerability assessment and penetration testing process in place. Every major and minor release of ICI Platform goes through rigorous functional testing by internal QA team. In addition, every release goes through internal and external security testing.

Microsoft Azure:

- Microsoft publishes reports on penetration testing and security assessments.
- Microsoft's Azure code deployment adheres to the Security Development Lifecycle (SDL). Icertis follows Microsoft recommended secured development lifecycle (SDL) which helps to build more secure software and address all security compliance requirements. For more details, please refer - https://www.microsoft.com/en-us/sdl/default.aspx

5.2. Incident Response

- Icertis has centrally managed SOC team in place. Incident Response Management is implemented.
- The incident response document contains the chain of command that needs to be followed in case of incidents.
- Incidents are tracked and shall be resolved in a timely manner as per the SLA.
- The customer is informed about the incident.
- Records of incidents are maintained.

B. Technical Organisational Measure of other sub-processor

1. General

All access doors are locked and can only be opened with a key, key card, transponder and/or PIN key locks. A staffed reception is in place that can welcome and verify visitors to ensure that only authorized persons are allowed on the premises. Premises are monitored and intrusion prevention systems are installed. Access to all systems is only granted through valid authentication and authorization and several other security measures. Systems can only be accessed by entering a username and password, whereby the password is subject to a password policy restricting length, complexity etc. Additionally passwords must be changed regularly. Gateways are protected by firewall systems and are monitored. Gateways and systems are regularly checked by the sub-processor themselves and third parties (e.g. pen tests, audits etc.). Physical networking technology measures are implemented to resist attacks by malicious users or malicious code.

2. Data access Control

Access rights are only granted on the basis of the need-to-know-principle via the corresponding usernames. Personal data is only transmitted in encrypted form. There is an authorization concept in place in which access rights are monitored and logged to ensure that no activity is possible without valid authentication and authorization.

3. Separation control

It is ensured that data access is only possible for the required purposes. Different environments and applications are operated separately so that applications cannot access other applications. There are logical controls in place to separate Personal Data from other data, including the data of other customers.

4. Transfer control

Encryption of data that is being transmitted is ensured by using industry standard protocols. The destruction, disposal and erasure of computer hardware and electronic storage media is carried out in a manner where forensic industry standards are met. The erasure and destruction process is documented.

5. Availability control

The availability of data and media is ensured by backups. Physical systems (Servers, storage etc.) use multiple levels of redundancy to ensure the availability of systems, data and applications. All backup media is stored in secure locations. Protective measures against damage caused by fire, water and other environmental hazards are installed.

6. Commitment of employees to data secrecy; security policy

The Processor conducts and documents formal privacy and security awareness trainings for all its employees working with personal data.

ANNEX III – LIST OF SUB-PROCESSORS

The controller / data exporter has authorised the use of the following Sub-Processors:

(1) The current Icertis List of Standard Sub-Processors is available at https://www.icertis.com/foundation/ Unless otherwise agreed, if the Data Exporter is located in Europe, the data centre location for the MS Azure Data Centre is located in the European Union.

(2) In addition the Sub-Processor listed below (if any).

No	Country where personal data is filed / processed	Name of Sub-Processor	Address of Sub-Processor	Processing Activities
1	fill in as required			
2	fill in as required			

ANNEX IV - SUPPLEMENTARY MEASURES

The Data Importer implemented the following supplementary measures:

1. If the Data Importer receives a valid and binding order from any public authority for disclosure of Customer Data, it will use every reasonable effort to redirect the requesting party to request Customer Data directly from Data Exporter.
2. The Data Importer will promptly notify the Data Exporter of a request to allow Data Exporter to seek a protective order or other appropriate remedy, if Data Importer is legally allowed to do so. If Data Importer is prohibited from notifying the Data Exporter about the request, it will use all reasonable and lawful efforts to obtain a waiver of prohibition.
3. If the Data Importer, after exhausting all steps, is compelled to disclose Customer Data, it will disclose only the minimum amount of data to satisfy the request.
4. All customer data we process in ICI is encrypted (in transit and at rest).

ANNEX V – AMENDMENT UNITED KINGDOM

United Kingdom Addendum to EU Commission Standard Contractual Clauses
International Data Transfer

(the "Addendum")

This Addendum applies if and to the extent that personal data from United Kingdom is transferred to country without an adequate level of data protection under or in connection with the underlying main agreement.

This Addendum is based on the Information Commissioner's version B1.0, in force 21 March 2022

Part 1: Tables

Table 1: Parties

Start date	**Date of the Data Processing Agreement**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	*Full legal name*: as per underlying main agreement *Trading name* (if different): n.a. *Main address (if a company registered address):* as per underlying main agreement. Official registration number (if any) (company number or similar identifier): Registered number: as per underlying main agreement.	*Full legal name*: Icertis Inc. *Trading name (if different)*: nan *Main address (if a company registered address):* 14711 NE 29th Place, Suite 100 Bellevue WA 98007, USA *Official registration number (if any) (company number or similar identifier):* File no 5703188 State of Delaware
Key Contact	*Full Name / Job Title:* Data Protection Officer *Contact details including email:*	*Full Name (optional):* *Job Title*: Global Data Protection Officer *Contact details including email:* GlobalDPA@icertis.com

		Tel. +91 20 6608 8400; representative in the European Union: Icertis GmbH, Taunusanlage 1 in 60329 Frankfurt, Germany, DSB@icertis.com
Signature (if required for the purposes of Section 2)	Entering into the Approved EU SCCs and any part of the Approved EU SCCs will have the same effect as signing this Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: *Date*: The signature date of Approved EU SCCs or the underlying main agreement (as the case may be).

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), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set out in the Approved EU SCCs to which this Addendum is appended.

Annex 1B: Description of Transfer: As set out in the Approved EU SCCs to which this Addendum is appended

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in the Approved EU SCCs to which this Addendum is appended.

Annex III: List of Sub processors (Modules 2 and 3 only): As set out in the Approved EU SCCs to which this Addendum is appended

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into the Approved EU SCCs and any part of the Approved EU SCCs will have the same effect as signing this Addendum.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum 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 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a) References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b) In Clause 2, delete the words:

    "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";

    c) Clause 6 (Description of the transfer(s)) is replaced with:

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

where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7 (i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8 (i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f) References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws".

References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with:

m) "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

n) Clause 17 is replaced with:

o) "These Clauses are governed by the laws of England and Wales.";

p) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer

before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

q) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

ANNEX VI – AMENDMENT SWITZERLAND

Swiss Addendum to EU Commission Standard Contractual Clauses International Data Transfer
(the "Addendum")

Date of this Addendum

1. This Addendum is effective on the effective date of the Data Protection Addendum.

Background

2. On August 27, 2021, the Federal Data Protection and Information Commissioner ("the FDPIC") announced that the new EU Standard Contractual Clauses (the "SCCs") may be relied on to legitimize transfers of personal data from Switzerland to countries without an adequate level of data protection, provided that the necessary amendments and adaptations are made for use under Swiss data protection law. As a result, the Parties have decided to enter into a separate Addendum to comply with Swiss specific data protection law to provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the GDPR and, with respect to data transfers from controllers to processors.

3. Annex VI applies if and to the extent that personal data from Switzerland is transferred to country without an adequate level of data protection under or in connection with the underlying main agreement.

4. This Addendum shall apply to all transfers of personal data that are subject to the Swiss Federal Act on Data Protection ("FADP") of June 19th, 1992, until the 31st of December 2022 and from January 1st, 2023, onward, the Revised Swiss Federal Act on Data Protection ("Revised FADP") of September 25th, 2020, (FADP and Revised FADP together referred to as "Swiss Data Protection Law").

Interpretation of this Addendum

5. Where this Addendum uses terms that are defined in the ANNEX those terms shall have the same meaning as in the ANNEX. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the ANNEX that incorporates the Clauses
The ANNEX	The Standard Contractual Clauses set out in the Data Protection Addendum that are based on the Commission Implementing Decision (EU)2021/914 of 4 June 2021.

Swiss Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in Switzerland, including the Federal Act on Data Protection (FADP).

6. This Addendum shall be read and interpreted in the light of the provisions of the Swiss Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

7. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in the Swiss Data Protection Laws.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re- enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

10. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

    a. for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter's processing when making that transfer; and

    b. to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR.

    c. the provision of the SCCs protect the data of legal entities until the entry into force of the revised FADP.

11. The amendments required by Section 10 above, include (without limitation):

    a. References to the "Clauses" means this Addendum as it incorporates the Clauses;

    b. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in ANNEX, Appendix Annex I.B where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

c. In Clause 13(a) and Part C of ANNEX, Appendix Annex II; the "competent supervisory authority" is the FDPIC; insofar as the data transfer is governed by the FADP; an EU authority insofar as the data transfer is governed by the GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed).

d. Clause 17 is replaced to state "These Clauses are governed by the laws of Germany".

e. Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of Germany. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts."

f. The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum

12. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Germany.

13. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 10 above.

Executing this Addendum

14. By signing the ANNEX, the parties agree to be bound by this Swiss Addendum to EU Commission Standard Contractual Clauses International Data Transfer including the terms of the ANNEX. This Annex is deemed to be signed if the Data Protection Addendum to which this is an Annex has been entered into.