**BRANDQUAD**
**PROTECTION OF PERSONAL DATA - CUSTOMER**

Brandquad is a cloud platform for manufacturers that helps to automate the work with commercial content. Brandquad attaches the greatest importance to the protection of Personal Data and is in a constant process of compliance with the GDPR and other regulations related to Personal Data.

With regard to the processing carried out within the framework of the agreements signed with its customers (the "**Agreement**"), Brandquad France:

- as controller for Personal Data processed as part of the formation, management and billing of the Agreement signed with Customer (See Privacy Policy);
- as a subcontractor for Personal Data process on behalf of the Customer for the execution of the Agreement (See DPA)

# PRIVACY POLICY - CUSTOMER

## 1. DEFINITIONS

When used in this document, capitalized words and phrases have the following meanings:

**Agreement:** the legally binding terms and conditions agreed between Brandquad and the Customer in relation to the purchase by the Customer of Brandquad's Products and/or Services.

**Personal Data:** any information relating to a person identified or identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

**Regulation:** Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable from May 25, 2018, as well as the law of January 6, 1978 relating to data processing, files and freedoms.

## 2. SCOPE

**This Privacy Policy describes how Brandquad France processes Personal Data as Controller in connection with the Agreement concluded with Customers and in accordance with the Regulation.**

Brandquad France is a company incorporated under French law, registration number 881710354, whose registered address is 19 rue d'Amiens, 59000 Lille (France).

## 3. PURPOSE OF THE PROCESSING

As part of the formation, management and billing of the Agreement concluded with Customer and commercial relationship, Brandquad France is required to collect and process the personal data of the managers and employees of the Customer. This process is based on Article 6.1. f) of the GDPR.

The Customer undertakes to communicate the aforementioned information to the persons concerned.

## 4. PERSONAL DATA

The data collected are identification data, contact data and other information shared with Brandquad France in the context of the Customer support.

This data is kept for the duration of the Agreement and as long as it is needed in order to comply with the law, legal prescription and prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation and take other actions permitted by law.

## 5. RECIPIENTS OF THE PERSONAL DATA

This data may be communicated to representatives and members of Brandquad France and to their possible partners for the purpose of carrying out some of the processing operations listed out above:

- for hosting and back-up purposes;
- for bug management purposes;
- to manage customer support and keep track of requests;
- to manage commercial relationship with the client.

## 6. TRANSFER OUTSIDE THE EU

Brandquad France may transfer some of Personal Data to its affiliates or third party service providers located or using servers located outside the European Union (the "EU"). In such a case, Brandquad France:

- has taken appropriate safeguards to require Personal Data to remain secure in all places to which it is transferred;
- or makes sure they are located in a country considered having an adequate level of protection by the European Union in terms of personal data or.

## 7. RIGHTS OF DATA SUBJECTS

Data subjects have a right of access, rectification, erasure, limitation of processing, and a right of opposition with regard to information concerning them, by sending an email here Dataprivacy@brandquad.com.

Data subjects also have the right to lodge a complaint with the CNIL, if they consider that the processing of the data does not comply with the regulations in force, at the following address: CNIL - Complaints Department, 3 place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07.

## DATA PROTECTION AGREEMENT - CUSTOMER

### 1. DEFINITIONS

When used in this document, capitalized words and phrases have the following meanings:

**Agreement:** the legally binding terms and conditions agreed between Brandquad and the Customer in relation to the purchase by the Customer of Brandquad's Products and/or Services.

**Controller:** the Customer on behalf of whom the Personal Data is processed by the Processor. Under this DPA, the Controller may be the Customer and/or the subsidiary(ies) or other entities authorized by Customer to access or use Brandquad's Product or Service.

**Personal Data:** any information relating to a User identified or identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

**Data Breach:** a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of the Personal Data transmitted, stored or otherwise processed, or unauthorised access to such Personal Data.

**Processor:** Brandquad France.

**Regulation:** Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable from May 25, 2018, as well as the law of January 6, 1978 relating to data processing, files and freedoms.

**Sub-processor:** a person or entity to whom the Processor entrusts all or part of the performance of the process, under the Processor's responsibility.

**User:** all users permitted by the Customer to access to or use of the Products and where applicable Services as specified in the Agreement.

### 2. SCOPE

Brandquad Product and Service are made available to Users (employees or collaborators) at the request of the Customer under the Agreement. In this context, the processing of Personal Data is carried out by Brandquad as "Processor" of Personal Data, on behalf of the Customer as "Controller".

In accordance with the regulations, the Controller and the Processor have agreed to specify their obligations in relation to Personal Data within this Data Processing Agreement ("**DPA**"). **This DPA is part of the Agreement.**

Controller acts as the sole point of contact for the Controller and must obtain all relevant authorization, consent and permission for the processing of Personal Data, in accordance with the Agreement. Any instruction from the Controller to the Processor will be deemed to be given in its name and in the name of the other controllers if necessary. Conversely, any information given by the Processor to the Controller will be considered given to the other controller if necessary.

### 3. COMPLIANCE WITH THE REGULATION

The Processor undertakes to comply with the Regulation.

The Controller undertakes to comply with all laws applicable to the personal data it transmits to the Processor, including the Regulation.

In the event that the Controller is legally required to carry out a data protection impact assessment under the Regulation, and/or receives a request from a regulatory authority, the Processor will reasonably cooperate with the Controller and provide the Controller with the documents available in connection with the Product and/or Service (for example: audit reports, certifications). Any additional assistance shall be mutually agreed between the Parties.

### 4. DATA PROCESSING

The Controller is solely responsible for the accuracy, quality and legality of the Personal Data transmitted to the Processor as well as the means by which the Controller obtained this data.

The details of the processing are set out in Appendix 1, which forms an integral part of this DPA.

### 5. INSTRUCTIONS

In accordance with this DPA, the Processor processes Personal Data on behalf of the Controller and only according to its documented instructions (unless required by law). The Controller entrusts the Processor with the processing of Personal Data in accordance with the Regulation:

(i) For the performance of the Product and/or Service;
(ii) Through the use by the Controller of the functionalities of the Product/Service;
(iii) As documented in the Agreement; and
(iv) As documented in any other written instruction given by the Controller and acknowledged by the Processor as constituting an instruction for the purposes of this DPA.

The Processor shall immediately inform the Controller if, in its opinion, an instruction constitutes a breach of the Regulation or of other provisions of Union law or the law of the Member States relating to data protection.

### 6. SUBCONTRACTORS

In accordance with the provisions of this section, the Controller generally authorizes the Processor to engage Sub-Processors to carry out specific processing activities under the conditions below:

(i) the Processor is authorized to use the Sub-Processors with which it already works on the date of this DPA;
(ii) the Processor is authorized to appoint its own parent/affiliate companies as Sub-processors;
(iii) the Processor may also recruit third parties as Sub-processors in the performance of the Product and/or Service.

The Processor undertakes to put in place with each Sub-processor agreements containing obligations at least equal to those provided for in this DPA concerning Personal Data, to the extent applicable to the nature of the service provided by the Sub-processor.

The Processor will inform the Controller of any new Sub-Processors engaged for the processing of Personal Data during the term of the Agreement. The Controller shall have the right to oppose the appointment of a new Sub-processor by notifying the Processor in writing within ten (10) days of notification by the Processor of the appointment of a new Sub-processor, if the Controller has legitimate reasons to reject this Sub-Processor for reasons of non-compliance with the Regulation. The Processor will use reasonable efforts to recommend to Controller commercially reasonable modifications to its configuration of the Product and/or Service or its use of the Product and/or Service in order to avoid the processing of Personal Data by the new Sub-processor.

At the Controller's request, the Processor will make available the updated list of Sub-Processors of the Product and/or Service.

**7. STAFF**

The Processor undertakes that the processing of Personal Data will be strictly limited to employees having an interest in accessing said Personal Data in the context of the performance of the Product and/or Service and that the latter will be subject to confidentiality agreements for Personal Data that they deal with.

**8. SECURITY**

The Processor undertakes to implement the technical and organizational measures described in Appendix 2 to protect the security, confidentiality and integrity of Personal Data, including protection against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access of Personal Data.

The Controller acknowledges having read the technical and organizational measures implemented by the Processor and agrees that they are appropriate for the processing of Personal Data.

The Processor is authorized to modify and change the technical and organizational measures it implements without notification, provided that the same level of security is maintained.

**9. DATA BREACH**

The Processor will inform the Controller as soon as possible after becoming aware of a Data Breach and will provide the Controller with the information available at the time of the notification.

The Processor will take all reasonable and necessary corrective actions to mitigate the negative effects as well as to prevent the recurrence of such Data Breach insofar as these actions fall within the reasonable control of the Processor. These obligations do not apply to Data Breach caused by the Controller or by the Users.

**10. AUDITING**

At the request of the Controller and subject to the confidentiality obligation stipulated in the Agreement, the Processor will make available to the Controller, all information necessary to demonstrate compliance with the obligations set out in this DPA.

In the event of non-compliance by the Processor with the previous paragraph, and under the conditions provided for by the audit clause mentioned in the Agreement, the Customer may request an on-site audit of the security measures relating to the protection of Personal Data.

**11. DELETION AND RESTITUTION OF PERSONAL DATA**

In accordance with the Agreement, provided that the Controller is up to date with his payments and at the latter's request, the Processor will return the Personal Data in an intelligible form within thirty (30) calendar days following the end of the Agreement.

Two (2) months after the end of the Agreement, the Processor will destroy all Personal Data within thirty (30) days subject to any legal requirement relating to the retention of such data which may be applicable to it and the archives computers operated in the normal course of its activities.

**12. REQUESTS FROM DATA SUBJECTS**

If a User asks the Processor directly to exercise their rights over their Personal Data, the Processor will notify the Controller of this request as soon as possible. Responses to Users requests are the sole responsibility of the Controller.

The Processor may reasonably assist the Controller in responding to data subject requests, on behalf of the Controller, only on the instructions of the Controller in accordance with this DPA, and to the extent permitted by applicable law.

**13. INTERNATIONAL TRANSFER**

The Processor is entitled to process Personal Data outside the European Union in accordance with the Regulation.

In such a case, the Processor:

- has taken appropriate safeguards to require Personal Data to remain secure in all places to which it is transferred;
- or makes sure they are located in a country considered having an adequate level of protection by the European Union in terms of personal data or.

Where required by the Regulation, the Parties acknowledge and agree to use the system of standard contractual clauses published by the European Commission.

## APPENDIX 1 – DETAILS OF THE PROCESSING

### 1. NATURE AND PURPOSE OF THE PROCESSING

The Processor will process Personal Data as necessary for the performance of the Product and/or Service, in accordance with the DPA and the instructions of the Controller in the context of its use of the product and/or Service.

### 2. DURATION OF THE PROCESSING

The duration of the processing is equal to that of the Agreement. However, the Controller acknowledges that he is able and that he is responsible for configuring and informing the Processor of the maximum duration during which the Personal Data will be stored in the Product and/or Service.

The Processor reserves the right to store and archive all technical information as well as any electronic exchange of any kind for the purpose of satisfying any applicable legal requirement or for evidentiary purposes in accordance with applicable law.

### 3. PROCESSING DETAILS

3.1 Purpose of processing. The Processor processes Personal Data in the context of the provision of the Product and/or Service under the Agreement (implementation, operation, monitoring, technical support, storage, hosting).

3.2 Categories of Data Subjects. People affected by the processing of Personal Data under this DPA are representatives and/or employees of the Controller authorized to access and use the Product and/or Service.

3.3 Categories of Personal Data. Personal Data may include, but is not limited to, the following categories: identification data, contact data, geographical zone, position, main responsibilities, role on the project, access to the Product and/or Service.

3.4 The Controller undertakes not to transmit sensitive data through the Service, whatsoever and at any time.

**APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES**

- ***security policy***
  *The information system of Brandquad has been designed to systematically and safely protect customer data as an International Organization for Standardization (ISO) Information Security Management System (ISMS) based on ISO 27001:2013 and other ancillary ISO standards.*
  *Brandquad considers information security to be a high priority and has established company-wide policies to ensure all personnel understand their responsibilities in the protection of information in order to maintain data confidentiality, integrity, accessibility, availability, and privacy.*
  *Brandquad provides its employees with communication systems, hardware, and software necessary to conduct business.*
  *All Brandquad employees must comply with Brandquad security policies and procedures when utilizing company information technology assets. Brandquad employees are trained on Brandquad security policies and are expected to apply and extend those concepts to fit the needs of day-to-day operations.*
  *This policy applies to all employees and contractors (to include consultants and temporary staff).*
- ***risk management***
  *Information security risks are defined as technical threats from external and internal sources, regulatory risks from failure to comply with laws and information security regulations for each country, region, or industry related to the business unit, risks to the loss of intellectual property or proprietary information, and mishandling of customer or partner data under contract and/or non-disclosure.*
  *All information systems security risks are tracked by Infosec, Brandquad's Information Security which performs periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.*
- ***Data center physical security***
  *Brandquad IT Operations rely on data centers that feature state of the art facilities. To ensure the highest level of security for customer data and platform infrastructure, these facilities include, at minimum, a physical access control policy who can access data storage centers, server rooms, physical records, and any other physical locations or resources.*
- ***Remote Access Policy***
  *Remote access policy requires that to interact with Brandquad's resources, while not at physical locations operated by Brandquad, users must follow rules to ensure they are accessing the network from a secure device, using a secure connection or a company VPN.*
- ***data access control***
  *Access to data is provided under Need-to-Know Principle. Users only have access to whatever resources they really need to perform their job.*
  *Access is secured by password, in compliance to a policy based on rules around what passwords are acceptable, and how users must handle their passwords (length, special characters, change of passwords periodically, guidelines never to share passwords...)*
- ***protection of workstations***

*Workstations are defined as a device - be it personal or company-owned - that contains company data. This includes desktops and laptops, as well as mobile devices Policies are designed to ensure that (i) workstations have operating systems supported by vendors and are up to date with critical security patches, (ii) data is encrypted as defined in the encryption policy, (iii) are protected by passwords according to company guidelines, and (iv) locked when unattended.*

- ***Security Incident***

  *If Brandquad becomes aware of any unlawful access to their Brandquad SaaS, or unauthorized access to these services, or unlawful access to any Customer Data stored on SaaS provider's equipment or facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a 'security incident'), Brandquad will (i) notify Customer of the security incident, (ii) investigate the security incident, and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.*