DATA PROCESSING ADDENDUM

(Rev. April 30, 2018)

This Data Processing Addendum ("**DPA**") forms part of the Master Services Agreement or other written or electronic agreement between BE and Client for the purchase of online from BE (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as **"Services"**) (the **"Agreement"**) to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent BE processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term **"Client"** shall include Client and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

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

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3 (including Appendices 1 and 2) and 4.
2. This DPA has been pre-signed on behalf of BE. The Standard Contractual Clauses in Schedule 3 have been pre-signed by Brand Embassy Ltd. as the data importer.
3. To complete this DPA, Client must:
   (a) Complete the information in the signature box and sign on Page 6.
   (b) Complete the information as the data exporter on Page 11.
   (c) Complete the information in the signature box and sign on Pages 14, 16 and 17.
4. Send the completed and signed DPA to BE by email to legal@brandembassy.com.

Upon receipt of the validly completed DPA by BE at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Client entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Brand Embassy entity that is party to the Agreement is party to this DPA.

If the Client entity signing this DPA has executed an Order Form with BE or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Brand Embassy entity that is party to such Order Form is party to this DPA.

If the Client entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Client entity who is a party to the Agreement executes this DPA.

If the Client entity signing the DPA is not a party to an Order Form nor a Master Services Agreement directly with BE, but is instead a customer indirectly via an authorized reseller of Services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Client Data contained in Client's Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. **"Authorized Affiliate"** means any of Client's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Client and BE, but has not signed its own Order Form with BE and is not a "Client" as defined under the Agreement.

1.3. **"BE" (or "Provider")** means the Brand Embassy entity which is a party to this DPA, being Brand Embassy Ltd, a company registered in England and Wales.

1.4. **"BE Group"** means BE and its Affiliates engaged in the Processing of Personal Data.

1.5. **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

1.6. **"Client Data"** means what is defined in the Agreement as "Client Content".

1.7. **"Data Protection Laws"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

1.8. **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

1.9. **"GDPR"** means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10. **"Personal Data"** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), where for each (i) or (ii), such data is Client Data.

1.11. **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12. **"Processor"** means the entity which Processes Personal Data on behalf of the Controller.

1.13. **"Standard Contractual Clauses"** means the agreement executed by and between Client and Brand Embassy Ltd. and attached hereto as Schedule 3 pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

1.14. **"Sub-processor"** means any Processor engaged by BE or a member of the BE Group.

1.15. **"Supervisory Authority"** means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Controller, BE is the Processor and that BE or members of the BE Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. **Client's Processing of Personal Data.** Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

2.3. **BE's Processing of Personal Data.** BE shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Client's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by BE is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data 2 (Subjects Processed under this DPA are further specified in Schedule Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS - DATA SUBJECT REQUESTS

BE shall, to the extent legally permitted, promptly notify Client if BE receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (**"Data Subject Request"**). Taking into account the nature of the Processing, BE shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, BE shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent BE is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from BE's provision of such assistance.

4. BE PERSONNEL

4.1. **Confidentiality.** BE shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. BE shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Reliability.** BE shall take commercially reasonable steps to ensure the reliability of any BE personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access.** BE shall ensure that BE's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Client acknowledges and agrees that (a) BE's Affiliates may be retained as Sub-processors; and (b) BE and BE's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. BE or a BE Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. **List of Current Sub-processors.** BE shall make available to Client the current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Sub-processor Lists**"). The current Sub-processor Lists is available at www.brandembassy.com/legal/subprocessors.

5.3. **New Sub-processors.** Brand Embassy's use of Sub-processors is at its discretion, provided that:

(a) Brand Embassy will notify Client in advance (by email or by posting by posting at www.brandembassy.com/legal/subprocessors) of any changes to the list of Sub-processors in place on the Agreement Effective Date (except for Emergency Replacements or deletions of Sub-processors without replacement).

(b) If Client has a legitimate reason that relates to the Sub-processors' processing of Personal Data, Client may object to Brand Embassy's use of a Sub-processor, by notifying Brand Embassy in writing within thirty days after receipt of Brand Embassy's notice. If Client objects to the use of the Sub-processor, the parties will come together in good faith to discuss a resolution. Brand Embassy may choose to: (i) not use the Sub-processor or (ii) take the corrective steps requested by Client in its objection and use the Sub-processor. If none of these options are reasonably possible and Client continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Client does not object within thirty days of receipt of the notice, Client is deemed to have accepted the new Sub-processor.

(c) If Client's objection remains unresolved sixty days after it was raised, and Brand Embassy has not received any notice of termination, Client is deemed to accept the Sub-processor.

5.4. **Emergency Replacement.** Brand Embassy may change a Sub-processor where the reason for the change is outside of Brand Embassy's reasonable control. In this case, Brand Embassy will inform Client of the replacement Sub-processor as soon as possible. Client retains its right to object to a replacement Sub-processor under Section 4.2(b).

5.5. **Liability.** BE shall be liable for the acts and omissions of its Sub-processors to the same extent BE would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

Controls for the Protection of Client Data. BE shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), confidentiality and integrity of Client Data, as set forth in Schedule 1 attached hereto. BE regularly monitors compliance with these measures. BE will not materially decrease the overall security of the Services during a subscription term.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

BE shall, notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data, including Personal Data, transmitted, stored or otherwise Processed by BE or its Sub-processors of which BE becomes aware (a "**Client Data Incident**"). BE shall make reasonable efforts to identify the cause of such Client Data Incident and

take those steps as BE deems necessary and reasonable in order to remediate the cause of such a Client Data Incident to the extent the remediation is within BE's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's Users.

8. RETURN AND DESTRUCTION OF CLIENT DATA

Upon termination of the Agreement or otherwise under instruction from Client, the Client Data shall be destroyed, provided that if the Provider is required to retain any data for valid legal or regulatory reasons such data may be retained by the Provider. Client acknowledges that Client Data stored by Supplier in backup logs and files are not automatically purged, and ages out of the system as part of the data lifecycle but in any event the Client Data will be destroyed within the timelines set forth in Schedule 4, entitled 'Data Deletion Procedures'. In such instances, the Provider undertakes that it will maintain the confidentiality of the Client Data transferred and will not actively process the Client Data transferred any further.

9. AUTHORIZED AFFILIATES

9.1. **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, the Client enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between BE and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Client.

9.2. **Communication.** The Client that is the contracting party to the Agreement shall remain responsible for coordinating all communication with BE under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3. **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with BE, it shall to the extent required under applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against BE directly by itself, the parties agree that (i) solely the Client that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Client that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2. The parties agree that the Client that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on BE and its Sub-Processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and BE, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, BE's and its Affiliates' total liability for all claims from the Client and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Client and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

11. EUROPEAN SPECIFIC PROVISIONS

11.1. **GDPR.** With effect from 25 May 2018, BE will Process Personal Data in accordance with the GDPR requirements directly applicable to BE's provision of its Services.

11.2. **Data Protection Impact Assessment.** With effect from 25 May 2018, upon Client's request, BE shall provide Client with reasonable cooperation and assistance needed to fulfil Client's obligation under the GDPR to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to BE. BE shall provide reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

11.3. **Transfer mechanism for data transfers.** Subject to the additional terms in this Section 11.3, to the extent the Services involve a transfer of Personal Data originating from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to Sub-processors located in countries outside the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom that have not received a binding adequacy decision by the European Commission or by a competent national EEA data protection authority, such transfers are subject to the terms of the Standard

Contractual Clauses incorporated into this Data Processing Addendum by reference, which are subject to the additional terms in this Section 11.3 below. For the purposes of the Standard Contractual Clauses, Client and BE agree that (i) Client will act as the data exporter on Client's own behalf and on behalf of any of Client's entities, (ii) Brand Embassy will act on its own behalf and/or on behalf of the relevant Brand Embassy Affiliates as the data importers, (iii) any third party Sub-processors will act as 'subcontractors' pursuant to Clause 11 of the Standard Contractual Clauses.

11.3.1. **Clients covered by the Standard Contractual Clauses.** The Standard Contractual Clauses and the additional terms specified in this Section 11.3 apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Client established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Services. For the purpose of the Standard Contractual Clauses and this Section 11.3, the aforementioned entities shall be deemed "data exporters".

11.3.2. **Instructions.** This DPA and the Agreement are Client's complete and final documented instructions at the time of signature of the Agreement to BE for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Client to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

11.3.3. **Appointment of new Sub-processors and List of current Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that (a) BE's Affiliates may be retained as Sub-processors; and (b) BE and BE's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. BE shall make available to Client the current list of Sub-processors in accordance with Section 5.2 of this DPA

11.3.4. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that BE may engage new Sub-processors as described in Section 5.3 of the DPA.

11.3.5. **Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by BE to Client pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by BE beforehand; and, that such copies will be provided by BE, in a manner to be determined in its discretion, only upon request by Client.

11.3.6. **Audits.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Client may contact BE in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Client shall reimburse BE for any time expended for any such on-site audit at the BE Group's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of any such on-site audit, Client and BE shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by BE. Client shall promptly notify BE with information regarding any non-compliance discovered during the course of an audit.

11.3.7. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by BE to Client only upon Client's request.

11.3.8. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

12. LEGAL EFFECT

This DPA shall only become legally binding between Client and BE (and Brand Embassy Ltd., if different) when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

LIST OF SCHEDULES

Schedule 1: Technical and Organizational Measures

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

Schedule 4: Data Deletion Procedures

The parties' authorized signatories have duly executed this Agreement:

[Signature page follows]

Provider: **Brand Embassy Ltd.**

Dated:

_____

Name: Damián Brhel
Title: Director

Client:

Dated:

_____

Name:
Title:

_____

Name:
Title:

SCHEDULE 1

TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the Provider's current security measures. Provider may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

1. Physical Access Control

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- Provider protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Provider buildings must register their names at reception and must be accompanied by authorized Provider personnel.

Additional measures for data centers:

- All third-party data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To ensure proper functionality, physical security equipment (e.g., CCTV, surveillance and detection systems, etc.) undergo maintenance on a regular basis.
- All third-party data center providers log the names and times of persons entering Provider's private areas within the data centers.

2. System Access Control

Data processing systems used to provide the Services must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access Provider's systems with a unique identifier (user ID).
- Provider has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- Provider has established a password rules that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Provider uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to Provider's corporate network and critical infrastructure is protected by strong authentication.

3. Data Access Control

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

- As part of the Provider's security rules, Personal Data requires at least the same protection level as "confidential" information.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. Provider uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the Provider security policies and standards. Confidential information must be processed confidentially.

- All production servers are operated in the data centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, Provider conducts internal security checks and penetration tests on its IT systems.
- Provider does not allow the installation of personal software or other software that has not been approved by Provider.
- A Provider security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

4. Data Transmission Control

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Provider to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data transfer over Provider internal networks are protected in the same manner as any other confidential data according to Provider security rules.
- When data is transferred between Provider and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Provider-controlled systems (e.g. data being transmitted outside the firewall of the Provider data center).

5. Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Provider data processing systems.

Measures:

- Provider only allows authorized persons to access Personal Data as required in the course of their work.
- Provider undertakes to implement a logging system for input, modification and deletion, or blocking of Personal Data by Provider or its subprocessors within Provider's Services to the fullest extent possible.

6. Job Control

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer.

Measures:

- Provider uses controls and processes to ensure compliance with contracts between Provider and its customers, subprocessors or other service providers.
- As part of the Provider security rules, Personal Data requires at least the same protection level as "confidential" information.
- All Provider employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Provider customers and partners.

7. Availability Control

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Provider employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.
- Provider undertakes to define contingency plans as well as business continuity and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

8. Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

- Provider uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

9. Data Integrity Control

Personal Data will remain intact, complete and current during processing activities.

Measures:

Provider undertakes to implement a multi-layered defense strategy as a protection against unauthorized modifications. Provider uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Antivirus software;
- Backup and recovery;
- Internal penetration testing;

SCHEDULE 2

DETAILS OF THE PROCESSING

Nature and Purpose of Processing

BE will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.

Duration of Processing

Subject to Section 8 of the DPA, BE will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- individuals collaborating and communicating with Client's customers, followers, fans and other internet users who use social networks, email, mobile applications and websites and Client's employees, agents and Client's subcontractors' employees operating the Services ("Account Data")
- Client's customers, followers, fans and other internet users communicating with Client's users via email or live chat tool ("Chat Data")
- Client's customers, prospects, marketing addresses etc. uploaded or imported by Client into the Services ("Client Content")
- Client's customers, followers, fans and other internet users who use social networks, email, mobile applications and websites, currently including, but not limited to, Facebook, Twitter, Google+, Youtube, Vkontakte, Instagram, WhatsApp, forums and websites owned by Client where Data Importer provides social and content management functionality on Client's behalf ("Social Data").

Type of Personal Data

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Account Data: transferred concern identification data (name, login), contact information (business email address) and work-related information (usage and/or performance data, social contact handling data)
- Client Content transferred concerns any category of Personal Data the Client uploads and/or stores into the Platform;
- Social Data transferred concerns content published or sent by social media users via Client's social media (such as Client's Facebook page), connected to the Platform (both public and private messages to Client) and publicly accessible data from social media networks and websites based on certain search queries defined by the Client. Social Data includes user IDs, social network profile names and information, profile picture, social network communications, email address and all kind of information shared across social media network and websites.
- Chat Data transferred concern name, email address, geolocation data, IP address, internet browser history (LiveChat only).

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization:

Address:

Tel.: ; e-mail:

Other information needed to identify the organization: ……

(the **data exporter**)

And

Name of the data importing organization: Brand Embassy Ltd.

Address: 1st Floor (North), Devonshire House, 1 Devonshire Street, London, W1W 5DS, The United Kingdom of Great Britain and Northern Ireland

e-mail: privacy@brandembassy.com

Other information needed to identify the organization: Company reg. ID: 07814317

(the **data importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 ***Definitions***

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 ***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 ***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 ***Obligations of the data importer***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 ***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 ***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data

protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ON BEHALF OF THE DATA EXPORTER:

Name (written out in full): Damián Brhel
Title: Director
Address: 1st Floor (North), Devonshire House, 1 Devonshire Street, London, W1W 5DS, The United Kingdom of Great Britain and Northern Ireland
Other information necessary in order for the contract to be binding (if any):

Signature……

ON BEHALF OF THE DATA IMPORTER:

Name (written out in full):
Title:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……

APPENDIX 1

TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter
The Data Exporter subscribed to a Services that allows Users to enter, amend, use, delete or otherwise process Personal Data.

Data Importer
The Data Importer provides the Services.

Data Subjects
The Personal Data transferred concern the following categories of Data Subjects:

- individuals collaborating and communicating with Data Exporter's customers, followers, fans and other internet users who use social, email, mobile applications, networks and websites and Data Exporter's employees, agents and Data Exporter's subcontractors' employees operating the Services ("Account Data");
- Data Exporter's customers, prospects, marketing addresses etc. uploaded or imported by Data Exporter into the Services ("Client Content")
- Data Exporter's customers, followers, fans and other internet users who use social networks, email, mobile applications and websites, currently including, but not limited to, Facebook, Twitter, Google+, Youtube, Vkontakte, Instagram, WhatsApp, forums and websites owned by Data Exporter where Data Importer provides social and content management functionality on Data Exporter's behalf ("Social Data").
- Client's customers, followers, fans and other internet users communicating with Client's users via email or live chat tool ("Chat Data")

Data Categories
The Personal Data transferred concerns the following categories of data:

- Account information transferred concern identification data (name, login), contact information (business email address) and work-related information (usage and/or performance data, social contact handling data)
- Client Content transferred concerns any category of Personal Data the Data Exporter uploads and/or stores into the Services;
- Social Data transferred concerns content published or sent by social media users via Data Exporter's social media (such as Data Exporter's Facebook page), connected to the Services (both public and private messages to Data Exporter) and publicly accessible data from social media networks and websites based on certain search queries defined by the Data Exporter. Social Data includes user IDs, social network profile names and information, profile picture, social network communications, email address and all kind of information shared across social media network and websites.
- Chat Data transferred concern name, email address, geolocation data, IP address, internet browser history (LiveChat only).

Special Data Categories (if appropriate)
The Personal Data transferred concerns the following special categories of data:

- Customer Content transferred may contain special categories of data, depending on what kind of data the Data Exporter uploads and/or stores into the Services.
- Social Data transferred may concern special categories of Personal Data, depending on Data Exporter's usage of the Brand Embassy Platform (such as definition of special search queries for collection of publicly accessible personal data on social media network or websites.

Processing Operations
The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Services (including Customer Care)
- provision of Professional Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centres (multi-tenant architecture)
- upload any fixes or upgrades to the Platform
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Client in accordance with this Agreement

Processing Operations
The Personal Data transferred will be subject to the following basic processing activities:

- Account Data transferred will be processed solely for the purpose of operating the Platform (authentication, login, audit trail)

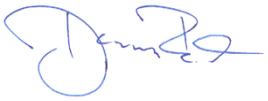
- Customer Content, Chat Data and Social Data transferred are processed for purposes of social media management, including social media listening and analytics, customer care and support, marketing analytics and management.

Instructions
The DPA and the Agreement are Data Exporter's complete instructions at the time of the signature of the DPA to Brand Embassy for the processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Data Exporter to process Personal Data: (i) processing in accordance with the MSA, (ii) processing initiated by Users in their use of the Platform and (iii) processing to comply with other documented reasonable instructions provided by Data Exporter.

Audits and Inspections
The audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section 6 of the DPA.

Certification of Deletion
The certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Brand Embassy to Data Exporter only upon Data Exporter's request.

ON BEHALF OF THE DATA EXPORTER:



Signature……
Name: Damián Brhel
Title: Director

ON BEHALF OF THE DATA IMPORTER:

Signature……
Name:
Title:

APPENDIX 2

TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Schedule 1 to the DPA. Data Importer will not materially decrease the overall security of the Services during a subscription term.

ON BEHALF OF THE DATA EXPORTER:

Signature……
Name: Damián Brhel
Title: Director

ON BEHALF OF THE DATA IMPORTER:

Signature……
Name:
Title:

Schedule 4

Data Deletion Procedures

Brand Embassy will, unless otherwise required by Data Protection Laws and subject to Brand Embassy's Storage Period, either overwrite, make inaccessible, or return to the Controller all Controller Personal Data upon termination or expiration of the Agreement. For the avoidance of doubt, the Controller can request download of the Content via the Services in accordance with the Agreement.

For the purposes of this Schedule 4, "Storage Period" means the period in which Brand Embassy overwrites Personal Data contained within Content (which is approximately on a rolling thirteen (13) month basis).