

DATA PROCESSING ADDENDUM ("DPA")/DATA PROCESSING AGREEMENT  
("DPA")

LAST UPDATED ON: 16/06/2022

Data Processing Addendum/Data Processing Agreement ("DPA")

This Data Processing Addendum or Data Processing Agreement ("DPA"), forms part of the Agreement between GoodBarber SAS ("GoodBarber") and the Customer ("Customer") and shall be effective on the date both parties execute this DPA ("Effective Date"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

## 1. Definitions

"Adequacy Decision": means, according to the European Data Protection Supervisor ([https://edps.europa.eu/data-protection/data-protection/glossary/a\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/a_en)): 'An "adequacy decision" is a decision adopted by the European Commission on the basis of Article 45 of the GDPR, which establishes that a third country (i.e. a country not bound by the GDPR) or international organization ensures an adequate level of protection of personal data. Such a decision takes into account the country's domestic law, its supervisory authorities, and international commitments it has entered into".

"Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"Agreement" means GoodBarber's Terms of Use, which govern the provision of the Services to Customer, as such terms may be updated by GoodBarber from time to time.

"Binding Corporate Rules" (BCR): mean according to the European Data Protection Supervisor ([https://edps.europa.eu/data-protection/data-protection/glossary/b\\_en#bindingrules](https://edps.europa.eu/data-protection/data-protection/glossary/b_en#bindingrules)): Binding corporate rules (BCRs) are a legal tool that can be used by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country.

"Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

"Customer Data" means any Personal Data or personal information that GoodBarber processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"Data Protection Laws" means all data protection and privacy laws or regulation applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"Data Controller" means an entity that determines the purposes and means of the processing of Personal Data.

"Data Processor" means an entity that processes Personal Data on behalf of a Data Controller.

"EU Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"EEA" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"Group" means any and all Affiliates that are part of an entity's corporate group.

"Hash": means a mathematical function that converts a file or any kind of data into a unique, unforgeable line of numbers and letters. The hash cannot be "reverse-engineered" to access the data.

"Personal Data or Personal Information" means any information relating to an identified or identifiable natural person.

"Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"Services" means services, products, applications, tools, offline components and features (individually the "Service" or collectively, the "Services") provided by our company GoodBarber, together with its affiliates, officers, directors, employees, agents and subsidiaries (hereinafter "GoodBarber", "we", "our" or "us").

“Standard Contractual Clauses” (SCC): means according to the European Data Protection Supervisor ([https://edps.europa.eu/data-protection/data-protection/glossary/s\\_en#standard\\_contractual\\_clauses](https://edps.europa.eu/data-protection/data-protection/glossary/s_en#standard_contractual_clauses)): Standard contractual clauses are legal tools to provide adequate safeguards for data transfers from the EU or the European Economic Area to third countries. In principle no authorisation is required from data protection authorities to be allowed to use these clauses. A formal notification to the authority might nevertheless be necessary.

"Sub-processor" means any Data Processor engaged by GoodBarber or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

## 2. Relationship with the Agreement

2.1 The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, the Agreement shall prevail to the extent of that conflict.

2.3 Any claims brought under or in connection with this DPA shall be subject to the Terms and Conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.4 Any claims against GoodBarber or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by GoodBarber in relation to the Customer Data or information that arises as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce GoodBarber's liability under the Agreement as if it were liability to the Customer under the Agreement.

2.5 No one other than a party to this DPA, its successors and permitted assigns shall have any right to enforce any of its terms.

2.6 This DPA shall be governed by and construed in accordance with governing law, regulations and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

## 3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that GoodBarber processes Customer Data or information that originates from the EEA and/or that is otherwise subject to EU Data Protection Law or regulation on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

3.2 Part A (being Section 4 – 8 (inclusive) of this DPA, as well as Annex A of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.

3.3 Part B (being Sections 9-12 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

#### Part A: General Data Protection Obligations

#### 4. Roles and Scope of Processing

4.1 Role of the Parties. As between GoodBarber and Customer, Customer is the Data Controller of Customer Data, and GoodBarber shall process Customer Data only as a Data Processor acting on behalf of Customer.

4.2. Customer Processing of Customer Data. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to GoodBarber; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws or regulation for GoodBarber to process Customer Data and information and provide the Services pursuant to the Agreement and this DPA.

4.3 GoodBarber Processing of Customer Data. GoodBarber shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to GoodBarber in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and GoodBarber.

#### 4.4 Details of Data Processing

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between GoodBarber and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of GoodBarber's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: GoodBarber provides an online service composed of tools enabling the Customer to create its own Application(s) as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("Users"); and any individual: (i) whose information is stored on or collected via the Services, or (ii) to whom Users engage or communicate with via the Services (collectively, "End Users").

(f) Types of Customer Data:

(i) Customer and Users: identification and contact data (name, address, title, contact details); financial information (credit card details, account details, payment information, billing information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data, various logs);

(ii) End Users: identification and contact data (name, date of birth, gender, general occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data, various logs).

4.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that GoodBarber shall have a right to use and disclose data and/or information relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, GoodBarber is the Data Controller of such data and accordingly shall process such data in accordance with the GoodBarber Privacy Policy and Data Protection Laws or regulation.

4.6 Tracking Technologies and similar technologies. Customer acknowledges that in connection with the performance of the Services, GoodBarber employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws or regulation to enable GoodBarber to deploy Tracking Technologies lawfully on, and collect data from, the devices of End Users (defined below) in accordance with and as described in the GoodBarber Cookie policy Statement.

## 5. Sub processing

5.1 Authorized Sub-processors. Customer agrees that GoodBarber may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by GoodBarber and authorized by Customer are listed in Annex A.

5.2 Sub-processor Obligations. GoodBarber shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws or regulation; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause GoodBarber to breach any of its obligations under this DPA.

## 6. Security

6.1 Security Measures. GoodBarber shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data and information, in accordance with GoodBarber's security standards described in Annex B ("Security Measures").

6.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by GoodBarber relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that GoodBarber may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data and personal information when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

## 7. Data Center Locations

GoodBarber processes Customer Data in France where GoodBarber maintains data processing operations. GoodBarber may transfer and process Customer Data anywhere in the world (GoodBarber will do so by implementing BCR and/or SCC and/or using Adequacy Decisions as required by EU law and regulation and guiding rules) where its Affiliates or its Sub-processors maintain data processing operations. GoodBarber shall at all times provide an adequate level of protection for the Customer Data or information processed, in accordance with the requirements of Data Protection Laws or regulations.

## Part B: GDPR Obligations from May 25th 2018

### 8. Additional Security

8.1 Confidentiality of processing. GoodBarber shall ensure that any person who is authorized by GoodBarber to process Customer Data (including its employees, staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). GoodBarber will ensure that its staff, employees and subcontractors' staff is continuously up to date with law and regulations and that state of the art security and confidentiality measures are maintained at all times and to state of the art levels.

8.2 Security Incident Response and notification. Upon becoming aware of a Security Incident or data breach, GoodBarber will notify Customer without undue delay, but not longer than seventy-two (72) hours and shall provide timely information relating to the Security Incident as soon as it becomes known. If a greater delay is needed this must be justified. GoodBarber must notify the CNIL if a security incident arises regarding Data Protection, Personal Information or Data Protection or Data Security breach, this notification to the CNIL will intervene in a maximum of seventy-two (72) hours, after GoodBarber knew or has been notified about this data violation or breach.

### 9. Changes to Sub-processors

9.1 GoodBarber shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email shall suffice).

### 10. Return or Deletion of Data

10.1 Upon termination or expiration of the Agreement, GoodBarber shall (at Customer's election) delete or return to Customer all Customer Data in its possession or control, save that this requirement shall not apply to the extent GoodBarber is required by applicable law or regulation to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data GoodBarber shall securely isolate and protect from any further processing, except to the extent required by applicable law or regulation. The data Return from GoodBarber to the Customer will be done in an interoperable file format or if, initially, the data received by GoodBarber was not in an interoperable format, the data will be returned in the same format in which GoodBarber received it.

### 11. Cooperation


11.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the

relevant Customer Data within the Services, GoodBarber shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to GoodBarber, GoodBarber shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If GoodBarber is required to respond to such a request, GoodBarber shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

11.2 If a law enforcement agency sends GoodBarber a demand for Customer Data or information (for example, through a subpoena or court order), GoodBarber shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, GoodBarber may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data or information to a law enforcement agency, then GoodBarber shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless GoodBarber is legally prohibited from doing so.

11.3 To the extent GoodBarber is required under EU Data Protection Law, GoodBarber shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law or regulation.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

<p>The Customer</p> <hr/> <p>Name: Title: GoodBarber project URL :</p> <hr/> <p>Date:</p>	<p>GoodBarber SAS d/b/a GoodBarber</p> <p>Name: Dominique Siacci Title: CTO/Co-founder Date: June 16, 2022</p> 
---	---

#### Annex A - List of GoodBarber Sub-processors

GoodBarber uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.



<b><u>Entity Name</u></b>	<b><u>Corporate Location</u></b>
Amazon Inc. (AWS)	Washington, USA, London, United Kingdom, Ireland, Stockholm, Frankfurt, Paris, Milan, EUROPE
Apple Inc.	California, USA
Atlassian	New-South Wales, AUSTRALIA Australia
Google LLC.	California, USA
Google Ireland Limited	Ireland, EUROPE
Slack Technologies	California, USA
StackPath	Texas, USA
OVH	France, EUROPE
Twilio	California, USA
SITEC	France, EUROPE
Paypal Inc.	California and Washington, USA
Mercado Pago	Buenos Aires, ARGENTINA
Stripe Inc.	California, USA
So You Start	Roubaix, Gravelines, Strasbourg, EUROPE
101 Domain	Vista, USA
Digital Ocean	New-York, USA
Gandi	Paris, Europe
GoDaddy	Tempe, USA
Kimsufi	Roubaix, Gravelines, Strasbourg, EUROPE
MaxCDN (Stackpath)	Dallas, USA
Pingdom (Solarwinds)	Austin, USA
Work4Cad (W4C)	Saône, Europe

Gaspard+Bruno	London, United Kingdom
Zoho CRM	Chennai, India

## Annex B - Security Measures

### Data Center Security

GoodBarber delivers millions of pageviews a month for thousands of Users. We use multiple resources, placed in different world-class data centers in France (EUROPE). Our data centers manage physical security 24/7 with mandatory personal identification, and high tech security access control and access monitoring in accordance with state of the art measures.

We have DDoS mitigation in place at all of our data centers, and aggressive use of firewalls and network isolation in our infrastructure.

Access to our server systems is allowed only through secure connections by our trusted and restrained team of administrators from the GoodBarber team.

### Protection from Data Loss, Data Corruption

We implement multiple layers of application logic that prevent corruption of data from one user account to another.

Account data is mirrored and regularly backed up off site. We secure the data in three (3) different data centers all located in France (EUROPE) hence under GDPR protection.

### Application Level Security

GoodBarber account passwords are hashed (cryptographic measures). Our own staff and employees can't view them or access them. If you lose your password, it can't be retrieved—it must be reset.

All login pages and all pages used to manage the Services (backend pages) pass data via TLSv1.2.

Login pages and logins via the GoodBarber API have brute force protection.

We perform regular external security penetration tests throughout the year using different vendors. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.

### Internal IT Security

GoodBarber offices are secured by badge access, and they are monitored 24h/24h and 7d/7d with cameras throughout.

Our office network is heavily segmented and centrally monitored.

We have a dedicated internal security team that constantly monitors our environment for vulnerabilities and breaches. They perform penetration testing and social engineering exercises on our environment.

#### Internal Protocol and Education

We continuously train employees and staff on best security practices, including how to identify social engineering, phishing scams, and hackers.

#### Protection Against Misuse

We can take all the measures to secure ourselves, but if your computer or any mobile device gets compromised and someone gets into your GoodBarber account, that's not good for either of us and GoodBarber will not be liable for such misuse or fraudulent access.

We monitor and will automatically suspend accounts for signs of irregular or suspicious login activity.

We monitor accounts and Application activity for signs of abuse.

In addition to our scalable algorithms, we employ another layer of human reviewers, who monitor for anomalous account and Application activity.