EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

**ANNEX**

***to the***

**COMMISSION IMPLEMENTING DECISION**

**on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

STANDARD CONTRACTUAL CLAUSES

SECTION I

*Clause 1*

*Purpose and scope*

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

[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

(b) The Parties:

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

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

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

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

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

*Clause 2*

*Effect and invariability of the Clauses*

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

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

*Clause 3*

*Third-party beneficiaries*

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

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

(ii) Clause 8 - Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 12 - Clause 12(a) and (d);

(iv) Clause 13;

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

(vi) Clause 16(e);

---

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 […].

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

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

*Clause 4*

***Interpretation***

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

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

*(i)* 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***

(j) 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.

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

(l) 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 Purpose limitation

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

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

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

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

### 8.2 Transparency

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

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

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

### 8.3 Accuracy and data minimisation

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

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

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

### 8.4 Storage limitation

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

### 8.5 Security of processing

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

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

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

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

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

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

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

---

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

### 8.6 Sensitive data

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

### 8.7 Onward transfers

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

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

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

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

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

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

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

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

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

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

---

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

### 8.9 Documentation and compliance

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

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

*Clause 9*

***Use of sub-processors***

[This Clause 9 is intentionally left blank as it does not apply to Module One: Controller to Controller Transfers]

*Clause 10*

***Data subject rights***

(cc) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

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

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

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

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

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

(ff) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

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

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

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

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

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

*Clause 11*

***Redress***

(jj) 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(kk) 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.

(ll) 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.

(mm) 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.

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

(oo) 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.

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

*Clause 12*

*Liability*

(pp) 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.

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

(rr) 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.

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

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

*Clause 13*

*Supervision*

(uu) 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.

(vv) 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*

(ww) 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.

(xx) 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[6];

(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.

(yy) 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.

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

(aaa) 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).

(bbb) 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***

[6] 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.

### 15.1 Notification

(ccc) 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.

(ddd) 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.

(eee) 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.).

(fff) 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.

(ggg) 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

(hhh) 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).

(iii) 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.

(jjj) 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*

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

(lll) 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).

(mmm) 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.

(nnn) 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.

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

*Clause 17*

*Governing law*

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

*Clause 18*

*Choice of forum and jurisdiction*

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

(qqq) The Parties agree that those shall be the courts of Cologne, Germany.

(rrr) 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.

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

# APPENDIX

## ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):**

1. **Name**: Cleverbridge GmbH (on behalf of itself and its affiliates)

**Address**: Gereonstraße 43-65, 50670 Cologne, Germany

**Contact person's name, position and contact details**: Cleverbridge Data Protection Officer, privacy@Cleverbridge.com

**Activities relevant to the data transferred under these Clauses**: As specified in Annex I.B.

**Signature and date**: _____

**Role (controller/processor)**: Controller

**Data importer(s):**

1. **Name**: CLIENT

**Address**: _____

**Contact person's name, position and contact details**: _____

**Activities relevant to the data transferred under these Clauses**: As specified in Annex I.B.

**Signature and date**: _____

**Role (controller/processor)**: Controller

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

- Natural persons ("**Customer**") who submit personal data to the data exporter to purchase or subscribe to products and services.
- Natural persons ("**Affiliate**") who host links to the online store, subscription portal or website.
- Natural persons ("**Contact**") who are employees, representatives, or other business contacts of the data exporter.

*Categories of personal data transferred*

- Customer data:
  - Name and contact details (which may include name, address, e-mail address, company name, phone and fax contact details, associated local time zone information and location data);
  - Support information and contact history;
  - Audio recordings of phone calls;
  - Sales and marketing information (records of purchases, records of marketing activity);
  - Statistical data;

- IP addresses and other usage data pertaining to the data subjects;
- Other unique identifiers;
- Billing information, excluding payment information, e.g. bank account and/or credit card information

- Affiliate data:
  - Name and contact details (which may include name, address, e-mail address, company name, phone and fax contact details, associated local time zone information and location data);
  - Sales and marketing information (records of purchases, records of marketing activity);
  - Statistical data;
  - IP addresses and other usage data pertaining to the data subjects;
  - Other unique identifiers;
  - Billing information, excluding payment information, e.g. bank account and/or credit card information
- Contact data:
  - Name and contact details (which may include name, address, e-mail address, company name, phone and fax contact details, associated local time zone information and location data)

*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.*

- Not applicable – sensitive personal data is not intentionally processed or transferred.

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

- Continuous

*Nature of the processing*

- Collection, disclosure, storage and other basic processing to perform any steps necessary for the performance of the Agreement.

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

- The transfer is made for the following purposes:
  - Any data processing operation applied to personal data that is provided by the data exporter in accordance with the applicable agreement between the data importer and data exporter.

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

- For as long as is necessary under the Agreement.

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

- Not applicable

## C. COMPETENT SUPERVISORY AUTHORITY

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

- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia)

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

As separate controllers, the Parties agree to abide by their own Technical and Organizational Measures (TOMs). Cleverbridge's TOMs are reproduced below. Client shall provide its TOMs upon request and agrees to implement similar measures when handling any Personally Identifiable Information or Customer Information passed from Cleverbridge to Client, and in any event, no less secure measures.

### Cleverbridge Technical and Organizational Measures

The technical and organizational measures (TOMs) provided below apply to all standard service offerings provided by Cleverbridge. Evidence of the measures implemented and maintained by Cleverbridge may be presented in the form of up-to-date attestations, reports, or extracts from independent bodies upon request from the Client.

1) Payment Card Industry Data Security Standard (PCI DSS):
   a) Cleverbridge is PCI DSS certified and shall maintain such certification during the Term of this Agreement. Therefore, Cleverbridge:
      i) Masks credit card numbers or bank details when displayed.
      ii) Maintains individual user-IDs for data processing systems as well as secure passwords according to PCI DSS standard.
      iii) Keeps storage of cardholder data at a minimum so that cardholder data is only stored for as long as necessary.
      iv) Maintains an up-to-date list of devices with the information specified by PCI for the clear identification of the devices and has implemented the measures provided by PCI DSS for the protection of devices against manipulation and replacement.
      v) Encrypts:
         (1) hard disks of the workstations (i.e. notebooks, PCs) used by employees for data processing.
         (2) credit card data in storage environment while at rest.
         (3) transmission of personal data from the credit card processor via public networks.
         (4) emails as needed or requested.
      vi) utilizes procedures for data backups according to PCI DSS standard.

2) Physical Security and Equipment Protection:
   a) All databases of the payment area are located on the servers in Cleverbridge's data center in a completely encrypted area.
   b) All servers used are located in an appropriately air-conditioned environment.
   c) Cleverbridge has installed appropriate fire protection measures in all areas where data processing takes place.
   d) Cleverbridge has implemented adequate power supply for systems by means of uninterruptible power supply (UPS).
   e) Physical security implemented on Cleverbridge premises includes:
      i) Badge-controlled access to buildings and secure areas where Cleverbridge IT networks are installed in such areas, with controlled access systems to limit access to restricted access areas to authorised personnel only.
      ii) Visitors allowed access to premises only when escorted by an authorised person with a record in the visitors register.
      iii) Security guard force present in certain selected buildings. CCTV in buildings.
      iv) Emergency response procedures in place for buildings in the case of fire, flood etc.

3) Security Incident Response/Prevention:
   a) Cleverbridge maintains an Incident Response Plan and a risk management process.
   b) Cleverbridge conducts regular vulnerability scans and penetration tests as well as use of intrusion detection and intrusion prevention systems.
   c) Cleverbridge equips all workstations and servers with anti-virus software that is updated automatically on a regular basis.
   d) Cleverbridge identifies security risks and all system components and regularly protects software applications with the latest security patches against known security risks to close security gaps.
   e) Cleverbridge specifies criteria for secure development of applications developed in-house. After development, Cleverbridge checks the individual program code for all potential security risks (dual control principle) and makes corrections, if necessary.
   f) To minimize the damage from security incidents:
      i) All incidents are reported through appropriate management and security incident reporting channels as quickly as possible.
      ii) All employees and contractors are made aware of the procedures for reporting the different types of security incident that might have an impact on classified information or on the information technology infrastructure and services.
      iii) Any physical security incidents, including security breaches or thefts, are reported immediately to the organization responsible for physical security.

4) Data Retention:
   a) Cleverbridge has implemented policies and procedures for data retention and deletion (deletion periods and processes for deleting data). As soon as personal data, in whatever form (especially in paper or electronic form), is no longer required, Cleverbridge destroys personal data in a manner that makes recovery impossible.

5) User Access Management:
   a) Cleverbridge has implemented:
      i) A roles and access rights concept.
         (1) Access authorizations are limited to the extent necessary to perform the activity according to responsibilities and information requirements (assignment of minimum authorizations according to the need-to-know principle).
      ii) Logging and protocol evaluation systems.
      iii) Strong cryptography and security protocols.
         (1) Only trustworthy keys and certificates are accepted. The protocol used supports only secure versions or configurations and the correct encryption strength is used.
      iv) Procedures to protect cryptographic keys against disclosure or misuse.
         (1) Key management processes and procedures for cryptographic keys are certified.
      v) Access controls and alarm systems for headquarters, video surveillance in server rooms as well as data centers.
      vi) A firewall configuration, or a demilitarized zone.
         (1) The firewall configuration is set up according to a standard defined for this purpose, is maintained regularly, and restricts incoming and outgoing connections between the internal company network and other networks.
      vii) A web application firewall to detect and prevent web-based attacks.
      viii) Separate development and test environments from the production environment.
      ix) Audit trails to track the entire access of individual users to system components or user activities in order to prevent or detect access protection violations and to identify the causes of problems.
      x) Systems to detect unauthorized changes (including additions and deletions) to critical system, configuration or content files.
   b) All access to client facing environments require authentication through a secure connection via approved methods such as VPNs and enforced with mutual certificate authentication. VPN access is further enforced by mutual transport layer security authentication.

c) Cleverbridge controls internal and external distribution of any kind of media and classifies media for this purpose according to the risk potential of the contained data.
   i) Cleverbridge also maintains media inventory lists.

6) Additional commitments to Client:
   a) Cleverbridge will maintain a record of all categories of processing activities carried out on Client's behalf to the extent required to enable Client to comply with its obligations under applicable data protection laws, and require any sub-processors to do the same.
   b) Cleverbridge will also take reasonable steps to ensure the reliability and obligation to confidentiality of any person authorized to process personal data, and will implement and maintain appropriate technical and organizational data protection and security measures to ensure the security and accountability of the personal data as required under Article 32 of the GDPR and various provisions of the CCPA.
   c) Cleverbridge will maintain policies and procedures that determine whether personnel and third parties engaged by Cleverbridge are suitable for their roles, and provide appropriate training and information. Cleverbridge maintains a security awareness program for personnel which provides training and awareness on corporate security policies and compliance with PCI-DSS
   d) Cleverbridge will maintain business continuity and disaster recovery plans designed to maintain Cleverbridge's delivery of the services with minimal interruption. Each plan will detail measures to support the restoration of full operations as soon as possible after an emergency. The plans will addresses the need for failover capability and provision of an alternate recovery site based upon the criticality of the business functions, with input from the business owners. Plans will be periodically tested to make Cleverbridge's most critical business applications readily available in the event of a declared disaster. Backups will be stored offsite from the primary data source to support the recoverability of data importer systems in the event of a disaster.