**EU STANDARD CONTRACTUAL CLAUSES**

**Module One: Transfer controller to controller &**

**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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter **"entity/ies"**) transferring the personal data, as listed in Annex I.A. (hereinafter each **"data exporter"**), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each **"data importer"**).

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

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

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

**Clause 2: Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

**Clause 3: Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two: 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 and Two: 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.

**MODULE ONE: Transfer controller to controller**

**8.1 Purpose limitation**

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

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

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

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

**8.2 Transparency**

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

**8.5 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter **"personal data breach"**). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter **"sensitive data"**), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter **"onward transfer"**) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

**8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

**8.9 Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

**Module Two: Transfer controller to processor**

**8.1 Instructions**

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

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

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

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

**8.4 Accuracy**

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

**8.5 Duration of processing and erasure or return of data**

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

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter **"personal data breach"**). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

**8.7 Sensitive data**

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

**8.8 Onward transfers**

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

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

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

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

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

**8.9 Documentation and compliance**

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

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

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

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

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

**Clause 9: Use of sub-processors**

**MODULE TWO: Transfer controller to processor**

(a) *OPTION 1: SPECIFIC PRIOR AUTHORISATION* *applies unless the data exporter has separately agreed in writing that OPTION 2 below applies*: The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

*OPTION 2: GENERAL WRITTEN AUTHORISATION applies only if the data exporter has separately agreed in writing that this OPTION 2 applies:* The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

**Clause 10: Data subject rights**

**MODULE ONE: Transfer controller to controller**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter **"automated decision"**), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

**Module Two: Transfer controller to processor**

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

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

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

**Clause 11: Redress**

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

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

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

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

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

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

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

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

**Clause 12: Liability**

**Module One: Transfer controller to controller**

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

**Module Two: Transfer controller to processor**

(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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

**Clause 18: Choice of forum and jurisdiction**

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

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

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

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

**APPENDIX**

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporters**:

| **Name** | **Address** | **Role** | **Contact** | **Activities** |
| --- | --- | --- | --- | --- |
| **Mayer Brown SELAS** | 10 avenue Hoche, 75008 Paris, France | Controller | privacy@mayerbrown.com | Recipient of goods and/or services from the data importer, as agreed between the parties in writing (the **"Agreement"**) |
| **Mayer Brown Europe-Brussels LLP** | Avenue des Arts 52, B – 1000 Brussels, Belgium | Controller | privacy@mayerbrown.com | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown LLP** | *Registered address*: 71 South Wacker Drive Chicago, IL 60606-4637, Illinois, USA*EU establishment*: Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germany | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown International LLP** | 201 Bishopsgate, London EC2M 3AF, United Kingdom | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown** | 16th - 19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown (Singapore) Pte Ltd** | 6 Battery Road, #10-01, 049909, Singapore | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown (Vietnam) LLC** | 17th Floor, Saigon Tower, 29 Le Duan Street, District 1, Ho Chi Minh City, Vietnam | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Tauil & Chequer Advogados** | *Of:*SCS Quadra 9, Bloco A, Torre B, Salas 503/504, Ed. Parque Cidade Corporate, Brasília, DF 70.308-200, BrazilAv. Nossa Senhora dos Navegantes, 451 - suite 1703 - 17th floor, 29050-335, Vitória – ES, BrazilAv. Juscelino Kubitschek, 1455, 5º, 6º e 7º Andares, Vila Nova Conceição, São Paulo, SP 04543-011, Brazil​Av. Oscar Niemeyer 2000, 15º Andar, Ed. Aqwa Corporate​​​​, Rio de Janeiro, RJ 20.220-297, Brazil | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown Mexico, S.C.** | Goldsmith 53, Piso 3, Polanco III Seccion, C.P. 11560, Miguel Hidalgo, CDMX, Mexico | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown Dubai** | Index Tower, Dubai International Finance Centre, Floor 11, Unit 1108, PO Box 507115, Dubai, UAE | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown Gaikokuho Jimu Bengoshi Jimusho** | Marunouchi Kitaguchi Building, 12th Floor, 1-6-5 Marunouchi, Chiyoda-ku, Tokyo, 100-0005, Japan | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown Representative Office (Shanghai)** | Suite 4710, Tower I, Plaza 66, 1266 Nan Jing Road West, Shanghai 200040, PRC | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown Representative Office (Beijing)** | Suite 1102, Tower 2, China Central Place, 79 Jianguo Road, Chaoyang District, Beijing 100025, PRC | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |
| **Mayer Brown (Beijing) Intellectual Property Agency Co. Ltd.** | Suite 1102, Tower 2, China Central Place, 79 Jianguo Road, Chaoyang District, Beijing 100025, PRC | Controller | *EU Representative*: Mayer Brown LLP, Friedrich-Ebert-Anlage 35-37, 60327, Frankfurt am Main, Germanyprivacy@mayerbrown.comT +49 69 7941 0 | Recipient of goods and/or services as set out in the Agreement |

**Data importer(s):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address** | **Role** | **Contact** | **Activities** |
| The entity or entities set out in the Agreement | As set out in the Agreement | Controller / Processor as set out in the Agreement | As set out in the Agreement | Provider of goods and/or services to the data exporters, as agreed in the Agreement |

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

* the Data Exporter's personnel (and job applicants) and any associated individuals such as dependents or beneficiaries;
* third parties who have provided their personal data to the Data Exporter(s) through websites and other online or digital media applications or in the normal course of business;
* the Data Exporter's clients and associated personnel; or
* third parties connected with legal services being provided by the Data Exporter(s).

*Categories of personal data transferred*

* personal data of the client's personnel (and job applicants) generated in the normal course of recruitment or human resources administration; or
* personal data of third parties generated or received in the normal course of the Data Exporter's business

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

* Special categories of personal data as defined in Regulation (EU) 2016/679, relevant to the nature of the goods and/or services provided by the Data Importer(s).

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

* As required for the purposes of the Data Importer(s) providing the goods and/or services to the Data Exporter(s), as agreed between the Parties.

*Nature of the processing*

* The personal data transferred will be subject to the processing activities that form part of the goods and/or services provided by the Data Importer(s) to the Data Exporter(s), as agreed between the Parties.

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

* For the purposes of the Data Importer(s) providing the goods and/or services to the Data Exporter(s), as agreed between the Parties.

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

* As required for the purposes of the Data Importer(s) providing the goods and/or services to the Data Exporter(s), as agreed between the Parties.

**C. COMPETENT SUPERVISORY AUTHORITY**

|  |  |
| --- | --- |
| **Data exporter** | **Supervisory authority** |
| **Mayer Brown SELAS** | France (CNIL) |
| **Mayer Brown Europe-Brussels LLP** | Belgium (Data Protection Authority) |
| **All other data exporter entities** | Germany (Hessen Commissioner for Data Protection and Freedom of Information) |

**ANNEX II:**

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

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

* An assessment of the security such that appropriate consideration shall be taken of all the risks that are presented by processing;
* Pseudonymisation and encryption of personal data;
* The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
* The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
* Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and
* Such other measures that are appropriate for processing of the personal data that the data importer(s) are processing under these Clauses (taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons).

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

* An assessment of the security such that appropriate consideration shall be taken of all the risks that are presented by processing;
* Pseudonymisation and encryption of personal data;
* The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
* The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
* Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and
* Such other measures that are appropriate to processing of the personal data that the sub-processor(s) are processing under or in connection with these Clauses (taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons).

**ANNEX III:**

**List of sub-processors**

**Module Two: Transfer controller to processor**

The data exporter has not authorised the data importer to use any sub-processors under these Clauses unless:

* the data exporter has separately agreed in writing to give the data importer a general written authorisation under Clause 9(a) Option 2; or
* the data exporter has separately agreed in writing to authorise specific sub-processors for use by the data importer and the data importer has provided the data exporter with the following details in relation to each such sub-processor:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Contact person's name, position and contact details** | **Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)** |
|  |  |  |  |

**Annex IV:**

**UK ADDENDUM TO EU STANDARD CONTRACTUAL CLAUSES**

**Part 1: Tables**

**Table 1: Parties**

|  |  |
| --- | --- |
| **Start date** | As set out in the Agreement  |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' Details**  | **Mayer Brown International LLP**201 Bishopsgate, London EC2M 3AF, United Kingdom**Mayer Brown SELAS**10 avenue Hoche, 75008 Paris, France**Mayer Brown Europe-Brussels LLP**Avenue des Arts 52, B – 1000 Brussels, Belgium**Mayer Brown LLP**71 South Wacker Drive Chicago, IL 60606-4637, USA**Mayer Brown**16th - 19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong**Mayer Brown (Singapore) Pte Ltd**6 Battery Road, #10-01, 049909, Singapore**Mayer Brown (Vietnam) LLC**17th Floor, Saigon Tower, 29 Le Duan Street, District 1, Ho Chi Minh City, Vietnam**Tauil & Chequer Advogados**,*of*:1. SCS Quadra 9, Bloco A, Torre B, Salas 503/504, Ed. Parque Cidade Corporate, Brasília, DF 70.308-200, Brazil
2. Av. Nossa Senhora dos Navegantes, 451 - suite 1703 - 17th floor, 29050-335, Vitória – ES, Brazil
3. Av. Juscelino Kubitschek, 1455, 5º, 6º e 7º Andares, Vila Nova Conceição, São Paulo, SP 04543-011, Brazil​
4. Av. Oscar Niemeyer 2000, 15º Andar, Ed. Aqwa Corporate, Rio de Janeiro, RJ 20.220-297, Brazil

**Mayer Brown Mexico, S.C.**Goldsmith 53, Piso 3, Polanco III Seccion, C.P. 11560, Miguel Hidalgo, CDMX, Mexico**Mayer Brown Dubai**Index Tower, Dubai International Finance Centre, Floor 11, Unit 1108, PO Box 507115, Dubai, UAE**Mayer Brown Gaikokuho Jimu Bengoshi Jimusho**Marunouchi Kitaguchi Building, 12th Floor, 1-6-5 Marunouchi, Chiyoda-ku, Tokyo, 100-0005, Japan**Mayer Brown Representative Office (Shanghai)**Suite 4710, Tower I, Plaza 66, 1266 Nan Jing Road West, Shanghai 200040, PRC**Mayer Brown Representative Office (Beijing)**Suite 1102, Tower 2, China Central Place, 79 Jianguo Road, Chaoyang District, Beijing 100025, PRC**Mayer Brown (Beijing) Intellectual Property Agency Co. Ltd.**Suite 1102, Tower 2, China Central Place, 79 Jianguo Road, Chaoyang District, Beijing 100025, PRC | As set out in the Agreement |
| **Key Contacts** | privacy@mayerbrown.comMark Prinsley, Data Protection Officer, mprinsley@mayerbrown.com | As set out in the Agreement |

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

|  |  |
| --- | --- |
| **"Addendum EU SCCs"** | The version of the Approved EU SCCs which this Addendum is appended to, including the Appendix Information. |

**Table 3: Appendix Information**

**"Appendix Information"** means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

|  |
| --- |
| Annex 1A: List of Parties: Annex I.A |
| Annex 1B: Description of Transfer: Annex I.B |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II |
| Annex III: List of Sub processors: Annex III (Module Two only) |

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

|  |  |
| --- | --- |
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section ‎19:[ ]  Importer[x]  Exporter[ ]  neither Party |

**Part 2: Mandatory Clauses**

|  |  |
| --- | --- |
| **"Mandatory Clauses"**  | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. |