**Standard Contractual Clauses**

**for the transfer of personal data outside the EEA**

***June 2021 version***

***Modules 1-3***

*Overview*: Your company, as data exporter, transfers personal data as a controller and possibly as a processor to the Alida entity you are contracting with for services (“**Alida**”), as data importer, whereby such personal data originates from the EEA. Alida is based outside the EEA and provides services to data exporter under a separate commercial agreement (“**Contract**”) and agrees to the attached Standard Contractual Clauses as:

1. A controller under Module 1 for limited business contact information concerning individual representatives who provide instructions to data importer; and
2. A processor under Module 2 and, if applicable, a subprocessor under Module 3, for all other personal data that data exporter makes available to data importer for processing on data exporter’s behalf, in which case data exporter’s instructions for processing are set forth in the descriptions of services that the data importer has agreed to provide in the Contract.

The parties shall not modify the text of the attached Standard Contractual Clauses and only complete blanks and Annexes.

The UK International Data Transfer Addendum to the Standard Contractual Clauses, as set out in Annex III, shall apply solely to the extent that the personal data pertains to individuals in the UK and/or where data exporter is established in the UK.

**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) ([[1]](#footnote-0)) 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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

(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 – Optional*

**Docking clause**

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

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

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

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.

**MODULE ONE: Transfer controller to controller**

8.1 **Purpose limitation**

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

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

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

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

8.2 **Transparency**

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

(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]](#footnote-1)) 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]](#footnote-2)) (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.

**MODULE TWO: Transfer controller to processor**

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 ([[4]](#footnote-3)) (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.

**MODULE THREE: Transfer processor to processor**

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([[5]](#footnote-4)).

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter 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.

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 rectify or erase 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 controller 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, 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. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([[6]](#footnote-5)) (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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**

**MODULE TWO: Transfer controller to processor**

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION 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 30 days 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. ([[7]](#footnote-6)) 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.

**MODULE THREE: Transfer processor to processor**

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. ([[8]](#footnote-7)) 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 or controller’s request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

*Clause 10*

**Data subject rights**

**MODULE ONE: Transfer controller to controller**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([[9]](#footnote-8)) 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.

**MODULE TWO: Transfer controller to processor**

(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.

**MODULE THREE: Transfer processor to processor**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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**

**MODULE ONE: Transfer controller to controller**

(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.

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

(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) [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ([[10]](#footnote-9));

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these 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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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 Germany.

*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 Germany.

(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.

**ANNEX I**

A. **LIST OF PARTIES**

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

1. **Name:** [insert]

**Address:** [insert]

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

**Activities relevant to the data transferred under these Clauses:** Recipient of data importer’s services

**Signature and date:** [insert]

**Role (controller/processor):** Controller for Modules 1 and 2 and possibly Processor for Module 3

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

1. **Name:** [insert name of contracting Alida entity]

**Address:** [insert address of contracting Alida entity]

**Contact person’s name, position and contact details:** Alida’s GDPR-specific representative is Alida GmbH, Friesenplatz 4, Floor 4, 50672 Cologne, Germany Phone: +49 221 65088931. Alida’s Data Protection Officer may be contacted at [privacyofficer@alida.com](mailto:privacyofficer@alida.com).

**Activities relevant to the data transferred under these Clauses:** Service provider to data exporter

**Signature and date:** [insert]

**Role (controller/processor):** Controller for Module 1, Processor for Module 2, and possibly Subprocessor for Module 3

B. **DESCRIPTION OF TRANSFER**

**MODULE ONE: Transfer controller to controller**

*Categories of data subjects whose personal data is transferred*

Individual representatives of data exporter in the European Economic Area.

*Categories of personal data transferred*

Business contact information.

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

None.

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

Continuous.

*Nature of the processing*

Use, storage and disclosure.

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

To manage the business relationship between data exporter and data importer.

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

Data importer shall retain the personal data for no longer than necessary for the purposes for which it is processed.

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

Processors will return or delete the personal data at the end of their relationship with the data importer and at any time at the data importer’s request.

**MODULE TWO: Transfer controller to processor**

*Categories of data subjects whose personal data is transferred*

The data subjects are data exporter’s authorized users of data importer’s services or any other individual whose personal data is collected by or introduced into the data importer’s services by data exporter.

*Categories of personal data transferred*

The categories of personal data transferred to data importer shall be solely determined by and the responsibility of data exporter while using the data importer’s services.

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

The categories of personal data transferred to data importer shall be solely determined by and the responsibility of data exporter while using the data importer’s services.

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

Continuous.

*Nature of the processing*

The personal data transferred may be subject to any processing activities including, without limitation, hosting, storage, transmission, redaction and use to provide services.

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

The purpose of processing is the provision of the services from data importer to data exporter. Such services are focused on helping companies analyze their interactions and strengthen their relationships with their customers.

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

The data importer will return or delete the personal data at the end of its relationship with the data exporter and at any time at the data exporter’s request.

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

Sub-processors will return or delete the personal data at the end of their relationship with the data importer and at any time at the data importer’s request.

**MODULE THREE: Transfer processor to processor**

*Categories of data subjects whose personal data is transferred*

The data subjects are data exporter’s authorized users of data importer’s services or any other individual whose personal data is collected by or introduced into the data importer’s services by data exporter.

*Categories of personal data transferred*

The categories of personal data transferred to data importer shall be solely determined by and the responsibility of data exporter while using the data importer’s services.

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

The categories of personal data transferred to data importer shall be solely determined by and the responsibility of data exporter while using the data importer’s services.

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

Continuous.

*Nature of the processing*

The personal data transferred may be subject to any processing activities including, without limitation, hosting, storage, transmission, redaction and use to provide services.

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

The purpose of processing is the provision of the services from data importer to data exporter. Such services are focused on helping companies analyze their interactions and strengthen their relationships with their customers.

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

The data importer will return or delete the personal data at the end of its relationship with the data exporter and at any time at the data exporter’s request.

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

Sub-processors will return or delete the personal data at the end of their relationship with the data importer and at any time at the data importer’s request.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

Germany’s federal supervisory authority or the supervisory authority of the state in which Alida’s German entity is located.

**ANNEX II**

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

# Alida Subscriber Data Protection Schedule

*Effective as of January 1, 2022*

The Alida entity that has entered into a contract with the Subscriber (“**Alida**” or “**we**”) serves the Subscriber and protects Subscriber Data in compliance with the terms of this Data Processing Schedule (“**Schedule**”).

## Definitions

1. “**Contract**” means the contract between Alida and Subscriber in which Alida agrees to make the Solution available to Subscriber, including all data sheets, service specifications, and other technical documentation, as amended from time to time, that may be incorporated by reference therein.
2. **“Backup”** means an extra copy of data to be used in the event that the original copy is damaged or unavailable. The extra copy of data is kept separately from the original copy.
3. **“Member”** means an individual whose data is processed in the Solution including when invited by or on behalf of Subscriber to visit, submit, view or comment on Subscriber Data on the Website and/or to participate in any forum, discussion, research, survey, study or any other means or form of data collection administered through the Solution.
4. **“Penetration Test”** means a search of software for misconfigurations and Security Defects by a security expert without access to the system’s source code;
5. **“Personal Data”** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
6. **“Production System”** and **“Production Network”** means a computing environment that is used to host the Solution and is subject to access controls and management processes governing the introduction of changes;
7. **“Security Breach”** means any confirmed unauthorized access to, use of, or disclosure of Subscriber Data;
8. **“Security Defect”** means a technical deficiency in the software or hardware that, if exploited, could result in unauthorized access to the Solution or the Subscriber Data;
9. **“Security Questionnaire”** means any Subscriber developed or proprietary form or any other means that collects information on the security, privacy or data protection capabilities of Alida;
10. **“Security Scan”** means an automated search of a system for Security Defects without access to the system’s source code;
11. “**Solution**” means the technology platform and automated services owned by Alida, including all standard upgrades and updates thereto but excluding any third-party products or software that may interoperate with Alida’s technology platform;
12. **“Subscriber”** is a customer of Alida who has entered into a subscription agreement with Alida to access and use the Solution, and such term includes Subscriber’s authorized users of the Solution;
13. **“Subscriber Data”** means information uploaded to or collected through the Solution by the Subscriber, or submitted to the Solution by Members;
14. **“Sub-Processor”** means a party that provides services to Alida for purposes of delivering the Solution and may have access to Subscriber Data; and
15. **“Supplier”** means a party that provides services to Alida for purposes of delivering the Solution and does not access Subscriber Data in provisioning such services.
16. **“Website”** means Subscriber’s online operating instance of the Solution identified by and accessed via a domain owned by Subscriber.

## Control and Ownership

Subscribers own and control all Subscriber Data. Alida does not use Subscriber Data, except: (a) in the interest and on behalf of the Subscriber; (b) as necessary to provide the Services; or (c) as contemplated or directed by the Contract. Alida reserves all rights to the Solution, Alida’s technology and Alida’s data, including any information that Alida discovers, creates or derives as it provides the Solution, except Subscriber Data.

## Security

Alida applies technical, administrative and organizational data security measures that meet or exceed the requirements described in Alida’s Statement of Technical and Organizational Measures (attached). Alida may update and modify its Statement of Technical and Organizational Measures from time to time, provided that Alida must not reduce the level of security provided thereunder, except with Subscriber’s consent or with 90 days prior written notice.

## Cooperation with Compliance Obligations

At Subscriber’s reasonable request, Alida will (a) reasonably assist Subscriber with data access, deletion, portability and other requests, subject to compensation for any custom efforts required of Alida, and (b) enter into additional contractual agreements to meet specific requirements that are imposed by mandatory laws on Subscriber pertaining to Subscriber Data and that, due to their nature, can only be satisfied by Alida in its role as service provider or that Subscriber specifically explains and assigns to Alida in an addendum or amendment to the applicable Contract, subject to additional cost reimbursement or fees as appropriate. At Subscriber’s request, where Subscriber is based within the EEA or the UK and is contracting with an Alida entity that is not based within the EEA or within an “adequate third country” (as determined by the European Commission) Alida will agree to the EU Commission Standard Contractual Clauses and UK International Data Transfer Addendum thereto for cross-border transfers. If Subscriber can no longer legally use Alida’s products due to changes in law or technology, Alida shall allow Subscriber to terminate certain or all contracts and provide transition or migration assistance as reasonably required, subject to termination charges and fees as mutually agreed in good faith by the parties.

## Security Breaches

In the event of a Security Breach, Alida shall use commercially reasonable efforts to: (i) contain and mitigate the impact of the Security Breach without undue delay; (ii) conduct an investigation into the cause of the Security Breach; (iii) notify Subscriber of the Security Breach without undue delay; and (iv) provide reasonably requested information to Subscriber to assist Subscriber in discharging its own legal obligations. For clarity, a respondent disclosing the contents of a Website to which they have been provided authorized access is not a Security Breach.

## Audits

On an annual basis and at its own cost Alida will procure an independent audit of its security and privacy capabilities by a qualified professional of Alida’s own choosing. Upon written request, Alida shall provide the resulting audit report (“**Audit Report**”) to Subscriber. Upon Subscriber’s written request, Alida will provide a commercially reasonable timeline for addressing any material defects in Alida’s privacy and security controls identified in the Audit Report (“**Identified** **Material Defects**”). Alida shall provide Subscriber or its designated auditor the opportunity to perform their own audit of Alida’s privacy and security controls (“**Subscriber Audit**”) only under the following circumstances: (i) the Audit Report is unavailable and Alida cannot provide a commercially reasonable timeline for when it will be made available to Subscriber; and (ii) the Audit Report includes Identified Material Defects for which Alida has not provided a remediation timeline. Any Subscriber Audit shall take place: (i) at Subscriber’s sole expense; (ii) during Alida’s normal business hours and over the course of no more than 2 business days: (iii) upon at least 10 business days’ advance written notice to Alida with the notice including a clear scope statement and any evidence or other resources that Subscriber wishes to review; (iv) with Alida’s written consent, which shall not be unreasonably withheld or delayed; (v) pursuant to appropriate confidentiality agreements; and (vi) only once per subscription year. For clarity, any request from Subscriber to complete a security questionnaire will be considered an invocation of audit rights, which Alida may satisfy with an Audit Report. Alida may also, at its own choosing, provide one of the following in lieu of responses to Subscriber’s security questionnaire: (i) a completed Standard Information Gathering (SIG) questionnaire provided by Shared Assessments and The Santa Fe Group; (ii) a completed Cloud Security Alliance (CSA) questionnaire; or (iii) another reasonably equivalent standard questionnaire.

## Hosting Locations

Alida’s core systems, and associated data storage, are housed in a hosting facility at one of the following locations in accordance with the following: (i) Subscriber Data of Subscribers based in the Americas is hosted in Amazon Web Services’ availability regions in the USA or Canada; (ii) Subscriber Data of Subscribers based in Europe, the Middle East or Africa is hosted in Amazon Web Services’ availability region in Germany; and (iii) Subscriber Data of Subscribers based in the Asia-Pacific region is hosted in Amazon Web Services’ availability region in Singapore. Alida may relocate its hosting facilities and all Subscriber Data therein provided that such relocation: (i) is posted to Alida’s website at least 60 days in advance; and (ii) Alida keeps Subscriber Data within the same relative geographical region which is one of: (a) North America for Subscribers in the Americas; (b) the European Union for Subscribers in Europe, the Middle East or Africa; or (c) the Asia-Pacific region for Subscribers in Oceania, South East Asia, South Asia and East Asia. Alida shall maintain an up-to-date list of hosting facilities at <https://www.alida.com/trust/legal/> or another page on its website with the same purpose (“**Subscriber** **Notices** **Page**”). For clarity, as between Alida and Subscriber, it is Subscriber’s responsibility to comply with any regulations that require hosting of Subscriber Data within a specific jurisdiction. Alida maintains a global user store to manage Subscriber administrative user account authentication and routing to the relevant hosting region as described above. The data in this user store is housed in Canada.

## Suppliers and Sub-Processors

Alida shall maintain appropriate legal agreements with all Suppliers and Sub-processors to ensure compliance with the obligations laid out within this Schedule and shall be responsible for its Suppliers’ and Sub-processors’ compliance with the terms of this Schedule. Alida shall maintain an up-to-date list of Suppliers and Sub-processors and their locations on its Subscriber Notices Page. Subscribers may register to receive automated notifications of updates to the list of Suppliers and Sub-processors.

## Deletion and Anonymization

Upon termination of the Contract, Alida will permit Subscriber 30 days to export Subscriber Data from the Solution. Following such 30-day period, Alida will have no responsibility to retain any Subscriber Data and will thereafter permanently delete all Subscriber Data stored within the Solution. Subscriber Data Backups shall be securely deleted or overwritten 90 days thereafter. Upon request and if available, Alida will provide Subscriber with the ability to designate specific fields within a survey as Personal Data that should be overwritten after a Subscriber specified period of time has passed. Only fields associated with Members that have had their account set to an inactive status will be overwritten after the Subscriber’s specified period of time has elapsed. For clarity, the Member’s record will be considered anonymized by the Solution when the fields specified by the Subscriber are overwritten such that they no longer contain identifying data; additionally the Solution will overwrite the Member’s email address, user ID, name and telephone number. Once overwritten the original data is retained as a Backup for 90 days thereafter. Notwithstanding the preceding statements, Alida does not purge security and performance log data on Subscription termination, such data is eventually overwritten from our central logging system over time. Logs generally do not contain Member-provided data although they may contain email address and IP address, and other identifying information in some cases.

## No Information Selling or Sharing for Cross‐Context Behavioral Advertising.

Alida does not accept or disclose any Subscriber Data as consideration for any payments, services or other items of value. Alida does not sell or share any Subscriber Data, as the terms “sell” and “share” are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act (“**CCPA**”). Alida processes Subscriber Data only for the business purposes specified in the written Contract. Alida does not retain, use, or disclose Subscriber Data (a) for cross‐context behavioral advertising, or (b) outside the direct business relationship with the Subscriber. Alida does not combine Subscriber Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA.

## EEA Personal Data

With respect to any Subscriber Data that is subject to the EU General Data Protection Regulation (GDPR) or similar laws of other countries as “personal data,” Alida accepts the following obligations as a data importer, processor or subprocessor of Subscriber and warrants that Alida

### processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or EU Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;

### ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

### takes all measures required pursuant to Article 32 of the GDPR (security of processing);

### respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;

### taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controller’s obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects)

### assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;

### at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

### makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

## Notice of Changes

From time to time Alida may update its security and privacy practices. Any material changes will be posted on the Subscriber Notices Page at least 30 days prior to their coming into effect unless otherwise specified in the Contract. In the event Subscriber determines any such material change(s) are not acceptable to them, Subscriber may terminate its Contract with Alida as per its terms.

## Integration

This Schedule is binding on Alida if and to the extent it is expressly agreed or incorporated by reference in a duly signed Contract. This Schedule shall not create third-party beneficiary rights. Alida does not accept or submit to additional requirements relating to Subscriber Data, except as specifically and expressly agreed in writing with explicit reference to the Contract and this Schedule.

# Alida Statement of Technical and Organizational Measures

## General

This Statement of Technical and Organizational Measures outlines the processes, infrastructure and policies that Alida has in place to protect its systems and Subscriber Data. Capitalized terms herein have the same meaning as in the Alida Subscriber Data Protection Schedule.

## Policies and Governance

Alida has implemented the following governance structure with respect to its security and privacy policies and standards (the “**Policies**”):

1. Alida’s Policies have been approved by Alida’s executive (the “**Executive**”);
2. A member of senior management is responsible for security and privacy at Alida and periodically reports to the Executive and Alida’s board of directors (the “**Board**”) on such matters;
3. Risks are centrally recorded and reported to the Executive and the Board as required;
4. Alida periodically reviews its Policies and supporting documentation for relevance;
5. Non-compliance with a Policy requires approvals in accordance with a clear authority framework;
6. Non-compliance without authorized approval of Policies has outcomes up to and including termination of employment;
7. Alida periodically reviews its Policies and supporting documentation for relevance;
8. On an annual basis, Alida conducts user security and privacy awareness education;
9. All employees sign-off on the Policies annually;
10. All new hires at Alida receive criminal background checks where permitted by law; and
11. All employees are subject to written confidentiality agreements.

## Data Centre Security

Alida houses the Solution in enterprise class data centres that provide:

1. Independent annual audit reports of their security and availability capabilities. Such reports include but are not limited to: AICPA’s Service Organization Controls (‘SOC’) audit reports or ISO27001 certifications;
2. Redundant cooling, fire suppression, power and communications; and
3. 24x7 guard services, physical access control and video surveillance.

## Infrastructure Security

Alida has implemented the following security mechanisms:

1. The Solution is protected by firewalls or functionally equivalent technology that restricts traffic to only that which is required to provide the service;
2. Network traffic into the networking hosting the Solution is monitored by intrusion detection;
3. All access to the Solution and its supporting infrastructure is centrally logged;
4. 24/7 automated monitoring for malicious activity;
5. Bastion hosts and two factor authenticated VPN access into the Production Network; and
6. Anti-virus software.

## Multi-tenant Environment

Alida provides a multi-tenant Solution which holds data for multiple Subscribers, and provides the following protections:

1. Each Website is dedicated to a single Subscriber;
2. Websites are uniquely identified by their domain name and underlying account identifier;
3. Access to Websites are only granted to the identities directly associated with the Subscriber’s account;
4. Data is logically segregated using either separate database schemas or data attributes that are used by the application code to make access decisions; and
5. Detailed infrastructure logs are not available to any Subscriber.

## Application Security

Alida provides the following controls within and around the Solution:

1. Username and password protected access to the administrator portal and optional integration with SAML 2.0 Identity Providers;
2. Authenticated access to the Website;
3. Logging of study creation/deletion/deployment as well as all user creation/modification/deletion; and
4. Secure development practices and use of safe software libraries. For the purposes of this section, a “safe software library” is one that is provided by the manufacturer that is free of known security defects and is designed such that developers are forced to use the library in a manner that does not unintentionally introduce security defects into the Solution.

## Data Encryption

1. All connections to the Solution are protected using encrypted channels including but not limited to Transport Layer Security (TLS);
2. All Backups are encrypted; and
3. All systems storing Subscriber Data use disk storage that is encrypted at rest.

## Operations

1. Alida has implemented processes including vulnerability management, incident response and security patching procedures to protect against known and emerging threats.
2. Changes to Production Systems can only be implemented by authorized system administrators following a defined quality assurance, change management, and approval process.

## Disaster Recovery and Business Continuity

1. Alida shall maintain onsite snapshots and capacity sufficient to restore individual Websites within 48 hours with no more than 24 hours of data lost;
2. If Alida sends backups of the data offsite such backups will be encrypted and the keys for the encryption will remain under Alida’s control; and
3. In the event of a catastrophic loss of an entire data centre, Alida shall use its commercially reasonable efforts to recover Subscriber’s Website.

## Privacy Policies and Logs

1. Alida maintains privacy policies to govern its own internal practices with regard to the secure and legal processing of Personal Data. Such policies address consent, collection limitation, data quality, limitation of use, disclosure, retention, transfers, data subject rights, and security as required by Applicable Privacy Regulation with regard to the processing of Personal Data. “**Applicable Privacy Regulation**” includes, but is not limited to:
   1. *The Personal Information Protection and Electronic Documents Act* (“**PIPEDA**”) of Canada;
   2. The General Data Protection Regulation 2016/679 (“**GDPR**”);
   3. The Federal Privacy Act 1988 of Australia;
   4. The Personal Data Protection Act 2012 of Singapore; and
   5. The California Consumer Privacy Act (“**CCPA**”).
2. Alida will retain logs containing personal information such as email addresses and IP addresses as well as actions taken on the Solution for security and monitoring purposes.

## Security Testing

1. Alida will conduct an annual Penetration Test of the Solution using an external provider determined in Alida’s sole discretion. Once identified Security Defects are remediated, Alida will confirm such remediation, or will arrange for same external provider to provide confirmation thereof;
2. Alida will conduct monthly Security Scans of the Solution;
3. Upon request by Subscriber, Alida will provide evidence that such Penetration Testing and Security Scanning has been performed;
4. Once per subscription year and with at least ten (10) business days of notice, Subscriber or its agent, may perform its own Penetration Testing against a Website provided by Alida, not the Subscriber’s Website. Subscriber agrees to forego this right if Alida, in its sole discretion, offers an equivalently scoped report that is no more than twelve (12) months old;
5. Notwithstanding the preceding limitations of Penetration Testing frequency, additional testing to confirm that issues previously reported have been remediated are not limited in frequency;
6. At times mutually agreed between the parties, a Subscriber or its agent, may perform Security Scanning against its own Website once their methodology has been reviewed and approved by Alida;
7. Such annual Penetration Testing or Security Scanning by the Subscriber is in addition to the audit rights as provided in the Alida Subscriber Data Protection Schedule;
8. Alida may reasonably withhold approval for Penetration Testing or Security Scanning if there is reason to believe that the methodology the Subscriber or its agent will use disrupts the performance, availability or integrity of the Solution;
9. If Penetration Testing or Security Scanning by Subscriber or its agent disrupts the performance, availability or integrity of the Solution then Alida may direct Subscriber to immediately stop or cause to be stopped all Penetration Testing of Security Scanning activity until such time Alida is satisfied as to the reason for disruption being addressed;
10. Subscriber will provide all information reasonably requested by Alida on the nature of their Penetration Testing and Security Scanning activities prior to commencing their work. Such information includes but is not limited to: source IP addresses, contact information, employee or agent names and times of testing;
11. Subscriber or its agent will comply with Alida’s guidance on performing Penetration Testing and Security Scanning and in return Alida will furnish Subscriber with the necessary access to perform such Penetration Testing and Security Scanning;
12. If Subscriber requires that identified Security Defects be remediated, Subscriber or its agent must provide in writing the full details of the Security Defect such that Alida may independently assess, replicate and verify the existence of the Security Defect; and
13. Within ten (10) business days of Alida confirming the existence of the reported Security Defects Alida will provide, upon request, a remediation plan in accordance with the timelines in the following section.

## Security Defect Remediation

1. Alida uses industry standard scoring techniques, such as Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS), for evaluating the severity of any identified security defect. Alida may, at its own discretion, replace them with equivalent scoring techniques.
2. Alida will score a security defect using the aforementioned techniques and categorize defects by impact as follows:

| **Common impact name** | **CVSS** | **CWSS** |
| --- | --- | --- |
| **Critical** | 9.0 to 10.0 | 90 to 100 |
| **High** | 7.0 to 8.9 | 70 to 89 |
| **Medium** | 4.0 to 6.9 | 40 to 69 |
| **Low** | 0.0 to 3.9 | 0 to 39 |

1. Alida will remediate Security Defects in our Solution using the following schedule once the reported Security Defect is confirmed:

| **Common impact name** | **Timing** |
| --- | --- |
| **Critical** | Promptly and not more than fourteen  (14) days |
| **High** | Within forty-five (45) days |
| **Medium** | Within ninety (90) days |
| **Low** | Within one hundred and eighty (180) days |

1. Alida, at its own discretion, may implement a temporary solution to the Security Defect to achieve the timelines listed above. Such temporary solutions may include temporarily disabling or altering specific functionality, while working to implement a permanent solution to the Security Defect. Should Alida choose to temporarily disable or alter functionality to address a Security Defect, Subscriber will not treat such actions as a reduction in service;
2. Alida may reasonably defer remediation of a reported security defect for reasons including, but not limited to:

#### The Security Defect is reported too late in the current release cycle to safely include relative to our change management practices;

#### A planned change or fix will address the Security Defect in a reasonable time frame; or

#### All available resources are already working on a Security Defect of a greater impact.

1. Alida may reasonably decline to remediate a Security Defect if the security defect provides no reasonable path for gaining access to Subscriber Data or the Solution.

**ANNEX III**

**International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

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

**Part 1: Tables**

**Table 1: Parties**

| 1. **Start date** | 1. Date of the last signature shown in Annex I.A above. | |
| --- | --- | --- |
| 1. **The Parties** | 1. **Exporter (who sends the Restricted Transfer)** | 1. **Importer (who receives the Restricted Transfer)** |
| 1. **Parties’ details** | 1. Full legal name: See Annex I.A above. 2. Trading name (if different): [insert] 3. Main address (if a company registered address): See Annex I.A above. 4. Official registration number (if any) (company number or similar identifier): [insert] | 1. Full legal name: See Annex I.A above. 2. Trading name (if different): 3. Main address (if a company registered address): See Annex I.A above. 4. Official registration number (if any) (company number or similar identifier): [insert] |
| 1. **Key Contact** | 1. Full Name (optional): [insert] 2. Job Title: [insert] 3. Contact details including email: [insert] | 1. Full Name (optional): 2. Job Title: Data Protection Officer 3. Contact details including email: [privacyofficer@alida.com](mailto:privacyofficer@alida.com). |
| 1. **Signature (if required for the purposes of Section ‎2)** | 1. See Annex I.A above. | 1. See Annex I.A above. |

**Table 2: Selected SCCs, Modules and Selected Clauses**

| 1. **Addendum EU SCCs** | ⌧ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:   1. Date: See Annex I.A above 2. Reference (if any): 3. Other identifier (if any): 4. Or   ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |
| --- | --- |

| 1. Module | 1. Module in operation | 1. Clause 7 (Docking Clause) | 1. Clause 11  (Option) | 1. Clause 9a (Prior Authorisation or General Authorisation) | 1. Clause 9a (Time period) | 1. Is personal data received from the Importer combined with personal data collected by the Exporter? |
| --- | --- | --- | --- | --- | --- | --- |
| 1. 1 |  |  |  |  |  |  |
| 1. 2 |  |  |  |  |  |  |
| 1. 3 |  |  |  |  |  |  |
| 1. 4 |  |  |  |  |  |  |

**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:

| 1. Annex 1A: List of Parties: See Annex I.A above. |
| --- |
| 1. Annex 1B: Description of Transfer: See Annex I.B. above. |
| 1. Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II above. |
| 1. Annex III: List of Sub processors (Modules 2 and 3 only): Available on Alida’s Subscriber Notices Page (see Annex II). |

**Table 4: Ending this Addendum when the Approved Addendum Changes**

| 1. **Ending this Addendum when the Approved Addendum changes** | 1. Which Parties may end this Addendum as set out in Section 19: 2. ⌧ Importer 3. ☐ Exporter 4. ☐ neither Party |
| --- | --- |

**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 this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this Addendum**

1. 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:

| 1. Addendum | 1. This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| --- | --- |
| 1. Addendum EU SCCs | 1. The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| 1. Appendix Information | 1. As set out in Table ‎3. |
| 1. Appropriate Safeguards | 1. 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. |
| 1. Approved Addendum | 1. 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. |
| 1. Approved EU SCCs | 1. The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| 1. ICO | 1. The Information Commissioner. |
| 1. Restricted Transfer | 1. A transfer which is covered by Chapter V of the UK GDPR. |
| 1. UK | 1. The United Kingdom of Great Britain and Northern Ireland. |
| 1. UK Data Protection Laws | 1. 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. |
| 1. UK GDPR | 1. As defined in section 3 of the Data Protection Act 2018. |

1. 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.
2. 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.
3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
4. 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.
5. 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**

1. 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.
2. 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.
3. 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**

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
   1. 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;
   2. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
   3. 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.
2. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
3. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
4. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
5. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
6. 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”;

1. 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.”;

1. 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”;

1. 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;”

1. 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;
2. References to Regulation (EU) 2018/1725 are removed;
3. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
4. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
5. Clause 13(a) and Part C of Annex I are not used;
6. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
7. In Clause 16(e), subsection (i) is replaced with:

“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;”;

1. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

1. 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

1. 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**

1. 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.
2. 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.
3. From time to time, the ICO may issue a revised Approved Addendum which:
4. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
5. 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.

1. 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:
   1. its direct costs of performing its obligations under the Addendum; and/or
   2. 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.

1. 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.

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915. [↑](#footnote-ref-0)
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. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)
4. 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. [↑](#footnote-ref-3)
5. See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725. [↑](#footnote-ref-4)
6. 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 purposes of these Clauses. [↑](#footnote-ref-5)
7. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-6)
8. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-7)
9. 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. [↑](#footnote-ref-8)
10. 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. [↑](#footnote-ref-9)