DATA PROCESSING ADDENDUM

The below Data Processing Addendum (DPA) constitutes an integral part of the agreement concluded with a Service Provider and is hereby incorporated to it by reference.

Notably, the DPA includes the list of EU Standard Contractual Clauses.

Although the DPA is incorporated to your Service Provider agreement and valid without the necessity to put your written signatures in the body of the DPA, it is required to execute an Executive Annex between the parties, draft of which constitutes Schedule 3 to this DPA. Processing of personal data on behalf of Syncron shall take place only if Executive Annex is concluded between the parties.

In case of any questions, please use the contact form here.

WHEREAS

This Data Processing Addendum ("**DPA**") is hereby incorporated to and forms part of the principal agreement t between Syncron and Service Provider (collectively as the "**Parties**") concerning their cooperation (the "**Principal Agreement**"), identified either as Services or otherwise in the applicable agreement ("**Services**"). This DPA is intended to reflect the parties' agreement regarding the processing of personal data that Syncron may transfer to Service Provider.

The Service Provider entity that is a party to the Principal Agreement should be a party to this DPA. The Syncron entity that is a party to the Agreement should be a party to this DPA.

In order for this DPA to be effective, Parties shall execute an Executive Annex (Schedule 3). Processing of personal data on behalf of Syncron shall take place only if Executive Annex is concluded between the Parties.

In the course of providing the Services to Syncron pursuant to the Principal Agreement, Service Provider may Process Personal Data on behalf of Syncron and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. Definitions and Interpretation

(a) Capitalized terms below will have the meanings set out below:

(i) **Contracted Processor**: The Service Provider or a Subprocessor;

(ii) **Syncron's Data**: Personal Data that is processed on behalf of Syncron (or of an affiliate of Syncron acting as a Controller or Processor) by a Contracted Processor in relation with the Principal Agreement;

(iii) **Data Protection Laws**: (1) GDPR and laws implementing or supplementing the GDPR, (2) European Union or Member State laws with respect to any Syncron's Data in respect of which Syncron is subject to EU Data Protection Laws, and (3) to the extent applicable, any other data protection or privacy laws of any other country;

(iv) **Executive Annex**: Annex to this DPA referring to Services, containing description of data processing under the DPA (Annex 1 as stated in Standard Contractual Clauses);

(v) **GDPR**: the EU Regulation (EU) 2016/679;

(vi) **Processor Clauses** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; or any document that replaces these clauses; the Standard Contractual Clauses are deemed to be amended from time to time to reflect any change made in accordance with Data Protection Laws as applicable by (i) the EU Commission to or of the equivalent contractual clauses approved by the EU Commission under the GDPR (in the case of the Data Protection Laws of the European Union or a member state); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another jurisdiction.

(vii) **Restricted Transfer** means a transfer of Syncron's Data from Syncron to a Contracted Processor or an onward transfer of Syncron's Data from a Contracted Processor to another Contracted Processor, or between two establishments of a Contracted Processor; in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses to be established under section 10 below;

(viii) **Subprocessor**: any person (other than an employee of the Service Provider or of any of its sub-contractors) appointed by or on behalf of the Service Provider to process Syncron's Data on behalf Syncron in connection with the Principal Agreement and these Terms;

(ix) **Syncron:** means the Syncron entity that is a party to this DPA, mentioned in Schedule 3, being Syncron Sweden AB, a company registered in Sweden, Syncron UK Ltd, a company registered in England and Wales, Syncron Germany GmbH, a company registered in Germany, Syncron Software India Private Limited, a company registered in Karnataka, India; Syncron Italy s. a r.l., a company registered in Italy, Syncron Poland sp. z o.o. company registered in Poland, Syncron Japan Corp., a company incorporated in Japan, Syncron Inc., a company incorporated in Illinois, Syncron France SAS, a company registered in France, Mize Inc., a company incorporated in Delaware, or Mize Software Solutions Private Limited, a company registered in Telangana, India; Syncron AB, a company registered in Sweden, as applicable.

(x) **Terms**: this DPA.

The terms **Controller**, **Data Subject**, **Member State**, **Personal Data**, **Personal Data Breach**, **Processing** (or **processing**) and **Supervisory Authority** will have the same meaning as in the GDPR (or, where the GDPR does not apply, other applicable Data Protection Laws).

2. Processing of Syncron's Data

(a) The Service Provider will process Syncron's Data solely on behalf of and for the benefit of Syncron. For purposes of this DPA, Syncron and the Service Provider agree that Syncron will generally act as a Controller and the Service Provider, as a Processor. Service Provider will process Syncron's Data only so far as necessary to perform its services or activities under the Principal Agreement. Due to the nature of use of Service Provider's services by Syncron, in relation to some personal data put into the services, Syncron may also act as a processor (personal data of Syncron's applications end users) before its customers, and Service Provider as Syncron's subprocessor.

Terms of this DPA will apply accordingly to the situations when Syncron acts as a processor (before its customers) and Service Provider as its subprocessor.

(b) Syncron will have the right to give binding instructions to the Service Provider for all processing of Syncron's Data by or on behalf of the Service Provider. Instructions must be given in writing (including by e-mail). Instructions may be changed, updated or replaced at any time in the same form.

(c) The Service Provider will:

(i) comply with all **Data Protection Laws** in the processing of Syncron's Data, including with all applicable documentation obligations; and

(ii) not process Syncron's Data other than on Syncron's documented instructions unless processing is required by **Data Protection Laws**, in which case the Service Provider will, to the extent permitted by **Data Protection Laws**, inform Syncron of that legal requirement before the relevant processing of that Personal Data.

(d) Where the Service Provider is required to process Syncron's Data under **Data Protection Laws**, the Service Provider will inform Syncron accordingly in writing before such processing unless prohibited by law. Where the Service Provider believes that compliance with an instruction given by Syncron would result in a violation of **Data Protection Laws**, the Service Provider will notify Syncron thereof without delay.

(e) Syncron hereby instructs the Service Provider (and authorises the Service Provider to instruct each Subprocessor) to Process Syncron's Data and transfer Syncron's Data to any country or territory if and to the extent required under the Principal Agreement and as far as such processing and/or transfer is in conformance with this DPA.

(f) In order for this DPA to be effective, Parties shall execute an Executive Annex, draft of which constitutes Schedule 3 to this DPA. Processing of personal data on behalf of Syncron shall take place only if Executive Annex is concluded between the Parties. Executive Annex shall govern the details of processing carried out by the Service Provider on behalf of Syncron, in particular the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, subprocessors acting on behalf of Service Provider, Restricted Transfer.

3. Confidentiality; Service Provider Personnel

(a) The Service Provider will keep and maintain all Syncron's Data in strict confidence, using such degree of care as it is appropriate to avoid unauthorized access, use or disclosure.

(b) The Service Provider will take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Syncron's Data, ensuring in each case that access is strictly limited to those individuals who need to know and/or access the relevant Syncron's Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with **Data Protection Laws** in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

(c) The Service Provider shall ensure that its personnel engaged in the Processing of Syncron's Data are informed of the confidential nature of the Syncron's Data, have received appropriate training on their responsibilities and have executed confidentiality undertakings. The Service Provider shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4. Security

(a) The Service Provider has implemented and maintains appropriate technical and organizational measures to ensure a level of security in relation to the Syncron's Data appropriate to the risk. Without limitation to the foregoing, the Service Provider will, if applicable, implement (i) the measures indicated in the Principal Agreement and (ii) set out or referred to in Schedule 2.

(b) The Service Provider will maintain a working process to review, assess and evaluate the effectivity of the technical and organizational measures on a regular basis to ensure appropriate security of Syncron's Data.

5. Subprocessing

(a) Syncron authorises the Service Provider to appoint Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

(b) Before appointing a new Subprocessor, subject to section 5(c), the Service Provider will give Syncron prior written notice (to be sent to privacy@syncron.com) including full details of the processing to be undertaken by the

Subprocessor. If, within two weeks of receipt of that notice, Syncron notifies the Service Provider in writing of any objections (on reasonable grounds) to the proposed appointment, the Service Provider will not appoint (nor disclose any Syncron's Data to) the proposed Subprocessor except with the prior written consent of Syncron.

(c) Without limitation to section 5(d), the Service Provider may appoint (or may continue to use, as applicable) the Subprocessors listed in Schedule 3.

(d) With respect to each Subprocessor, the Service Provider will:

(i) before the Subprocessor first has access to Syncron's Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Syncron's Data required by the Principal Agreement;

(ii) ensure that the arrangement with the Subprocessor is governed by a written contract including terms that offer at least the same level of protection for Syncron's Data as those set out in these Terms and meet the requirements of applicable Data Protection Laws;

(iii) if that arrangement involves a Restricted Transfer, ensure that the Processor Clauses as from time to time available are incorporated into the agreement with the Subprocessor, or before the Subprocessor first processes Syncron's Data procure that it enters into an agreement Processor Clauses with Syncron; and

(iv) provide to Syncron for review such copies of the agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of the DPA) as Syncron may request from time to time.

(v) The Service Provider will ensure that each subprocessor performs its obligations as they would apply to the processing of Syncron's Data by the Service Provider, as if it were party to the DPA in place of the Service Provider. The Service Provider remains responsible at all times for compliance with the terms of this its subprocessors to the same extent it would be liable if performing the services /activities of each sub-processor directly under the terms of this DPA.

6. Data Subject Rights; Cooperation

(a) The Service Provider will reasonably assist Syncron to respond to requests to exercise Data Subject rights under the Data Protection Laws (including those stipulated under articles 15 to 22 of the GDPR). The Service Provider will:

(i) promptly notify Syncron if any Contracted Processor receives a request from a Data Subject (e.g. a request to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing), in respect of Syncron's Data; and

(ii) ensure that the Contracted Processor does not respond to that request except on the documented instructions of Syncron or as required by **Data Protection Laws**, in which case the Service Provider will inform Syncron of that legal requirement beforehand.

(b) In relation to processing of Syncron's Data by the Contracted Processor, the Service Provider will provide reasonable assistance to Syncron with any data protection impact assessments and prior consultations with Supervising Authorities or other competent data privacy authorities that Syncron reasonably considers to be required under applicable Data Protection Laws.

(c) The Service Provider will inform Syncron without delay, to the extent permitted by **Data Protection Laws**, (i) in the event that a Supervisory Authority addresses the Service Provider directly in a matter related with the Contracted Processor's Processing of Syncron's Data, and (ii) in the event that any Syncron's Data is or is at risk to be affected by a seizure, bankruptcy proceedings or other similar events and will inform any third party (including authorities) involved in relevant measures that the control over the Syncron's Data is with Syncron.

7. Personal Data Breach

(a) The Service Provider will notify Syncron immediately upon the Contracted Processor becoming aware of a Personal Data Breach affecting Syncron's Data, providing Syncron with sufficient information to allow Syncron to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. The Service Provider shall make reasonable efforts to identify the cause of such incident and take those steps as it deems necessary and reasonable in order to remediate the cause of such incident to the extent the remediation is within its reasonable control.

(b) The Service Provider will cooperate with Syncron and take such reasonable steps as are directed by Syncron to assist in the investigation, mitigation and remediation of each such Personal Data Breach. The Service Provider agrees (i) that it will not inform any third party of any Personal Data Breach without first obtaining Syncron's prior written consent, except as required by applicable law; and (ii) that Syncron will have the sole right to determine whether notice of the Personal Data Breach is to be provided to any individuals, Supervisory Authority or other parties as required by **Data Protection Laws** or otherwise in Syncron's discretion.

8. Term and Termination; Deletion or Return of Syncron's Data

(a) Subject to sections 8(b) and 8(c), and without limitation to the right to give instructions under section 2(b), the Service Provider will promptly and in any event within four weeks of the date of cessation of any services/activities involving the processing of Syncron's Data (the **Cessation Date**), delete and procure the deletion of all copies of those Syncron's Data.

(b) Subject to section 8(c), Syncron may in its discretion by written notice to the Service Provider within two weeks of the Cessation Date require the Service Provider to

(i) return a complete copy of all Syncron's Data to Syncron by secure file transfer in a format reasonably requested by Syncron; and

(ii) delete and procure the deletion of all other copies of Syncron's Data Processed by any Contracted Processor. The Service Provider will comply with any such written request within four weeks of the Cessation Date.

(c) The Service Provider will provide written certification to Syncron that the Service Provider has complied with this section 8 within three weeks of the Cessation Date.

9. Audit Rights

(a) Subject to section 9(b), the Service Provider will make available to Syncron on request all information necessary to demonstrate compliance with the DPA, and will allow for and contribute to audits (including inspections) by Syncron or an auditor mandated by Syncron in relation to the processing of the Syncron's Data by the Contracted Processor. Audits will be carried out after prior announcement during normal business hours and without disruption to the Service Provider's business operations. Syncron will treat the information provided by the Service Provider as confidential information.

(b) Information and audit rights of Syncron only arise under section 9(a) to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.

10. Restricted Transfers

(a) Transfer of Syncron's Data from Syncron to the Service Provider is made subject to this DPA and standard contractual clauses with Syncron acting as the "data exporter" and the Service Provider acting as the "data importer". Clauses constitute integral part of this DPA and prevail over it in case of any discrepancies. Whenever the transfer between Syncron and the Service Provider is seen as a Restricted Transfer, the clauses shall apply. The parties will indicate in Schedule 3 which module of clauses is applicable.

(b) In case the Service Provider will engage a Subprocessor and such transfer to a subprocessor would be seen as Restricted Transfer, the Service Provider shall include the applicable standard contractual clauses in the agreement with the Sub processor.

(c) The Processor Clauses will come into effect on the date of signing of this Schedule 3.

(d) This section applies, if pursuant to the Executive Annex the transfer between Syncron and the Service Provider is seen as a Restricted Transfer.

11. Liability; Indemnity

(a) Processor shall be liable for any damages (direct or indirect) arising from processor's acts or omissions in complying with this DPA, Processor Clauses or with Data Protection Laws.

(b) Notwithstanding anything agreed in the Principal Agreement, the Service Provider will defend, indemnify and hold harmless Syncron and Syncron's affiliates and their respective officers, directors, employees, agents and contractors (each a **Syncron Party**) against all damages of whatever nature (including losses, liabilities, fines and costs), including reasonable attorneys' fees, arising from a third-party claim against any Syncron Party in relation with the Service Provider's breach of any of its obligations under the DPA.

12. Order of Precedence

(a) Nothing in this DPA reduces the Service Provider's obligations under the Principal Agreement in relation to the protection of Personal Data or permits the Service Provider to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement.

(b) With regard to the subject matter of this DPA, in the event of inconsistencies between this DPA and any other agreement between the Parties, including the Principal Agreement and including (except where expressly agreed otherwise) agreements entered into or purported to be entered into after the date of this DPA, the provisions of the DPA will prevail, subject to section 12(c) below.

(c) In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

(d) In the event of any conflict or inconsistency between this DPA and the Executive Annex, the Executive Annex shall prevail.

(e)

13. Miscellaneous

(a) Syncron may:

(i) by at least 30 calendar days' written notice to the Service Provider make any variations to the Principal Agreement and/or to the DPA that are required as a result of any change in applicable Data Protection Laws or decision of a competent authority, and

(ii) propose any other variations to the DPA which Syncron reasonably considers to be necessary to address the requirements of any Data Protection Laws, in which case the Parties will promptly and expeditiously discuss the proposed variations.

(b) The applicable law and jurisdiction clauses in the Principal Agreement will apply, without prejudice to anything agreed in the Processor Clauses, provided, however, that this section 13 will not affect Syncron's right

(i) to seek an injunction, interim relief or other provisional measure before any competent court of jurisdiction as is considered appropriate; and

(ii) to bring a claim against the Service Provider in third party proceedings involving Syncron as permitted under applicable procedural law.

(c) This DPA supersedes any and all prior agreements, promises and correspondence, either oral or written, between the Parties with respect to the processing of personal data, except for such agreements, promises and correspondence expressly embodied in this DPA. Accordingly, all information and data contained in general product documentation and price lists, whether in electronic or any other form, are binding only to the extent they are by reference expressly included in the Contract.

(d) If any provision of this DPA shall be held invalid or unenforceable, either partially or wholly, the remainder of this DPA will not be affected thereby and will continue to be in full force and effect. Furthermore, the Parties will jointly seek an agreement having a legal and economic effect as similar as possible to the invalid or unenforceable provision.

<u>On behalf of Service Provider</u>

Service Provider's acceptance of the Schedule 3 shall constitute its agreement to this DPA and its Schedules.

<u>On behalf of Syncron</u>

Syncron's acceptance of the Schedule 3 shall constitute its agreement to this DPA and its Schedules.

Schedule 1: Standard Contractual Clauses

[*These Standard Contractual Clauses shall take effect upon signing of the Schedule 3 by the Parties.*

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement)of these Clauses (or any equivalent thereof) made in accordance with those Data Protection Laws by the Commission or an equivalent competent authority.]

MODULE TWO: Transfer controller to processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)1 for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex 1.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 1.A (hereinafter each “data importer”).

have agreed to these standard data protection clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.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 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 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 (Schedule 2 of this DPA) 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 (Schedule 2 of this DPA). The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 14 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. 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 subprocessor 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 subprocessor 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

(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 (Schedule 2 of this DPA) the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage. (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

[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;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where: (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension; (ii) the data importer is in substantial or persistent breach of these Clauses; or (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Agreement.

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 EU Member State which law governs the Agreement (or other underlying agreement) between the Parties.

(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.

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(a) 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")

(iii) have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

(c) 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 Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

(iv) Clause 12 - 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

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 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[2].

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[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 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

(a) 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 14 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.[4] 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

(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

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

[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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and

proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the 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). 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, 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 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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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.

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.). 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. 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 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) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Sweden.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Sweden.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Schedule 2: Technical and Organizational Measures

This Appendix forms part of the DPA.

In order to ensure a level of security in relation to the Syncron's Data appropriate to the risk, and without prejudice to any measures indicated in the Principal Agreement (if applicable), the Service Provider will implement at least the following technical and organizational measures:

Data Access

- Security of Premises
  - Access control to premises and facilities by a badge, whereby sensitive areas are only accessible with an additional identification
  - Engage Security Staff
  - Lock offices outside working hours
  - Install alarm system that is activated outside working hours
- Server Room Security
  - Limit number of persons with access
  - Keep a log of all access to server room
  - Install an alarm system that is continuously in action
- Workplace Security
  - Monitors cannot be seen from the door
  - Don't leave printed documents unattended near the printer
  - Lock away printed documents and sensitive objects in the evening
  - Virus scanner on each PC
- Identification and Authentication
  - User account only used by one person.
  - Different applications need a renewed authentication
  - Use strong passwords that are changed regularly
- Data Access
  - Users have differentiated access permission to the IT system
  - Access permission matrix used to define each access permission
  - Authentication needed every time the system is switched on
  - Keep a log of all access to the system
- Access from outside the Organization
  - Secure access for persons who access data from outside the organization
  - Two elements for authentication used
  - Personal computers protected with a firewall
  - Keep a log of all access

Data Life Cycle

- Data Input
  - Data only captured by trained and authorized persons
  - Helpful data entry mechanisms installed
  - As far as possible only fictional or anonymized data used in tests
  - Keep a log of data input
- Logging
  - Set of clearly described criteria for logging mechanism
  - Content and storage duration of log files defined in relation to the data and processing taking place
  - Persons informed that traces will be stored of every action
  - Data files resulting from the logging process kept secure
  - Access rights to log files clearly defined and limited to specific functions in the organisation
  - Logging mechanism protected from attacks and unauthorized access
- Pseudonymization and Anonymization
  - Data anonymized if possible; otherwise work with pseudonymized data; if neither anonymized nor pseudonymized data is possible store sensitive personal data in encrypted form
  - No indirectly identifying information is processed if data is pseudonymized or anonymized
- Encryption
  - Encryption algorithm and the length of the key proportionate to the data sensitivity level
  - Keep encryption keys secure
  - Give only limited number of employees access to the keys
- Security of storage media
  - Train staff about risks associated with connecting an unknown external storage medium to the PC
  - Encrypt external storage media that contain sensitive personal data or sensitive customer data
  - Keep external storage media under lock and key
  - Set up a process for the destruction of storage media
- Data Backup
  - Define backup strategy based on the data and its quantity and change frequency
  - Inform staff about the backup strategy
  - Secure backup servers with same security measures as the central servers

- Specially train persons entrusted with restoring data
- Data Destruction
  - Destroy data on paper in document shredder
  - Physically and irretrievably delete data on rewritable storage media by means of special programs
- Outsourcing of tasks
  - Oblige suppliers to adhere to our standards
  - Check regularly it the data protection conditions are being observed
  - Safeguard the security of the data transfer to the supplier

Data Exchange

- Network Security
  - Keep the data transfer from the intranet to the outside world via the internet to the absolute minimum
  - Consider using Transport Layer Security protocol (LTS)
  - Set up VPN connection to access the system from outside
- Message Encryption
  - Determine the most suitable type of encryption (symmetrical or asymmetrical)
  - Symmetrical encryption: use a secure protocol for transmitting the key
  - Asymmetrical encryption: set up encryption measures
- Handovers of Storage Media
  - Make sure that recipients of mobile storage media can be securely authenticated
  - Pack mobile storage media securely before transporting them
  - Encrypt mobile storage media
  - Define the transport process for mobile storage media
  - Use dual control to ensure that the data is correctly handed over and received
- Data Exchange Logging
  - Clear description of how the sender and the recipient, the route followed by the data, and all the important points along the data route are to be logged
  - Preferably entrust the transfer of mobile storage media to the same employee each time
  - Make sure the data exchange logs adhere to the principle of proportionality in terms of volume, duration etc

Right to Information

- Data Subject's rights
  - Clear information is available to the data subjects and they are informed of their rights
  - Processes for dealing with information requests are set up and announced to the staff
  - System is equipped with reliable search mechanism
  - Process to change, correct, block or destroy data is reliable and documented
  - Log every processing activity
- Reproducibility of the Processes
  - Program the functions enabling the data subjects to exercise the right to information into the system
  - All staff should use the same procedure
  - Regulatory authority is able to check the system's built-in procedure

Schedule 3: Draft Executive Annex

Executive Annex to the DPA

Description of data processing

Whereas Syncron and the Service Provider have entered into Data Processing Addendum, hereby the Parties agree that the entrustment of the processing of personal data by Syncron to the Service Provider shall be as follows:

A. LIST OF PARTIES

Data exporter:

Syncron as described in the Principal Agreement, e.i. ……

Activities relevant to the data transferred under the Clauses: fulfilment of Services pursuant to the Principal Agreement

Role (controller/~~processor~~)

Data importer:

Service Provider as described in the Principal Agreement, e.i. ……..

Activities relevant to the data transferred under the Clauses: fulfilment of Services pursuant to the Principal Agreement

Role (~~controller~~/processor)

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data is transferred:

[to be completed each time, e.g. Syncron staff, Customer representatives, Syncron customers' end users of Syncron SaaS Solution]

Categories of personal data transferred:

[to be completed each time, e.g. Syncron staff business contact information, Customer representatives business contact information, Syncron Customers' end user SaaS Solution account-related information and business contact information]

The frequency of the transfer: the data is transferred on a continuous basis throughout the term pursuant to the Principal Agreement.

Nature of the processing: *[to be completed each time, e.g. data will be processed automatically]*

Processing activities may include but are not limited to: *[to be completed each time, e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and other activities that may be necessary to provide Services pursuant to the Principal Agreement.]*

Purpose(s) of the data transfer and further processing:[Service description]

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

Term of the Principal Agreement and up to 30 days after its termination or expiration.

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

as specified in the Schedule 3 of the DPA.

Restricted transfer (please specify countries outside EEA to which personal data will be transferred to): *[to be completed each time, e.g. USA, UK].*

Module of the standard contractual clauses

Module 2 – Controller to Processor

Module 3 – Processor to Processor

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: supervisory authority applicable to the EU member state law indicated in DPA.

D. LIST OF AUTHORIZED SUBPROCESSORS

The Service Provider may appoint or continue to use, as applicable, the following Subprocessors, in accordance with Sec. 5 (c), of the DPA, for the following services/purposes:

[Please specify if you use any subprocessors; please list all third-party entities which may access data disclosed by Syncron. As per GDPR, we need to have a control over personal data which we are responsible for. Please note that Affiliates are also subprocessors.]

Name	**Address**	**Purpose of use/services provided by Subprocessor**	**Types of personal data processed by Subprocessor**
Third Party Sub-processors (as applicable):			

E. Contact details

For purposes of performance of this Executive Annex, the Parties designate contact persons:

For Syncron: Data Protection Officer, e-mail: privacy@syncron.com

For Service Provider: [to be completed]

For Syncron	**For Service Provider**
Syncron's acceptance of the DPA and this Executive Annex shall constitute its agreement to enter into and be bound by this Annex.	Service Provider's acceptance of the DPA and this Executive Annex shall constitute its agreement to enter into and be bound by this Annex.
Name: ……	Name: ……
Date: ……..	Date: ……..