WebBeds Client Data Protection Terms and Standard Contractual Clauses (Controller to Controller).

These Data Protection Terms (the "Terms") and Standard Contractual Clauses supplement the Client Agreement between Client and WebBeds Contracting Party or WebBeds Contracting Parties (together "WebBeds"), or other agreement between Client and WebBeds, governing Client's use of the WebBeds Services (the "Agreement").

Definitions

"Data Privacy Laws" means all applicable laws governing the handling of Personal Data, including but not limited to, *EC Regulation 2016/679* ("GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the *e-Privacy Directive (Directive 2002/58/EC)* (the "e-Privacy Directive") (collectively, "EU Data Protection Law"); the GDPR as it forms parts of the United Kingdom domestic law by virtue of *Section 3 of the European Union (Withdrawal) Act 2018* ("UK GDPR"); and (2) the local law of the place(s) where Processing by a party and its Personnel takes place; in each case, all of the foregoing as amended, replaced or supplemented from time to time, and all subordinate legislation made under them, together with any codes of practice, regulations or other guidance issued by the governments, agencies, data protection regulators, or other authorities in the relevant countries or jurisdictions.

"Controller Personal Data" means any Personal Data that is provided or made available by a Party to the other Party under the Agreement in connection with the providing party's provision or use (as applicable) of WebBeds Services.

"Data Subject" means a natural person to whom any Controller Personal Data pertains.

"EEA" means the European Economic Area.

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure of Personal Data. The terms "process", "processes" and "processed" will be interpreted accordingly.

"Personal Data" or the equivalent 'personal information' means any information relating, directly or indirectly, to an identified or identifiable natural person or otherwise as defined in the applicable Data Privacy Laws.

"Personal Data Breach" means confirmed unauthorised, accidental, or unlawful Processing, access, loss, or disclosure of Controller Personal Data.

"Personnel" means all officers, directors and employees, independent contractors, or service providers of a party.

"Services" means the services as described in the Agreement.

The terms "controller", and "processor" as used in the Terms have the meanings given in the GDPR.

Roles of the parties

For purposes of EU Data Protection Law, WebBeds and Client will act as independent controllers of the data. Each party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under EU Data Protection Law. The parties agree that they are not joint Controllers of any Controller Personal Data. Each party will individually determine the purposes and means of its Processing of Controller Personal Data.

Obligations of the parties

a) Each Party shall comply with all applicable requirements of Data Privacy Laws.
b) Each Party represents and warrants at all times that:
   i. it has the necessary right and authority to enter into the Terms and to perform its obligations herein;
   ii. its execution and performance under the Terms and the Agreement will not violate any agreement to which it is a party;
   iii. it has provided all required information to Data Subjects including, where required, that Personal Data that may be passed to third parties for the purposes of the Agreement;
   iv. in collecting Controller Personal Data, it did not violate Data Privacy Laws;
   v. where required, it has obtained any legally required consent to the collection, use and disclosure of Controller Personal Data to allow WebBeds to Process such Controller Personal Data in connection with the Services; and
   vi. where required, it has notified the Data Subjects of the identity and details of WebBeds as the recipient and independent controller of the Controller Data.

c) Without limiting the foregoing, each party will maintain a publicly accessible privacy policy on its website that is compliant with Data Privacy Laws.

d) Each party will notify the other in writing of any action or instruction of the other party under the Terms or the Agreement which, in its opinion, infringes applicable Data Privacy Laws.

e) Subject to the Terms, each party, acting as a Controller, may Process the Controller Personal Data in accordance with, and for the purposes permitted in, the Agreement.

f) The types of Controller Personal Data that may be processed are set out in Schedule 1, Annex 1.

Security and Confidentiality

Each party shall implement appropriate technical and organisational measures to protect the Controller Personal Data from unauthorised, accidental, or unlawful access, loss, disclosure, or destruction. In the event that a party suffers a Personal Data Breach, it shall notify the other party without undue delay and both parties shall cooperate in good faith to agree and take such measures as may be necessary to mitigate or remedy the effects of the Personal Data Breach.

Nothing herein prohibits either party from providing notification of the Personal Data Breach to regulatory authorities as may be required by Data Protection Laws prior to notification of the other party, so long as the notifying party provides notification to the other party without undue delay. Each party shall ensure that all of its Personnel who have access to and/or Process Controller Personal Data are obliged to keep the Controller Personal Data confidential.

Transfers outside the EEA

Where a Party receiving Controller Personal Data is located in a country not recognized by the European Commission as providing an adequate level of protection for Personal Data within the meaning of EU Data Protection Law, the Standard Contractual Clauses ("SCCs") in Schedule 1 shall apply as between the parties, and such SCCs are incorporated herein by reference. To extent that and for so long as the SCCs as implemented in accordance with the Terms and the Agreement cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference, and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in the Annexes to Schedule 1 of the Terms.

Data Subject Requests and Cooperation.

Each party will process its own requests for Data Subjects to exercise their individual rights. With respect to requests from, or on behalf of Data Subjects to the Processing of Personal Data that is shared between the parties, the parties will collaborate to honor such requests.
Both parties agree to reasonably cooperate and assist each other in relation to any complaint or investigation concerning the Controller Personal Data shared between the parties.

Data Retention.

Both parties shall fulfill their obligations with regards to their respective data retention periods as stated in their respective privacy policies.

Liability and Costs.

The liability of the Parties under or in connection with this Agreement will be subject to the exclusions and limitations of liability in the Agreement. Each party shall perform its obligations under this the Terms at its own cost, except as otherwise specified herein.

Miscellaneous.

If any provision or condition of the Terms is held or declared invalid, unlawful, or unenforceable by a competent authority or court, then the remainder of the Terms shall remain valid. The Terms shall be governed by and construed in accordance with the laws governing the Agreement, and any disputes shall be resolved by the courts agreed for resolution of disputes under the Agreement.

Schedule 1: Standard Contractual Clauses (Controller to Controller)

Section I.

Clause 1

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

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

3 Third-party beneficiaries

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

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

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

(iii) N/A

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

(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

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

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

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

7 Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Section II – Obligations of the Parties.

Clause 8

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

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

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

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

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

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

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

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

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

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

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

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

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

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

Clause 9

9 Use of sub-processors

N/A

Clause 10

10 Data subject rights

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

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

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing

meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

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

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

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

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

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

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

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

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

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

Clause 11

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

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

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

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

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

Clause 13

13 Supervision

a) 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.

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

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).

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

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

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon

as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

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

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

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

15.2 Review of legality and data minimisation

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

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

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

Section IV – Final provisions.

Clause 16

16 Non-compliance with the Clauses and termination

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

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until

compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

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 Spain.

Clause 18

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 Spain.

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.

---

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

[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.

[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.

[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.

[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.

ANNEX I.

A. List Of Parties

Data exporter:

Name: Client (as specified in the Agreement).

Address: Address of Client as specified in the Agreement.

Contact person's name, position

and contact details: Contact details for the data exporter are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The data exporter uses the Services of the data importer in accordance with the Agreement.

Signature and date: The parties agree that in compliance with their respective obligations under the Agreement and the requirements of *Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation*) the execution of the Agreement and continued use of the Services pursuant to the Agreement, shall constitute execution of these Clauses by both parties.

Role: Controller

Data importer(s):

Name: WebBeds FZ-LLC (trading as Sunhotels, Lots of Hotels, FIT Ruums, Destinations of the World ("DOTW") and/or JacTravel)

Address:	Suite 3210-3213 Al Shatha Tower, PO Box 502115, Dubai
Contact person name:	Tammy Helg
Position:	Data Protection Officer
Contact details:	Email: dpo@webjetlimited.com **Phone:** +613 9828 9500

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that in compliance with their respective obligations under the Agreement and the requirements of *Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation*) the execution of the Agreement and continued use of the Services pursuant to the Agreement, shall constitute execution of these Clauses by both parties.

Role: Controller

B. Description Of Transfer

Categories of data subjects whose personal data is transferred

The individuals about whom personal data is provided to the data importer via the Services by (or at the direction of) the data exporter, including:

- Consumers (i.e., the end-travelers benefiting from reservations arranged in connection with the Agreement); and
- Clients (i.e., staff of, or persons authorised to act on behalf of, the Client).

Categories of personal data transferred

- contact information (customer name addresses, telephone numbers, emails addresses);
- passport and/or VISA information (if applicable);
- financial payment information (such as credit card and bank account details);
- passport and/or VISA information (if applicable)
- financial payment information (such as credit card and bank account details);
    - information regarding dietary requirements (is necessary to facilitate Consumer requirements or requests);
    - information regarding disabilities (if necessary to facilitate Consumer accessibility requirements or requests,).

Sensitive data transferred (if applicable)

Personal data transferred via the Services by (or at the direction of) the data exporter may include special categories of personal data. This may include, for example: personal data revealing racial or ethnic origin, religious or philosophical beliefs, data concerning health or data concerning a natural person's sex life or sexual orientation, if such information is necessary to provide the Services to the Consumer.

The restrictions and safeguards specified in Annex II apply to these categories of sensitive data (if any). Sensitive data shall be transferred and processed only when necessary for the purpose identified below.

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

Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the Agreement (as applicable).

Nature of the processing

The data importer will process personal data to provide, secure and monitor the Services in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

The data importer will transfer and process personal data to provide, secure and monitor the Services accordance with 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

For the duration of the Agreement, until deletion in accordance with the provisions of the Agreement (as applicable) when no longer necessary for the purpose identified above.

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

The data may be transferred to suppliers of the Services (including hotels and other travel and tourist service providers for the purpose of identified above, for the duration necessary to fulfil the purpose identified above.

C. Competent Supervisory Authority

Agencia Española de Protección de Datos ("AEPD")

C/Jorge Juan, 6, 28001 Madrid, Spain

Telephone: +34 901 100 099/ +34 91 266 35 17

Website: www.aepd.es

ANNEX II- Technical and organisational measures including technical and organisational measures to ensure the security of the data.

1. Security Governance and Compliance

a) The Data Importer maintains an information security management system which documents the Data Importer's security policies, responsibilities, practices, procedures, processes, and resources, used by the Data Importer to manage information security in respect of the provision of the Services, including in relation to the accessing and processing of personal data.

b) The Data Importer ensures that at all times it maintains sufficient resources, management structures and management oversight to allow it to meet its security obligations under the Agreement.

c) The Data Importer uses auditable, repeatable, and integrated processes to effectively identify, manage and report risks in a manner that is consistent with the nature and scope of the Services.

2. Data Protection

a) Data Importer will protect the confidentiality, authenticity, and integrity of the personal data at rest as well as in transit processed within the infrastructure of the Data Importer or sub-contractors (including processors) Data Importer has engaged to provide services under the Agreement.

b) Personal data will be encrypted while transmitted over external networks using TLS 1.2 or above. Encryption algorithms and technologies in use shall be publicly validated and subject to the acceptable industry standards.

3. Data Availability

a) Data Importer ensures that back-up of all relevant personal data is made immediately prior to any modification, update, upgrade or other change to its system or the Services that may affect any the personal data.

b) Data Importer has implemented controls to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

C) Data Importer regularly tests and updates business continuity and disaster recovery plans to ensure that they are up to date and effective.

4. Data Access

a) Data Importer maintains controls to prevent unauthorized access to systems, networks, applications, and data (including personal data). Data Importer maintains access management practices that ensure:

(i) access is granted through an access profile (role);

(ii) access rights are assigned to a role on a need-to-know basis and least privilege basis to ensure segregation of duties and the assignment of roles follows a structured and documented procedure;

(iii) users have a unique identifier for their own use so that activities can be traced to the responsible individual;

(iv) withdrawal of access to personal data and related assets is performed in a timely manner for personnel who exit Data Exporter's organization or are re-assigned outside the scope of services under the Agreement;

(v) user accounts and system privileges are regularly reviewed;

(vi) the use of strong passwords according to industry standards on all systems processing or storing personal data;

(vii) remote access to systems uses multi-factor authentication and is only provided on a needs basis.

b) In relation to any access to or use of any part of the Services, system or infrastructure, the Data Exporter must comply with Data Importer's security policies and practices as current from time to time and notified to the Data Exporter.

5. Data Handling

a) Data Importer ensures that any personal data that it processes is classified and managed in accordance with applicable information classification and data management standards.

b) Data Importer ensures that all personnel delivering Services under the Agreement are made aware of and trained on information security threats and are equipped to support organizational information security policies in general as well as within their specific job functions.

c) Data Importer maintains disciplinary procedures to sanction individual unintentional or intentional misconduct leading to a breach of information security policies and procedures.

6. Physical Security

a) Data Importer maintains effective procedures to prevent unauthorized physical access, damage, and interference to processing facilities, systems, networks, and information, including personal data, used in delivery of Services, including but not limited to:

(i) procedures to monitor physical access to ensure that only authorized personnel are allowed access;

(ii) controls to prevent unauthorized removal of personal data related to the Services on portable storage media by personnel.

7. Vulnerabilities Management & Change Management

a) Data Importer has implemented appropriate change management and capacity management processes, including reviewing and testing all changes before they are deployed in a live environment to ensure that it maintains secure operations of information processing systems.

b) Data Importer ensures that security is included in development and support processes to maintain the security of application system software and information, including by ensuring that segregation of duty is enforced amongst individuals with development responsibilities and

production privileges and by implementing adequate procedural controls to prevent the usage of production data in a test environment.

c) The Data Importer uses an appropriate risk assessment framework to measure risk related to technical vulnerabilities in order to define patch severity/criticality level and shall maintain a vulnerability management process that reduces risks resulting from exploitation of vulnerabilities.

d) Data Importer obtains timely information about vulnerabilities applicable to systems, applications and networks being used for or connected to the delivery of services under the Agreement and shall evaluate their exposure to such vulnerabilities and take appropriate measures to address the associated risk in a timely manner.

8. Risk Assessment and Audit

Data Importer has established and implemented processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of personal data handling commensurate with the risk involved in performing the Services in scope of the Agreement.

9. Security Incident Management

a) Data Importer maintains a consistent and effective approach for security incident management, which includes monitoring capabilities and effective procedures to detect and manage in a timely manner, events indicating a potential Security Incident.

b) The Data Importer performs daily monitoring of the critical events in its environment and have the technical capability to detect anomalies and malicious behaviour.

c) Data Importer has implemented reasonable controls in order to restore the availability and access to personal data in a timely manner in the event of a Security Incident.

d) Upon becoming aware of a Security Incident related to systems or data relevant for the delivery of Services under the Agreement Data Importer shall notify Data Exporter as soon as is reasonably practicable. The parties agree to promptly cooperate with each other in any investigations or enquiries of the Security Incident, including by a regulatory or law enforcement agency, and through third-party forensics professionals.

10. PCI-DSS Compliance

If the Data Importer obtains, processes or transfers credit or debit, or any other form of payment card details (including the account number, cardholder name, expiry date and card verification number), the Data Importer shall ensure compliance with the Payment Card Industry Data Security Standard (PCI-DSS) in effect from time to time.

11. Solutions Security

a) To the extent the Data Importer is providing a software solution to the Data Exporter, the Data Importer shall ensure that:

b) The solution supports Single-Sign-On (SSO) protocols such as SAML2.0 or OAuth/OIDC and that this can be enforced as the only login method.

c) The solution supports Multi-factor Authentication (MFA).

d) The solution provides audit logging and alerting capabilities that can be enabled to monitor user activities and transactions.

e) The solution includes patching of the solution/application as part of the scope of the Agreement.

f) The solution includes Role Based Access Controls that allow separation of duties and permissions for individual users (e.g., Administrators vs. regular users).