BrandSwap Limited

Data Processing Agreement

This agreement is dated [DATE]

PARTIES

1. [FULL COMPANY NAME] incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (Customer)
2. BrandSwap Limited incorporated and registered in England and Wales with company number 1424 4549 whose registered office is at 1 Barons Court Graceways, Whitehills Business Park Blackpool. FY4 5GP (Provider)

BACKGROUND

1. The Customer and the Provider entered into a Master Service Agreement (“Service Agreement”) that may require the Provider to process Personal Data on behalf of the Customer.
2. This Personal Data Processing Agreement (“Agreement”) sets out the additional terms, requirements and conditions on which the Provider shall process Personal Data when providing services under the Service Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) for contracts between controllers and processors and the General Data Protection Regulation ((EU) 2016/679) (EU GDPR).

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

* 1. Definitions:

1. Business Purposes: The services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified in ANNEX A.
2. **Commissioner**:The Information Commissioner (see Article 4(A3), UK GDPR and section 114 of the UK Data Protection Act (DPA 2018).
3. **Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing**: have the meanings given to them in the Data Protection Legislation.
4. **Data Protection Legislation:**
   1. To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.
   2. To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or Provider is subject which relates to the protection of personal data.
5. Data Subject: The identified or identifiable living individual to whom the Personal Data relates.
6. EU GDPR: The General Data Protection Regulation ((EU) 2016/679).

EEA: The European Economic Area.

1. Personal Data: Means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Service Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
2. Processing, processes, processed, process: Any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third parties.
3. Personal Data Breach: A breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
4. **Processor**: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
5. **Records**: Has the meaning given to it in Clause 12.
6. **Term**: This Agreement's term as defined in Clause 10.
7. **UK GDPR:** Has the meaning given to it in section 3(10) as supplemented by section 205(4) of the DPA 2018.
   1. This Agreement is subject to the terms of the Service Agreement and is incorporated into the Service Agreement. Interpretations and defined terms set forth in the Service Agreement apply to the interpretation of this Agreement.
   2. The Annexes form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.
8. Personal data types and processing purposes
   1. The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:
      1. the Customer is the Controller and the Provider is the Processor.
      2. ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.
9. Provider's obligations
   1. The Provider shall only process the Personal Data to the extent and in such a manner as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider shall not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider shall notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.
   2. The Provider shall comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data or to stop, mitigate or remedy any unauthorised processing.
   3. The Provider shall maintain the confidentiality of the Personal Data and shall not disclose the Personal Data to third parties unless it is required by domestic or EU law, court or regulator including the Commissioner. If a domestic or EU law, court or regulator including the Commissioner requires the Provider to process or disclose the Personal Data to a third-party, the Provider shall inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement unless the domestic or EU law prohibits the giving of such notice.
   4. The Provider shall reasonably assist the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.
   5. The Provider shall notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of the Service Agreement or this Agreement.
10. Provider's employees
    1. The Provider shall ensure that all of its employees:
       1. are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;
       2. are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.
11. Security
    1. The Provider shall at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including but not limited to the security measures set out in ANNEX B.
    2. The Provider shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
       1. the pseudonymisation and encryption of personal data;
       2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
       3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
       4. a process for regularly testing, assessing and evaluating the effectiveness of the security measures.
12. Personal data breach
    1. The Provider shall without undue delay notify the Customer in writing if it becomes aware of:
       1. the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider shall restore such Personal Data at its own expense as soon as possible.
       2. any accidental, unauthorised or unlawful processing of the Personal Data; or
       3. any Personal Data Breach.
    2. Following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties shall co-ordinate with each other to investigate the matter. Further the Provider shall reasonably co-operate with the Customer in the Customer's handling of the matter, including but not limited to:
       1. assisting with any investigation;
       2. providing the Customer with physical access to any facilities and operations affected;
       3. facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;
       4. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and
       5. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.
    3. The Provider agrees that the Customer has the sole right to determine:
       1. whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion including the contents and delivery method of the notice; and
       2. whether to offer any type of remedy to affected Data Subjects including the nature and extent of such remedy.
13. Cross-border transfers of personal data
    1. The Provider shall transfer or otherwise process the Personal Data outside the UK or the EEA to a third country or international organisations when necessary, without obtaining the Customer's prior consent as long as adequate safeguards are in place in accordance with Article 45 and Article 46 of the UK GDPR or EU GDPR.
14. Subprocessors

8.1 The Provider has the Customer’s general authorisation for the engagement of subprocessor(s) from an agreed list. The Provider shall specifically inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The Provider shall provide the Customer with the information necessary to enable the Customer to exercise its right to object.

* 1. Where the Provider engages a sub-processor(s) to carry out specific processing activities on behalf of the Customer it shall do so by way of a written contract that provides for in substance the same data protection obligations as those binding the Provider under these clauses including in terms of third-party beneficiary rights for data subjects.
  2. The Provider shall remain fully responsible to the Customer for the performance of the sub-processor’s obligations under its contract with the Provider. The Provider shall notify the Customer of any failure by the sub-processor to fulfil its obligations under that contract.
  3. The Provider shall agree a third-party beneficiary clause with the subprocessor whereby – in the event the Provider has factually disappeared, ceased to exist in law or has become insolvent the Customer shall have the right to terminate the subprocessor contract and to instruct the sub-processor to erase or return the personal data.
  4. Those subprocessor(s) approved as at the commencement of this Agreement are as set out in ANNEX A. The Provider list all approved subprocessor(s) in Annex A and include any subprocessor’s name and location.

1. Complaints, data subject requests and third-party rights
   1. The Provider shall take such technical and organisational measures as may be appropriate and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:
      1. the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
      2. information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.
   2. The Provider shall notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.
   3. The Provider shall notify the Customer within 5 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.
   4. The Provider shall give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
2. Term and termination
   1. This Agreement shall remain in full force and effect so long as:
      1. the Service Agreement remains in effect; or
      2. the Provider retains any of the Personal Data related to the Service Agreement in its possession or control (Term).
   2. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Service Agreement in order to protect the Personal Data shall remain in full force and effect.
   3. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Service Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation 30 days either party may terminate the Service Agreement with immediate effect on written notice to the other party.
3. Data return and destruction
   1. On termination of the Service Agreement for any reason or expiry of its term the Provider shall securely delete or destroy or if directed in writing by the Customer, return and not retain all or any of the Personal Data related to this Agreement in its possession or control.
   2. If any law, regulation or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it shall notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention and establishing a specific timeline for deletion or destruction once the retention requirement ends.
4. Records
   1. The Provider shall keep written records regarding any processing of the Personal Data including but not limited to the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (Records).
5. Audit
   1. The Provider shall permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least 30 days' notice during the Term. The Provider shall give the Customer and its third-party representatives all reasonable assistance to conduct such audits. The assistance may include but is not limited to:
      1. physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;
      2. access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and
      3. inspection of Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.

This Agreement has been entered into on the date stated at the beginning of it.

|  |  |  |
| --- | --- | --- |
| Signed by [NAME OF DIRECTOR] |  |  |
| for and on behalf of [NAME OF **Customer**] |  | Director |
| Signed by [NAME OF DIRECTOR] |  |  |
| for and on behalf of [NAME OF **Provider**] |  | Director |

**Annex A: Personal Data processing purposes and details where BrandSwap acts as the processor**

|  |  |
| --- | --- |
| **Subject matter of processing** | To carry out the services as per the Service Agreement |
| **Duration of Processing** | Until termination of the Service Agreement |
| **Nature of Processing** | To enable Customers to propose additional offers and rewards to the End User. |
| **Personal Data Categories** | End User personal data can include:  **Identity data:** Includes first name, last name, username or similar identifier and title  **Contact data:** Email addresses  **Technical Data**: Includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use.  **Profile Data:** Searches made by End User  **Usage Data:** Includes information about how you use our website and services. |
| **Data Subject Types** | Customer’s customer personal data known as “End User”. |

**Subprocessor list**

Where the processor uses subprocessors, the following subprocessors are used:

|  |  |
| --- | --- |
| **Name of subprocessor** | **Location** |
| Microsoft Azure | Dublin (Ireland), Amsterdam (Holland) |
| MongoDB Atlas | Dublin (Ireland), Amsterdam (Holland) |
| Hubspot | Germany |
|  |  |

Annex B: Security measures

Description of the Provider’s technical and organisational data security measures.

## System and data access controls

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data. The platform also enforces 2FA as part of the initial authentication mechanics.

Authorisation: Customer Data is stored in multi-tenant storage systems accessible to Customers only via application user interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

## Transmission controls

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and on all parts of the platform. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security.  We have implemented technologies to ensure that stored data is encrypted at rest.

## Input controls

Detection: We designed our platform and infrastructure to log extensive information about the system behaviour, traffic received, authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel. Appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimise product and customer damage or unauthorised disclosure.

## Data backups

Data is backed up with incremental snapshots of the data **every six hours**. This data can be restored from a selected point in time within the last 72 hours. We also take daily snapshots and retains these daily snapshots for 35 days.

## Data segregation

Data is logically segregated and accessed by using user specific access tokens that is made available after successful login to the platform. Each access token has authorisation rules built in making sure access can be given and restricted on an individual user basis.