GPTW Cross-Border Transfer Mechanisms

Last updated: November 2026

Table of Contents

1. ANNEX I.A. – EU COMMISSION PROCESSOR TO PROCESSOR SCCS 2
2. ANNEX I.B. – UK PROCESSOR TO PROCESSOR DATA PROTECTION CLAUSES 17
3. ANNEX I.C. – EU COMMISSION CONTROLLER TO PROCESSOR SCCS 23
4. ANNEX I.D. – UK CONTROLLER TO PROCESSOR DATA PROTECTION CLAUSES 36
5. ANNEX I.E. – SWISS ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES 42
6. ANNEX I.F. – BRAZILIAN STANDARD CONTRACTUAL CLAUSES 44

1. Annex I.A. – EU Commission Processor to Processor SCCs

Standard Contractual Clauses

MODULE THREE

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 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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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:

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

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

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

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

(vi) Clause 13;

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

(viii) Clause 16(e);

(ix) 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 the accession agreement (Annex 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 shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.[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 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. 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).

2 See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

GPTW Public Information - Proprietary

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 Onwards 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[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

3 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(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 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s) under the conditions as described in the applicable data processing addendum or any other agreement replacing or supplementing it.

(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

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

GPTW Public Information - Proprietary

(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 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;[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

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

5 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 EEA Data Exporter, as respectively specified in Schedule 1.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of the EEA Data Exporter, as respectively specified in Annex 1.

(b) The Parties agree that those shall be the courts of the EEA Data Exporter, as respectively specified in Schedule 1.

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

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

ANNEX I

A. LIST OF PARTIES

List of Exporting Parties: Refer to GPTW List of Affiliates located in the European Union.

List of Importing Parties: Great Place to Work Institute, Inc.

B. DESCRIPTION OF TRANSFERS

- The data exporter engages the data importer as a further processor in accordance with each Customers', Suppliers' and any other End Users' Agreement.
- Signature and date: The parties agree that accession to the Intra-Group Data Processing Agreement (IDTA) by the data exporter shall constitute execution of these Clauses by both parties (a) as of 27 September 2021, where the accession date of the data exporter is on or before 27 September 2021, or (b) otherwise, as of the accession date of the data exporter.

Data subjects

The personal data transferred concern the following categories of data subjects:

Past, present, and prospective consumer customers of the Data Exporter and past, present, and prospective staff and any individual users of any GPTW product or service of the Data Exporter's corporate or business customers or partners or vendors or suppliers (including, volunteers, agents, independent contractors, interns, temporary and casual workers of corporate or

business customers or partners or vendors or suppliers) ("Customers and Suppliers"); and
Visitors to websites owned and operated by GPTW including from the categories above and job applicants ("Other End Users").

Purposes of the transfer(s)

The transfer is made for the following purposes:

- to carry out the Data Processing Activities related to:

    - The provision, management and administration of products and services including the administration of orders and accounts, including processing payments and provisioning access and licenses; product management; business development; marketing, advertising and public relations; customer relationship management including satisfaction surveys, customer claims and after sales service; and other activities for the conduct of business activities.

    - The management and administration of customer relationships including but not limited to: the management and administration of accounts; contracting with customers; statistics and data analytics; customer support and customer service. Data may include information necessary to provide the information security services, including but not limited to scanned files, information about customer endpoints, traffic, activities, computer, other devices. Data may also include usage information for the purposes of supporting the provision of services and for data monetization.

    - The administration, maintenance, performance and functionality of GPTW websites, intranets, portals, and applications; the provision of services through GPTW websites; web analytics; and other processing necessary for the conduct of business activities.

    - The management and administration of purchased products and services including but not limited to the administration of orders and accounts, including processing payments and provisioning access; the selection and vetting of Suppliers; information gathering regarding Suppliers; Supplier relationship management; statistics and data analytics.

Categories of data

The personal data transferred concern the following categories of data:

Customers and Suppliers and Other End Users personal data may include:

- Contact details: first and last name; personal and business contact information such as personal and business email address, personal and business telephone number (including mobile telephone number), facsimile, personal and business address; date of birth, place of birth, nationality, photograph, supplier/customer/client ID.
- Professional details: job title; employer, academic and professional qualifications, data related to transactions involving goods and services.
- Academic and professional qualifications: degrees, titles, skills, language proficiency, training information, employment history, CV/résumé.
- Identifiers: tax ID, government identification number, employer identification number.
- Content: photos, texts, and similar content provided to GPTW for websites, conferences, meetings, and other uses.
- Financial data: bank account number, payment information, bank details.
- IT and Registration data: including first and last name, login/password, affiliated organization, computer ID, user ID and password, domain name, IP address, log files, software and hardware inventory, browser type, software and hardware usage pattern tracking information, clickstream and navigation data; information collected by cookies and other online tracking technologies (such as pages visited, language preferences, etc.), web and email traffic, file names and content, access credentials, cookies, geolocation of devices, and language preferences.
- Lifestyle and timekeeping: punches, hobbies, social activities, holiday preferences.
- Data needed to provide products and services.
- Other data provided by Customers in the course of the customization of GPTW products and services.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients: Those recipients who are involved in the Data Processing Activities.

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

- Only in relation to Licensee conducting international surveys on Emprising involving **Customers based within the United States**, employees of such Customers, at their own discretion, will be given the opportunity to provide information with respect to racial, ethnic origin, religious beliefs, health or sexual orientation.
- GPTW does not anticipate the collection of any sensitive data as a Controller from any individuals other than GPTW Employees in connection with valid employment purposes and with consent of the Data Subject as required.
- Race and ethnicity may appear indirectly on photos and other information available on passports and national IDs, which are necessary to comply with local immigration laws and for Employee travel management. However, race/ethnicity are not Processed purposefully in Europe.
- Health information, including information on specific disability.
- Trade union membership may be collected but only where permitted and for the purposes defined under Information Protection Laws.
- The parties will not export sensitive personal data, unless such export is not otherwise restricted by local data protection laws and any requirements from regulators.
- Other data upon Customers' instructions and provided in the course of the customization of GPTW products and services.

Frequency of the Data Transfers

Continuous basis as required for the purpose of intercompany commercial operations until the data importer deletes it to enable the data exporter to fulfil its obligations pursuant to each Suppliers' and Customers' Agreements.

Nature of the Processing

The data importer will process Customers', Suppliers' and Other End Users' Personal Data to enable the data exporter to fulfil its obligations under each agreement.

Purpose(s) of the data transfer and further processing

- The data importer will process personal data to enable the data exporter to fulfil its obligations under each agreement
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: as provided under applicable data processing agreement.
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: as provided under applicable data processing agreement.

Retention Period

For as long as required for the purpose of intercompany commercial operations. Personal Data for each Customer Agreement may be transferred to the data importer on a continuous basis.

Contact points for data protection enquiries

- privacy@greatplacetowork.com

C. COMPETENT SUPERVISORY AUTHORITY

The relevant and competent supervisory authority is that of the EEA Data Exporter:

Name of the Entity	Address of the Entity*	Country	Data Protection Authority
GPTW GmbH	Nibelungengasse 1-3, Top 50 1010, Vienna Austria	Austria	Österreichische Datenschutzbehörde
Vlerick Business School (Belgium)	c/o Vlerick Leuven Gent Management School Reep 1 BE-9000 Gent Belgium	Belgium	Autorité de Protection des données (ADP)
Great Place to Work (Cyprus) Limited	Great Place To Work® Cyprus 36, Costa Mishiaoulis Street, Kato Deftera 2450, Nicosia, Cyprus	Cyprus	Commissioner for Personal Data Protection
Danmarks Bedste Arbejdspladser A/S	Great Place to Work® Vesterbrogade 149, bygning 12, 3. th. 1620 København V	Denmark	Datatilsynet
GPW Institute Finland Oy	Työpajankatu 3 00580 Helsinki Finland	Finland	Office of the Data Protection Ombudsman
Best Workplaces France S.A.S	1 bis, avenue de la République 75011 Paris France	France	Commission Nationale de l'Informatique et des Libertés - CNIL
GPTW Deutschland GmbH	Hardefuststraße 7 D-50677 Köln Germany	Germany	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Great Place to Work Hellas Private Company	3 Drosini & Tatoiou Str. 14452 Metamorfosi, Attica 14452 Greece	Greece	Hellenic Data Protection Authority
Business Development Systems	Fitzwilliam Hall, Fitzwilliam Place Dublin 2, D02 T292, Ireland	Ireland	Data Protection Commission
Great Place to Work Insititute Italia s.r.l	Viale Andrea Doria, 3 - 20124 Milano Italy	Italy	Garante per la protezione dei dati personali
Great Place to Work Sàrl	63-65 rue de Merl, L-2146 Luxembourg Luxembourg	Luxembourg	Commission Nationale pour la Protection des Données
GPTW Nederland BV	Great Place to Work Nederland Gonnetstraat 26 2011 KA Haarlem The Netherlands	Netherlands	Autoriteit Persoonsgegevens
Great Consulting AS	Rosenkrantz' Gate 7 0159, Oslo Norway	Norway	Datatilsynet
GPTW Institute Polska Sp. z o.o.	Kazimierzowska 43/29 02-572 Warszawa POLAND	Poland	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)
Sperantia, Lda.	Rua Miguel Torga nº2 10ºD 2825-441 Santo António da Caparica Portugal	Portugal	Comissão Nacional de Proteção de Dados - CNPD
Instituto GPTW España SL	Calle Lopez de Hoyos 135, floor 4th, A1, 28002 Madrid, Spain	Spain	Agencia Española de Protección de Datos (AE

Great Place to Work Institue Sverige AB	Arena, Malmskillnadsgatan 36, 111 57 Stockholm, Sweden	Sweden	Integritetsskyddsmyndigheten
GPTW Switzerland AG	GPTW Switzerland AG Schiffbaustrasse 7 8005 Zürich	Switzerland	Datatilsynet
GPTW Switzerland AG	GPTW Switzerland AG Schiffbaustrasse 7 8005 Zürich	Liechtenstein	Data Protection Authority, Principality of Liechtenstein
People Productivity Solutions Inc	Legal Notice Address: Olukunle Malomo, 6030 Marshallee Drive, # 615 Elkridge, MD 21075, USA	Iceland	Persónuvernd

D. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer will implement and maintain security standards at least as protective as those set out in the Data Processing and Security Terms (Customers) (available on www.greatplacetowork.com ("DPA").

The technical and organisational measures to be taken by Subprocessors are at least as protective as those described in the DPA.

The technical and organisational measures taken by the data importer to 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 are equivalent to those described in the DPA coupled with this Module 3.

ANNEX III - LIST OF SUB-PROCESSORS

The controller has authorised the use of sub-processors, which are listed under the agreements executed with its partners, customers and end-users.

2. Annex I.B. – UK Processor to Processor Data Protection Clauses

UK Standard Data Protection Clauses

MODULE THREE

Part 1: Tables

Table 1: Parties

Start Date	September 27, 2021	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See DPA.	See DPA.
Key Contact	privacy@greatplacetowork.com	privacy@greatplacetowork.com
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: 27 September 2021 Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3	x	x	x	General	30 days	
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: See DPA.
Annex 1B: Description of Transfer: See DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.

Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies only to this Addendum and the transfers cite din Schedule 1.

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

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers of UK data as detailed in Schedule 1, the hierarchy in Section 10 will prevail.

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

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

Incorporation of and changes to the EU SCCs

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

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

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs for UK data only, as specified in Schedule 1; and

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

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

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

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made with respect to UK data as detailed in Schedule 1:

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

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

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

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

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

Amendments to this Addendum

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

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

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

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;
c. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

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

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

b. its risk under the Addendum,

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

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

3. Annex I.C. – EU Commission Controller to Processor SCCs

Standard Contractual Clauses

MODULE TWO

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) [6]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 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

6 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

GPTW Public Information - Proprietary

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16 (e);

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

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 (Optional)
Docking clause

(Intentionally Omitted)

SECTION II – OBLIGATIONS OF THE PARTIES

GPTW Public Information - Proprietary

Clause 8

Data Protection Safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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

GPTW Public Information - Proprietary

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 [7](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.

[7] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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 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 under the conditions as described in the applicable data processing addendum or any other agreement replacing or supplementing it.

(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[8]. 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

(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.

8 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

GPTW Public Information - Proprietary

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 effecting 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[9];

9 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 PROVISONS

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.

GPTW Public Information - Proprietary

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 France.

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 the EU Member State in which the data exporter is established.

(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 exporter(s):

Name: Customer's name as indicated on the first page of the Data Processing Agreement (DPA). Address: As stated in the Agreement.

Contact person's name, position and contact details: As stated in the Agreement.

Activities relevant to the data transferred under these Clauses: Services pursuant to the Agreement and is the Controller of the Customer Personal Data.

Signature and date: As stated in the Agreement.

Role: Controller

Data importer:

Name: Great Place to Work Institute, Inc., and its Affiliates. Address: As stated in the Agreement.
Contact information:
Tel: + 1 800-432-1729 e-mail: privacy@greatplacetowork.com

Activities relevant to the data transferred under these Clauses: The data importer designs, markets, implements and supports employee engagement products and services for its customers.

Activities relevant to the data transferred under these Clauses: As a processor, the data importer receives personal data from the data exporter in order to deliver the Services pursuant to the Agreement.

Signature and date: As stated in the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit personal data to data importer in order for data importer to deliver the Services to the data exporter pursuant to the Agreement, the extent of which is determined and controlled by the data exporter, and which may include, but is not limited to personal data relating to the following categories of data subjects:

- As set forth in Schedule 1 to the DPA. Categories of personal data transferred

Based on the Services that the data exporter requests, data importer processes information, including personal data, at the data exporter's direction, such as:

- As set forth in Schedule 1 to the DPA.

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.

- As set forth in Schedule 1 to the DPA. The frequency of the transfer:

Continuous basis according to the terms of the Agreement between the data exporter and the data importer. Nature of and Purpose(s) of the data transfer and further processing:
Provision of the Services as described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Provision of the Services as described in the Agreement.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Provision of the Services as described in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 as set forth under Scheduled 1 of the DPA or as applicable, Section C Annex I of Annex I.A. – EU Commission Processor to Processor SCCs.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING 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:

As set forth in Schedule 2 to the DPA.

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

The data importer's sub-processors maintain reasonable and adequate administrative, technical, and physical measures to safeguard personal data from unauthorized access, loss, use, disclosure, alteration or destruction as appropriate given the personal data being handled and the services being provided by such sub-processor.

4. Annex I.D. – UK Controller to Processor Data Protection Clauses

UK Standard Data Protection Clauses

MODULE TWO

Part 1: Tables

Table 1: Parties

Start date	27 September 2021	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Data Processing Addendum (DPA).	See DPA.
Key Contact	See point of contact designated in the applicable agreement.	privacy@greatplacetowork.com
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below including the Appendix Information: Date: 27 September 2021 Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x			General	30 days	
3						
4						

Table 3: Appendix Information

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

Annex I.A: List of Parties: See DPA.
Annex I.B.: Description of Transfer: See DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

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

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies only to this Addendum and the transfers cited in Schedule 1.

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

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers of UK data as detailed in Schedule 1, the hierarchy in Section 10 will prevail.

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

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

Incorporation of and changes to the EU SCCs

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

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

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs for UK data only, as specified in Schedule 1; and

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

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

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

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made with respect to UK data as detailed in Schedule 1:

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

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

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

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;
    c. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

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

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

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

5. Annex I.E. – Swiss Addendum to the EU Commission Standard Contractual Clauses

This is a Swiss Addendum to the EU Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as displayed in https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en and as applicable in each case ("EU SCCs"). This Swiss Addendum has been drafted in accordance with the Federal Protection and Information Commissioner guidelines on the transfer of personal data issued on August 27, 2021 and entered into force on September 27, 2021. The Federal Data Protection and Information Commissioner ("Swiss DPA") considers that the EU SCCs provides appropriate safeguards for international data transfers from Switzerland when it is entered into as a legally binding contract and, hence, they may be relied on to legitimize transfers of personal data from Switzerland to countries without an adequate level of data protection, provided that the necessary amendments and adaptations are made for use under Swiss data protection law.

Part 1: Parties to the Addendum:
Exporter: Great Place To Work Institute, Inc. United States acting on its own name and on behalf of its affiliates that may receive personal data Address: Oakland, California. 1901 Harrison Street, Suite 1100, CA 94612. (Headquarters)

Contact person's name, position and contact details: privacy@greatplacetowork.com

Importer: The data importer is the legal entity (along with its affiliates) to which the data exporter transfers personal data based on the relevant services agreement ("the Agreement") which incorporates the EU Standard Contractual Clauses ("EU SCCs") to which this Addendum is appended.

Signature and date: Signed by virtue of reference to and incorporation of the EU SCCs to which this Addendum is appended into the relevant agreement and signature of the latter by the data exporter.

Part 2: Amendments to the EU SCCs:

1. Each Party agrees to be bound by the terms and conditions set out in this Swiss Addendum.

2. This Swiss Addendum and the EU SCCs that incorporates must always be interpreted in a manner that is consistent with all laws relating to data protection, personal data and/or electronic communications in force from time to time in Switzerland, including the Swiss Federal Act on Data Protection of 25 September 2020 ("Swiss Data Protection Laws"). If there is any inconsistency or conflict between Swiss Data Protection Laws and this Swiss Addendum or the EU SCCs that incorporates, Swiss Data Protection Laws applies.

3. Where this Swiss Addendum incorporates EU SCCs which have been entered into to protect transfers subject to the Regulation (EU) 2016/679 of 27 April 2016 ("GDPR"), the Parties acknowledge that nothing in this Swiss Addendum impacts those EU SCCs.

4. The respectively applicable set of EU SCC applies mutatis mutandis to international data transfers carried out by GPTW to any applicable subprocessor out of Switzerland.

5. The SCC shall be deemed to be amended as follows: - References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" in the EU SCCs shall be deemed to include Switzerland. This includes references to the court in a member state in Clause 18 c, that shall also include the Swiss courts as an alternative place of jurisdiction for data subjects residing in Switzerland. - References to "competent supervisory authority" and "supervisory authority" are to be considered the Swiss DPA when data is exclusively subject to the Swiss Data Protection Laws; and to both the Swiss DPA and the EU competent supervisory authority insofar as the data transfer is governed by both the Swiss Data Protection Laws and the GDPR. This includes Clause 13(a) and Part C of Annex I of the EU SCCs. - References to "GDPR" "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the

European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are to include the "Swiss Data Protection Laws" as well. References to specific Article(s) of "Regulation (EU) 2016/679" are to include also the equivalent or more similar Article of Swiss Data Protection Laws. References to the "Clauses" means this Swiss Addendum, incorporating the EU SCCs into it. References to the "European Commission" shall include Swiss competent authorities as well. Where an international data transfer of GPTW controlled personal data is subject to a law that protects legal entities as data subjects, the EU SCCs will apply to legal entities as well. This Swiss Addendum (including the EU SCCs) shall be governed by the laws of Switzerland and any dispute arising from it is resolved by the courts of Switzerland. To the extent the data transfer is exclusively subject to the Swiss Data Protection Laws, reference to the governing law in clause 17 of the EU SCCs shall be referred to the Swiss Data Protection Laws or the law of an EU country in accordance with the EU SCCs, provided that it allows and grants rights as a third-party beneficiary for contractual claims regarding data transfers.

6. Annex I.F. – Brazilian Standard Contractual Clauses

The text of the clauses included in this Annex corresponds to the version approved by Resolution CD/ANPD No. 19/2024, as set forth in the annexes of the Regulation on International Data Transfers issued by the Brazilian Data Protection Authority (ANPD).

Clause 1 – Identification of the Parties 1.1. By this contractual instrument, the Exporter and the Importer (hereinafter "Parties"), identified below, agree to adopt the standard contractual clauses (hereinafter "Clauses") approved by the Brazilian Data Protection Authority (ANPD), to govern the International Data Transfer described in Clause 2, in accordance with Brazilian law.	**Cláusula 1 – Identificação das Partes** 1.1. Pelo presente instrumento contratual, o Exportador e o Importador (doravante, "Partes"), abaixo identificados, resolvem adotar as cláusulas-padrão contratuais (doravante "Cláusulas") aprovadas pela Autoridade Nacional de Proteção de Dados (ANPD), para reger a Transferência Internacional de Dados descrita na Cláusula 2, em conformidade com as disposições da legislação brasileira.
Clause 2 – Object 2.1. These Clauses apply to International Data Transfers from the Exporter to the Importer, as described below: – Main purposes of the transfer: __ – Categories of personal data transferred: __ – Data retention period: __ – Other relevant information: __	**Cláusula 2 – Objeto** 2.1. Estas Cláusulas se aplicam às transferências internacionais de Dados Pessoais do Exportador ao Importador, conforme descrito abaixo: – Finalidades principais da transferência: __ – Categorias de dados pessoais transferidos: __ – Prazo de retenção de dados: __ – Outras informações relevantes: __
Clause 3 – Onward Transfers (Option A or B as applicable) Option A: 3.1. The Importer may not carry out Onward Transfers of the Personal Data subject to this International Data Transfer, except in the cases provided in Clause 18.3. Option B: 3.1. The Importer may carry out Onward Transfers, provided the conditions in Clause 18 are respected.	**Cláusula 3 – Transferências Posteriores (Onward Transfers)** (Opção A ou B conforme aplicável) Opção A: 3.1. O Importador não poderá realizar transferências posteriores dos Dados Pessoais objeto desta transferência internacional, salvo nas hipóteses previstas na Cláusula 18.3. Opção B: 3.1. O Importador poderá realizar transferências posteriores, desde que obedecidas as condições da Cláusula 18.
Clause 4 – Responsibilities of the Parties Option A / Option B (controller / processor) — depending on the Parties' role — with obligations concerning publication (Clause 14), handling subject requests (Clause 15), incident notification (Clause 16), etc.	**Cláusula 4 – Responsabilidades das Partes** Opção A (controlador) / Opção B (operador) — conforme o papel das Partes — com obrigações de publicação (Cláusula 14), atendimento a titulares (Cláusula 15), notificação de incidentes (Cláusula 16) etc.
Clause 5 – Purpose 5.1. These Clauses aim to enable the secure international flow of personal data, establish minimum guarantees and valid conditions for performing International Data Transfers, and ensure adoption of appropriate safeguards under Brazilian data protection law.	**Cláusula 5 – Finalidade** 5.1. Estas Cláusulas destinam-se a viabilizar o fluxo internacional seguro de dados pessoais, estabelecer garantias mínimas e condições válidas para a execução da transferência internacional, e assegurar a adoção de salvaguardas adequadas ao regime de proteção de dados previsto na legislação brasileira.
Clause 6 – Definitions 6.1. For the purposes of these Clauses, the definitions in art. 5 of the LGPD and art. 3 of the International Data Transfer Regulation apply, without prejudice to further normative acts by ANPD. The Parties also agree to regard the terms below with	**Cláusula 6 – Definições** 6.1. Para os fins destas Cláusulas, aplicam-se as definições do art. 5 da LGPD e do art. 3 do Regulamento de Transferência Internacional de Dados, sem prejuízo de outros atos normativos da ANPD. As Partes concordam em considerar os termos abaixo com seus respectivos sentidos: a) agentes de tratamento: controlador e operador; b) ANPD: Autoridade Nacional de Proteção de Dados;

their respective meanings: a) processing agents: controller and processor; b) ANPD: Brazilian Data Protection Authority; c) Clauses: the standard contractual clauses approved by ANPD, comprising Sections I, II and III; d) Linked Agreement: contractual instrument between the Parties or, at least, between one and a third-party controller ("Third-Party Controller"), having linkage or dependency with the contract governing the International Data Transfer; e) Controller; f) Personal Data; g) Sensitive Personal Data; h) Deletion; i) Exporter; j) Importer; k) Brazilian Legislation; l) Arbitration Law; m) Security Measures; n) Research Body; o) Processor; p) Designated Party; q) Parties; r) Access Request; s) Subprocessor; t) Third-Party Controller; u) Data Subject; v) Transfer; w) International Data Transfer; x) Onward Transfer	c) Cláusulas: as cláusulas-padrão aprovadas pela ANPD, que compreendem as Seções I, II e III; d) Contrato Vinculado: instrumento contratual entre as Partes ou, ao menos, entre uma delas e um terceiro controlador ("Third-Party Controller"), que tenha vínculo ou dependência com o contrato que rege a transferência internacional; e) Controlador; f) Dados Pessoais; g) Dados Sensíveis; h) Eliminação; i) Exportador; j) Importador; k) Legislação Brasileira; l) Lei de Arbitragem; m) Medidas de Segurança; n) Entidade de Pesquisa; o) Operador; p) Parte Designada; q) Partes; r) Pedido de Acesso; s) Subcontratada; t) Third-Party Controller; u) Titular; v) Transferência; w) Transferência Internacional; x) Transferência Posterior (Onward Transfer)
Clause 7 – Applicable Law & ANPD Supervision 7.1. The International Data Transfer subject to these Clauses shall be governed by Brazilian law and supervised by ANPD, including power to apply preventive measures, sanctions, limit, suspend or prohibit transfers arising from these Clauses or a Linked Agreement.	**Cláusula 7 – Legislação Aplicável e Fiscalização da ANPD** 7.1. A transferência internacional sujeita a estas Cláusulas será regida pela legislação brasileira e supervisionada pela ANPD, incluindo a aplicação de sanções, limitação, suspensão ou proibição das transferências originárias destas cláusulas ou de Contrato Vinculado.
Clause 8 – Interpretation 8.1. Application of these Clauses must follow: a) interpretation most favorable to the Data Subject and consistent with Brazilian law; b) in case of doubt, the meaning most aligned with national law prevails; c) no clause here or Linked Agreement may be construed to limit or exclude liability under Brazilian law; d) provisions in Sections I and II prevail over additional clauses or Sections III/IV or Linked Agreement.	**Cláusula 8 – Interpretação** 8.1. A aplicação destas Cláusulas deve obedecer: a) interpretação mais favorável ao Titular e conforme a legislação brasileira; b) em caso de dúvida, prevalece o sentido mais alinhado à legislação nacional; c) nenhum dispositivo destas Cláusulas ou Contrato Vinculado poderá ser interpretado para limitar ou excluir a responsabilidade das Partes conforme a legislação brasileira; d) as disposições das Seções I e II prevalecem em caso de conflito com cláusulas adicionais ou Seções III/IV ou Contrato Vinculado.
Clause 9 – Third-Party Adherence 9.1. By mutual agreement, a processing agent may adhere to these Clauses as Exporter or Importer via written instrument that becomes part of this contract. 9.2. The acceding party shall have the same rights and obligations as the original Parties, according to position and agent category.	**Cláusula 9 – Adesão de Terceiros** 9.1. Por acordo mútuo, um agente de tratamento pode aderir a estas Cláusulas como Exportador ou Importador, mediante assinatura de instrumento escrito que passe a integrar este contrato. 9.2. A parte aderente terá os mesmos direitos e obrigações das Partes originais, segundo a posição assumida e categoria de agente.
Clause 10 – General Obligations of the Parties 10.1. The Parties commit to adopting and, when necessary, demonstrating effective measures	**Cláusula 10 – Obrigações Gerais das Partes** 10.1. As Partes comprometem-se a adotar e demonstrar medidas eficazes capazes de comprovar a observância e o cumprimento destas Cláusulas e da legislação brasileira, e,

capable of proving compliance with these Clauses and Brazilian law, and in particular: a) use Personal Data only for the specific purposes in Clause 2, not for incompatible processing; b) ensure processing is compatible with purposes informed to the Data Subject; c) limit processing to minimum necessary; d) ensure Data Subjects have access to clear information about processing, form, duration, per law; e) adopt security measures compatible with risks; f) not process data for discriminatory or abusive purposes; g) ensure persons under authority (including subprocessors) process data only per instructions and these Clauses; h) maintain record of processing operations subject to transfer and provide documentation to ANPD when requested.	em particular: a) usar os Dados Pessoais apenas para as finalidades específicas da Cláusula 2, sem posterior utilização incompatível; b) assegurar compatibilidade com finalidades informadas ao Titular; c) limitar o tratamento ao mínimo necessário; d) garantir que os Titulares tenham acesso a informações claras sobre o processamento, forma e duração, conforme legislação; e) adotar medidas de segurança compatíveis com os riscos envolvidos; f) não tratar dados para fins discriminatórios ou abusivos; g) garantir que pessoas sob autoridade das Partes (incluindo subcontratadas) processem dados apenas conforme instruções e estas cláusulas; h) manter registro das operações de tratamento objeto da transferência e fornecer documentação à ANPD quando solicitado.
Clause 11 – Sensitive Personal Data 11.1. If the transfer involves Sensitive Personal Data, additional safeguards must be applied, including specific security measures proportional to the risks, nature of data, and interests of the Data Subject.	**Cláusula 11 – Dados Sensíveis** 11.1. Se a transferência envolver Dados Sensíveis, as Partes aplicarão salvaguardas adicionais, inclusive medidas de segurança específicas proporcionais aos riscos, à natureza dos dados e aos interesses do Titular.
Clause 12 – Data of Children & Adolescents 12.1. If data relate to children or adolescents, additional safeguards apply to ensure processing in their best interest, per Brazilian law and applicable international instruments.	**Cláusula 12 – Dados de Crianças e Adolescentes** 12.1. Se envolver dados de crianças ou adolescentes, aplicarão salvaguardas adicionais para assegurar o melhor interesse, conforme a legislação brasileira e instrumentos internacionais aplicáveis.
Clause 13 – Lawful Use of Data 13.1. The Exporter warrants that the Personal Data were collected, processed, and transferred in compliance with Brazilian law.	**Cláusula 13 – Uso Legal dos Dados** 13.1. O Exportador garante que os Dados Pessoais foram coletados, tratados e transferidos de conformidade com a legislação brasileira.
Clause 14 – Transparency 14.1. The Designated Party must publish, on its website, an accessible document in simple language, containing: a) method, duration, and purpose of international transfer; b) destination country of data; c) identification and contact of the Designated Party; d) data sharing and purpose; e) responsibilities of the processing agents; f) Data Subject rights and means of exercise, including accessible channel and right to complain to ANPD; g) onward transfers, naming recipients and purpose. 14.2. The document may be on a dedicated page or	**Cláusula 14 – Transparência** 14.1. A Parte Designada deverá publicar, em seu site, documento acessível, em linguagem simples, contendo: a) forma, duração e finalidade da transferência internacional; b) país de destino dos dados; c) identificação e contato da Parte Designada; d) compartilhamento de dados e finalidade; e) responsabilidades dos agentes; f) direitos dos Titulares e meios de exercício, incluindo canal acessível e direito de reclamação à ANPD; g) transferências posteriores incluídas informações sobre destinatários e propósito. 14.2. O documento pode estar numa página específica ou integrado na Política de Privacidade. 14.3. A pedido, as Partes deverão fornecer ao Titular cópia gratuita destas Cláusulas (sujeita a segredos comercial/industrial). 14.4. Todas as informações exigidas devem estar em

integrated into Privacy Policy. 14.3. Upon request, provide free copy of these Clauses (subject to trade/industrial secrets). 14.4. All required information must be presented in Portuguese.	português.
Clause 15 – Data Subject Rights 15.1. The Data Subject has the right to obtain from the Designated Party, at any time, under Brazilian law: a) confirmation of processing existence; b) access to data; c) correction of incomplete, inaccurate, or outdated data; d) anonymization, blocking, deletion of data processed unlawfully or in excess; e) portability to another service/product, upon express request; f) deletion of data processed with consent (except where law allows retention); g) information about entities sharing data; h) information about the possibility of refusal of consent and consequences; i) withdrawal of consent via free, facilitated procedure; j) review of decisions based solely on automated processing; k) information about criteria & procedures used in automated decisions (subject to trade/industrial secrets). 15.2. The Data Subject may object to processing based on legal bases exempting consent, in case of non-compliance with Clauses or law. 15.3. The deadline to respond is 15 (fifteen) days unless a different term is provided by ANPD. 15.4. If the request is made to a non-designated Party, it shall: a) inform the Data Subject of the designating Party's contact; or b) forward the request to the Designated Party to respond within legal term. 15.5. The Parties shall immediately inform agents with whom they shared data about corrections, deletions, anonymization or blocking, unless demonstrably infeasible. 15.6. The Parties will provide mutual assistance to fulfill Data Subject requests.	**Cláusula 15 – Direitos do Titular** 15.1. O Titular tem direito de obter da Parte Designada, a qualquer tempo, nos termos da legislação: a) confirmação da existência de tratamento; b) acesso aos dados; c) correção de dados incompletos, imprecisos ou desatualizados; d) anonimização, bloqueio ou eliminação de dados excessivos ou tratados em desacordo; e) portabilidade para outro serviço ou produto, mediante solicitação expressa; f) eliminação dos dados tratados com consentimento (exceto em hipóteses legais); g) informação sobre entidades com quem os dados foram compartilhados; h) informação sobre possibilidade de não fornecer consentimento e consequências; i) revogação do consentimento por procedimento gratuito e facilitado; j) revisão de decisões baseadas em tratamento automatizado; k) informação sobre critérios e procedimentos usados em decisões automatizadas (resguardados segredos comercial/industrial). 15.2. O Titular pode se opor ao tratamento baseado nas hipóteses legais de dispensa de consentimento, em caso de descumprimento destas Cláusulas ou da legislação. 15.3. O prazo para resposta a solicitações previstas nesta Cláusula é de 15 (quinze) dias, salvo prazo diverso fixado pela ANPD. 15.4. Se o pedido for dirigido à Parte não designada para cumprir esta Cláusula, deverá: a) informar canal da Parte Designada; ou b) remeter o pedido à Parte Designada tão logo possível para resposta dentro do prazo legal. 15.5. As Partes deverão informar imediatamente a agentes com quem compartilharam os dados sobre correção, eliminação, anonimização ou bloqueio, salvo impossibilidade demonstrável. 15.6. As Partes promoverão assistência mútua para atender pedidos dos Titulares.
Clause 16 – Security Incident Notification 16.1. The Designated Party shall notify the ANPD and the Data Subjects, within 3 (three) business days, of a security incident that may lead to relevant risk or harm, as per Brazilian law. 16.2. The Importer must keep record of security	**Cláusula 16 – Notificação de Incidentes de Segurança** 16.1. A Parte Designada notificará à ANPD e aos Titulares, em até 3 (três) dias úteis, a ocorrência de incidente de segurança que possa acarretar risco relevante ou dano aos Titulares, conforme a legislação. 16.2. O Importador manterá registro de incidentes de

incidents in accordance with Brazilian law.	segurança conforme a legislação brasileira.
Clause 17 – Liability & Compensation 17.1. The Party that causes material, moral, individual or collective damage, in breach of these Clauses or Brazilian law, shall compensate. 17.2. The Data Subject may seek compensation from any Party. 17.3. Claims may be brought individually or collectively as per applicable law. 17.4. The Processor is jointly liable for failures to comply with Clauses or instructions from the Controller. 17.5. Controllers involved are jointly liable, subject to Clause 17.6. 17.6. The Parties are not liable if they prove that: a) they did not perform the assigned processing; b) there was no breach of Clauses or law; c) the damage resulted solely from fault of the Data Subject or a third party, not being Importer/subcontractor. 17.7. Under Brazilian law, burden of proof may be reversed in favor of the Data Subject if the claim is credible, evidence is insufficient or evidence production is too burdensome for the Data Subject. 17.8. The indemnifying Party may seek recourse from others proportionally to their involvement.	**Cláusula 17 – Responsabilidade e Indenização** 17.1. A Parte que causar dano material, moral, individual ou coletivo, em violação destas Cláusulas ou da legislação brasileira, deverá indenizar. 17.2. O Titular pode buscar indenização por danos de qualquer das Partes. 17.3. A defesa dos interesses dos Titulares pode ser feita individual ou coletivamente, conforme a legislação aplicável. 17.4. O Operador é responsável solidário se violar estas Cláusulas ou instruções lícitas do Controlador. 17.5. Controladores envolvidos são responsáveis solidários, salvo disposições da Cláusula 17.6. 17.6. As Partes não respondem se comprovarem que: a) não desempenharam o tratamento atribuído; b) não houve violação das Cláusulas ou legislação; ou c) o dano decorreu exclusivamente de culpa do Titular ou terceiro, não sendo destinatário de Onward Transfer ou subcontratado. 17.7. Sob a legislação brasileira, o juiz pode inverter o ônus da prova em favor do Titular se o pedido for crível, houver insuficiência de produção de provas ou quando for excessivo para o Titular produzi-las. 17.8. A Parte que indeniza o Titular pode exercer direito de regresso contra outras Partes, proporcionalmente à participação no evento danoso.
Clause 18 – Safeguards for Onward Transfer 18.1. The Importer may only make Onward Transfers if explicitly authorized per Clause 3. 18.2. In any case, the Importer must: a) ensure compatibility of the onward transfer's purpose with Clause 2; b) ensure via written contract that recipient observes the safeguards in these Clauses; c) be liable for irregularities by recipient. 18.3. Onward Transfers may also be made based on another valid legal mechanism under Brazilian law, regardless of authorization in Clause 3.	**Cláusula 18 – Salvaguardas para Transferência Posterior** 18.1. O Importador só poderá realizar transferências posteriores se expressamente autorizado conforme a Cláusula 3. 18.2. Em qualquer caso, o Importador: a) deve garantir compatibilidade da finalidade da transferência posterior com a Cláusula 2; b) assegurar que o destinatário da transferência posterior observe as mesmas salvaguardas contratadas; c) será considerado responsável por irregularidades do destinatário na transferência posterior. 18.3. As transferências posteriores também podem ocorrer com base em outro mecanismo válido previsto na legislação brasileira, independentemente da autorização da Cláusula 3.
Clause 19 – Access Request Notification 19.1. The Importer shall notify the Exporter and the Data Subject of any Access Request regarding the transferred data, unless prohibited by law in the processing country. 19.2. The Importer shall take lawful measures to protect Titular rights if notification is prohibited. 19.3. To comply with requests from ANPD or Exporter, the Importer shall keep a record of Access Requests (date, requester, purpose, data types,	**Cláusula 19 – Notificação de Pedido de Acesso** 19.1. O Importador notificará o Exportador e o Titular de qualquer Pedido de Acesso relacionado aos Dados transferidos, salvo se proibido por lei do país do processamento. 19.2. O Importador adotar medidas legais para proteger os direitos do Titular, se aplicável, caso não possa notificar. 19.3. Para cumprir solicitações da ANPD e do Exportador, o Importador manterá registro dos Pedidos de Acesso (data, solicitante, finalidade, tipo de dados, quantidade, medidas

number, legal measures).	legais adotadas).
Clause 20 – Termination & Deletion of Data 20.1. The Parties must delete the transferred data after processing ends, within technical limits, retaining only for: a) legal or regulatory compliance; b) research by Research Body, ensuring anonymization where possible; c) transfer to third party (provided compliance with these Clauses and law); d) exclusive use by Controller, preventing third-party access, if anonymized. 20.2. Processing ends when: a) purpose achieved; b) data no longer needed; c) term of processing expires; d) Titular request fulfilled; e) determination of ANPD upon violation.	**Cláusula 20 – Término do Tratamento e Eliminação de Dados** 20.1. As Partes eliminarão os Dados pessoais objeto da transferência após o término do tratamento, dentro dos limites técnicos, com retenção apenas para: a) cumprimento de obrigação legal; b) pesquisa por entidade de pesquisa, garantindo anonimização, quando possível; c) transferência para terceiro desde que requisitos destas Cláusulas e da legislação sejam respeitados; d) uso exclusivo do Controlador, sem acesso por terceiros, e se os dados forem anonimizados. 20.2. Término do tratamento ocorre quando: a) a finalidade for alcançada; b) os dados deixarem de ser necessários; c) prazo de tratamento expirar; d) solicitação do Titular for atendida; e) determinação da ANPD em caso de descumprimento.
Clause 21 – Data Processing Security 21.1. The Parties shall adopt security measures to protect the transferred data, even after processing ends. 21.2. The Parties shall specify in contract the Security Measures adopted, considering data nature, processing features, technology, and risk to Data Subjects. 21.3. The Parties shall perform periodic evaluations to maintain adequate security levels as context and risks evolve.	**Cláusula 21 – Segurança do Tratamento de Dados** 21.1. As Partes adotarão medidas de segurança para proteger os Dados pessoais objeto desta transferência, inclusive após o término do tratamento. 21.2. As Partes especificarão no contrato as Medidas de Segurança adotadas, levando em conta a natureza dos dados, características do processamento, tecnologia envolvida e riscos aos Titulares. 21.3. As Partes devem adotar avaliações periódicas para revisar o nível de segurança adequado conforme a evolução do contexto e dos riscos.
Clause 22 – Legislation of Recipient Country 22.1. The Importer declares not having identified laws or administrative practices preventing compliance with these Clauses. 22.2. If normative changes alter this situation, the Importer shall notify the Exporter for assessment of continuity.	**Cláusula 22 – Legislação do País do Importador** 22.1. O Importador declara não haver identificado leis ou práticas administrativas que o impeçam de cumprir estas Cláusulas. 22.2. Se ocorrer mudança normativa que altere essa situação, o Importador notificará o Exportador para avaliação da continuidade do contrato.
Clause 23 – Non-Compliance by Importer 23.1. In case of breach or inability to comply by Importer, Exporter shall be notified immediately. 23.2. After notification or verification, Exporter shall take necessary measures to protect Data Subjects' rights and ensure compliance, which may include: a) suspension of transfer; b) request return, transfer or deletion of data; c) contract termination.	**Cláusula 23 – Descumprimento pelo Importador** 23.1. Em caso de descumprimento destas Cláusulas ou impossibilidade de cumprimento pelo Importador, o Exportador deverá ser notificado imediatamente. 23.2. Após notificação ou verificação de descumprimento, o Exportador adotará medidas necessárias para proteger os direitos dos Titulares e garantir conformidade com esta Cláusula ou legislação, incluindo: a) suspensão da transferência internacional; b) solicitar devolução, transferência a terceiro ou eliminação dos Dados; c) rescisão do contrato.
Clause 24 – Choice of Forum &	**Cláusula 24 – Escolha de Foro e Jurisdição**

Jurisdiction 24.1. These Clauses are governed by Brazilian law, and disputes will be resolved in Brazil's competent courts, subject to forum agreed in Linked Agreement, if any. 24.2. Data Subjects may sue Exporter or Importer in Brazilian courts, including in their residence jurisdiction. 24.3. Parties may agree to arbitration in Brazil, per Arbitration Law.	24.1. Estas Cláusulas são regidas pela lei brasileira, e disputas serão resolvidas nos tribunais competentes do Brasil, respeitada escolha de foro no contrato vinculado, se houver. 24.2. Os Titulares poderão acionar Exportador ou Importador nos tribunais brasileiros, inclusive no domicílio do Titular. 24.3. As Partes podem acordar uso de arbitragem no Brasil, de acordo com a Lei de Arbitragem.
1. Parties • **Transferring Entity**: As listed in Schedule 1 of the DPA(Brazilian operations). • **Receiving Entity**: Any GPTW Affiliate receiving Personal Data from Brazil.	**1. Partes** • **Entidade Exportadora**: conforme listado no Anexo 1 do DPA (operações no Brasil). • **Entidade Importadora**: qualquer Afiliada G PTW que receba Dados Pessoais do Brasil.
2. Applicable Law These clauses are governed by the LGPD and applicable ANPD regulations.	**2. Legislação Aplicável** Estas cláusulas são regidas pela LGPD e pelas regulamentações aplicáveis da ANPD.
3. Data Subject Rights The Receiving Entity shall guarantee that Data Subjects can exercise their LGPD rights, including: • Access, correction, anonymization, portability, deletion; • Information on sharing of data; • Revocation of consent.	**3. Direitos dos Titulares** A Entidade Importadora deve assegurar o exercício dos direitos previstos na LGPD, incluindo: • Acesso, correção, anonimização, portabilid ade, eliminação; • Informação sobre compartilhamento de dad os; • Revogação de consentimento.
4. Supervisory Authority The **ANPD** is designated as the competent supervisory authority.	**4. Autoridade Supervisora** A **ANPD** é a autoridade supervisora competente.
5. Language These clauses are executed in English and Portuguese. In the event of conflict, the Portuguese version prevails.	**5. Idioma** Estas cláusulas são firmadas em inglês e português. Em caso de conflito, prevalece a versão em português.
6. Enforcement and Jurisdiction The competent courts of Brazil shall have jurisdiction to hear disputes arising from these clauses.	**6. Execução e Foro** O foro brasileiro é eleito para dirimir quaisquer controvérsias d ecorrentes destas cláusulas.
7. Annexes • **Annex I** – Description of transfers (refer to the DPA). • **Annex II** – Security measures (refer to the DPA).	**7. Anexos** • **Anexo I** – Descrição das transferências (conforme Anex o DPA). • **Anexo II** – Medidas de segurança (conforme do DPA).
