Base44 – Data Processing Addendum – Users

This data processing addendum (the "**DPA**"), is part of the Terms of Service governing the services provided to you by Base44, Inc. (the "**Company**"), and any other agreement or documents executed between the parties (collectively, the "**Agreement**").

If as part of the services provided to you, including building your application, hosting your application, provide you with artificial intelligence capabilities and application programming interface to third parties, or any other action required to provide you with our platform and improve it (collectively, the "**Services**"), To the extent the Company processes, on your behalf, any information of your users, clients, prospects, or any other individual who interacts with your application ("**Data Subject**"), this DPA shall govern the processing of all information receives, collects, accesses, or uses in connection to the Agreement on your behalf ("**Personal Data**").

1. **Roles and Instructions**
   - 1.1. You acknowledge and agree that with regard to the processing of any Personal Data, you either act as:
     - 1.1.1. a controller of the data, determining the purpose and means of the processing of Personal Data ("**Controller**").
     - 1.1.2. or a processor, which processes Personal Data for third parties ("**Processor**").
   - 1.2. Company shall be considered your processor, and in no event shall be considered as the controller of the data.
   - 1.3. You hereby instruct Company to process Personal Data in accordance with the terms of this DPA, which shall be considered the complete, exclusive and final instructions regarding the processing of Personal Data by the Company, and no additional instructions that deviates from the listed herein, or which impose any additional liability or expenses shall be introduced.
   - 1.4. You hereby undertake and warrant that all Personal Data provided under this DPA to the Company, was collected lawfully, without infringement of any right or freedom of any Data Subject and in compliance with all Applicable Data Protection Laws (as defined below).
2. **Processing by Company**
   - 2.1. Each party will comply with all laws, rules and regulations applicable to it regarding processing Personal Data, including the European Union Regulation 2016/679, and the national law of the applicable EEA member state that implements the GDPR, United States Data Protection Laws, the UK General Data Protection Regulation, United States' federal and state laws, Canada's Federal Personal Information Protection and Electronic Documents Act, Brazil's Lei Geral de Proteção de Dados and Israel Protection of Privacy Law ("**Applicable Data Protection Laws**").
   - 2.2. Company shall process Personal Data in order to provide the Services, in accordance with the Agreement. The nature and purposes of the processing, its duration, categories of Personal Data, shall be determined solely by you, depending on your use of the Services.
   - 2.3. Company shall implement appropriate technical and organizational measures, designated to:
     - 2.3.1. Prevent unauthorized access, disclosure, or corruption of your Personal Data, as outlined under Exhibit B.
     - 2.3.2. Assist you with complying with requests you may receive by Data Subjects.
     - 2.3.3. 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 regarding their responsibilities, and have committed themselves to confidentiality.
     - 2.3.4. Company may allow you to integrate with other third-parties using the platform, and share Personal Data with them. It shall be clarified that the engagement between these third-parties and you is at your sole discretion, and we strongly advise you to review and execute terms for such integrations.

2.3.5. Company shall only use Personal Data for the provision of the Services, or following full anonymization process, removing all personal attributes, or in an aggregated manner.

3. Sub-processors

3.1. Company may process Personal Data using third-parties ("**Sub-processors**"), in order to provide you with the Services under the restrictions set forth herein. Sub-processors shall not process Personal Data, except for processing on an aggregated or anonymized basis, for any purpose other than providing the Services.

3.2. Sub-processors will be subject to terms materially similar to the terms set forth herein.

3.3. Company shall remain liable to you under any breach of this DPA that is caused by its Sub-processors, and ensure and maintain appropriate due diligence on its Sub-processors.

3.4. All the current Sub-processors engaged by Company are listed in Exhibit C.

3.5. Company allows you to subscribe to the Sub-processors list, and receive notification of any intended addition or replacement of Sub-processors, which shall be delivered seven days prior to such change. In order to subscribe to such notification, send an email to compliance@base44.com.

3.6. You may reasonably object to the appointment or replacement of a Sub-processor by Company on documented reasonable grounds relating to data protection, by submitting a written and reasoned objection to Compliance@base44.com, within seven (7) days from receipt of a change notification.

3.7. In such an event, Company may, in its sole discretion, choose to use commercially reasonable efforts (but is not required to) make available to you an alternative solution to avoid the processing of Personal Data, by the new Sub-processor you objected to. Until Company makes a decision concerning your objection, it may be required to temporarily suspend the processing of Personal Data which may result in some features of the Services to deactivate.

3.8. If Company finds that it is unable to resolve your objection or to provide you with such alternative solution, within thirty (30) days from receipt of your valid reasoned objection, as determined in Company's full and sole discretion (with no obligation to provide any reasoning), you may, as a sole remedy, discontinue the use of the affected Services by providing written notice to compliance@base44.com. Such discontinuation will be without prejudice to any fees incurred by you prior to the discontinuation of the affected Services and you will have no further claims against Company in connection with the discontinuation of the affected Services. If no objection has been raised to the replacement or appointment of a new Sub-processor within the above mentioned time frame, Company will deem you to have authorized the new Sub-processor.

4. Security

4.1. Company has implemented and will maintain industry-standard technical and organizational security measures designed to prevent unauthorized access, disclosure, or corruption of your Personal Data, as listed under Exhibit B.

4.2. You are responsible for reviewing the information Company makes available regarding its data security, and making an independent determination as to whether the Services meet your needs, requirements and legal obligations.

4.3. To the extent applicable, you are further responsible for properly configuring the Services and using features and functionalities made available to maintain appropriate security of Personal Data.

4.4. By using Company's Services, you hereby agree to the adequacy of the organizational, technical and security measures implemented by Company.

5. Audit

5.1. Upon your reasonable written request, at reasonable intervals (no more than once every 12 months) and subject to confidentiality (if applicable) undertakings by you, Company will make available to you reports, certifications, or extracts thereof were readily available from a source charged with auditing Company's data protection practices to enable you to assess Company's compliance with this DPA regarding your Personal Data.

5.2. To the extent such documentation cannot fulfill Company's legal obligations towards you under the Applicable Data Protection Laws, Company shall allow you to conduct an independent audit, by sending reasonable questionnaires or interviewing Company's personnel, or other reasonable methods as required by the Applicable Data Protection Laws, all without imposing any additional expense on the Company.

6. Security Incident

6.1. Upon becoming aware of any confirmed security incident in which Personal Data was accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed, Company shall notify you without undue delay as required by the Applicable Data Protection Laws.

6.2. Company will use reasonable efforts to include in such notifications relevant information concerning: the nature of the related breach, the scope and type of affected records and affected Data Subjects, the anticipated consequences and details about any remediation and other measures deployed by Company.

6.3. You acknowledge that such notification shall not be deemed or construed as an acknowledgement by Company of any fault or liability with respect to such incident.

6.4. You also acknowledge that in the event of such an incident, you may also be obligated to take measures required under Applicable Data Protection Laws to mitigate damages to Data Subjects.

7. Assistance and Personal Data Requests

7.1. Unless prohibited from doing so by law, Company shall promptly notify you if it receives requests, demands, warrants, or similar inquiry from authorities to access Personal Data. Company shall not provide access to Personal Data unless it reasonably believes the requests are binding, and in these cases, it shall limit the access to Personal Data to the extent necessary to comply with such inquiries.

7.2. Company shall promptly notify you when it receives a request from a Data Subjects specifically regarding the processing of Personal Data on your behalf. Company shall not be responsible for responding to such requests, and shall provide you with the readily available information required to respond to such requests.

7.3. Company will make available to you mechanisms (either automatic or manual) in order to help you to comply with such binding requests.

7.4. To the extent required by the Applicable Data Protection Laws, Company shall maintain records of its processing activities on your behalf, and upon request provide you with necessary records to demonstrate compliance with such legal requirements.

8. Cross Border Transfer

8.1. Company shall only transfer Personal Data to its Sub-processors from the European Economic Area (EEA), Switzerland and the United Kingdom, using lawful mechanisms required to ensure that the relevant cross-border transfer is in compliance with the Applicable Data Protection Laws, such as: (i) transfer to countries that are recognized by the EEA as providing adequate level of protection to Personal Data;; (ii) EU-US Data Privacy Framework and its applicable extensions; (iii) EU Standard Contractual Clauses, Module 2 or 3 (as applicable), ("**SCC**") as approved by the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; (iv) any other approved mechanisms.

8.2. To the extent the applicable cross-border transfer mechanism deployed is the SCC, the parties agree to incorporate it to this DPA, with the following:

8.2.1. Clause 7: shall not apply;

8.2.2. Clause 9: option 1 shall apply;

8.2.3. Clause 17: the "EU member State" shall be Ireland;

8.2.4. Clause 18: the "EU member State" shall be Ireland.

8.3. For transfers outside of UK or Switzerland, the applicable mandatory changes shall apply mutatis mutandis.

9. Termination

9.1. Upon your written request, Company will delete your account, including all Personal Data stored thereof, except for the following:

9.1.1. Any data retained by Company to the extent required by law;

9.1.2. Any data retained by the Company during its automatic back-up procedures, which are deleted after set intervals.

9.2. To the extent Personal Data is retained pursuant to the termination of this DPA in accordance to the above exceptions, it shall be subject to the terms of this DPA, and will not be accessed or used for any other purpose, until deleted from the systems.

10. US State Laws Specific Terms

10.1. The following terms are relevant to Personal Data originating from the United States:

10.1.1. For the avoidance of doubt, the definitions of "Personal Data", "Data Subject", "Controller" and "Processor" includes the definitions "Personal Information", "Consumer", "Business", and "Service Provider", respectively, all as defined under the legal name of the California Consumer Privacy Act is California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). In addition, the terms "Sell" and "Share" shall have the meaning ascribed to them under the CCPA.

10.1.2. Company may not:

10.1.2.1. Sell or Share, Personal Data.

10.1.2.2. use Personal Data for any purpose other than the business purposes specified in this DPA, or outside of the data processing activities specified in this DPA.

10.1.2.3. Combine the Personal Data it receives from, or on behalf of you with any other information collected by Company not in respect of the Services.

10.1.2.4. Engage with any other party to assist or partake in processing of Personal Data without notifying you in accordance with this DPA.

10.1.3. You have the right to: (a) verify the processing of Personal Data is consistent with this DPA; (b) take reasonable steps, as defined in Section 5(Audit), to ensure that Company uses the Personal Data in a manner consistent with Company's obligations under this DPA or the CCPA; and (C) upon unauthorized use of Personal Data, terminate the DPA, upon providing written notice to Company, and delete your account and Personal Data.

10.1.4. Company hereby acknowledge that it understands and complies with the requirements under the Applicable Data Protection Laws when Personal Data originates in the United States, including all the binding restrictions regarding it.

11. General

11.1. Company shall provide you a notification if it cannot longer meet its obligations under this DPA or the Applicable Data Protection Laws.

11.2. The terms of this DPA may be amended from time-to-time by Company, by posting the relevant amended DPA on its website. Your continued use of the Services after the amended DPA is posted constitutes your agreement to, and acceptance of, the amended DPA.

11.3. If any provision of this DPA is deemed by a court of competent jurisdiction to be invalid, unlawful, void, or for any reason unenforceable, then such provision shall be deemed severable and will not affect the validity and enforceability of the remaining provisions.

11.4. For avoidance of doubt and to the extent allowed by applicable law, all liability under this DPA, including limitations thereof, will be governed by the relevant provisions of Company's Terms of Service.

11.5. This DPA was written in English and may be translated into other languages for your convenience. If a translated (non-English) version of this DPA conflicts in any way with its English version, the provisions of the English version shall prevail.

Exhibit A – Details of the Processing

1. **Nature and Purpose of Processing**. We may use the Personal Data for the following purposes (and tasks related to such purposes), all in accordance with the Agreement and in a way that is proportionate and that respects your and your Users-of-Users privacy rights:
   1.1. Providing you with the Services including through Sub-processors;
   1.2. Acting upon your instructions, including providing you with professional assistance, only upon your request; provided your instructions are consistent with the terms of this DPA and the Services;
   1.3. Preventing, investigating and mitigating data security risks and incidents, fraud, errors and/or illegal or prohibited activities;
   1.4. Complying with applicable laws and regulations;
2. **Duration of Processing**. You determine the duration of the processing based on your needs and your sole discretion. Company shall, in accordance with the terms of this DPA, delete Personal Data pursuant to Section 9.
3. **Type of Personal Data**. Subject to your content restriction obligations under this DPA and the Agreement, the scope and nature that is controlled and determined solely by you in compliance with Applicable Data Protection Laws.
4. **Categories of Data Subjects**. Subject to your content restriction obligations under this DPA and the Agreement, you may submit Personal Data to the Service, which may include (but is not limited to), Personal Data relating to the following categories of Data Subjects, all as controlled and determined solely by you: existing and prospective employees, candidates, agents, consultants, freelancers, business partners and/or sub-contractors (and their respective employees, contact persons, agents, etc.), who are natural persons; (ii) your existing and prospect customers and end users (and their respective employees, contact persons and agents), who are natural persons; and (iii) any other third party individual with whom you decide to engage through the Service.

Exhibit B
Technical and Organizational Measures

The company deploys and maintains technical and organizational security measures to protect Personal Data. Below is an overview of the measures the Company employs to keep our platform and Personal Data secure.

1. General
   - 1.1. The Company maintains a documented information security policy, consistent with industry standards, reviewed and updated annually. Security policy development and maintenance, is managed by personnel with expertise in the field of information security.
   - 1.2. All personnel computers shall be updated with antivirus software, or similar protective mechanisms.
2. Training and Personnel
   - 2.1. All Company's personnel undergo a security training program at least once every calendar year.
   - 2.2. Upon termination, no personnel may retain any access keys, codes, or similar access to any Personal Data or the Company's facilities.
3. Access Control
   - 3.1. The Company's information security policies shall establish reasonable steps to prevent unauthorized access to, or loss of, Personal Data.
   - 3.2. Company shall designate a system administrator, which restricts access of other personnel to Personal Data in accordance with these Technical and Organizational Measures, which access permissions which shall be reviewed on an annual basis.
   - 3.3. Company shall require authentication process for all access and remote access by its personnel, which can consist of strong passwords, two-factor authentication, or other mechanisms which prevents unauthorized access.
   - 3.4. Access, data insertion, deletion, and modification logged, including time stamps.
4. Physical Security
   - 4.1. Company ensures the physical security of its premises, and monitors any access, or entrance to its premises.
   - 4.2. Company requires all of its personnel to refrain from retaining physical copies of sensitive data for any longer than necessary, according to Company's policies.
   - 4.3. Visitors access to Company's facilities is monitored and restricted, managed by dedicated personnel.
   - 4.4. All Personal Data shall be hosted and stored in machine located in facilities with reasonable environmental measures, such as, temperature regulation, fire suppression, smoke detectors, etc.
5. Integrity
   - 5.1. Company regularly back-up its systems, and undertakes to review software to find and remediate security vulnerabilities during initial implementation and upon any significant modifications and updates.
   - 5.2. Company undergoes penetration testing at least once every calendar year, and remediates any finding in accordance with its internal policies.
   - 5.3. Company undertakes to change all default account access configurations and authentication keys prior to the implementation of all new systems following the effective date of this Agreement.
   - 5.4. All personnel laptops are managed by Company, and monitored regularly.
   - 5.5. Company shall not store Personal Data outside of its monitored environments unless it is protected by strong encryption.
6. Deletion
   - 6.1. Company undertakes to delete all Personal Data in accordance with the DPA.

6.2. Company maintains automatic back-up practices of Personal Data, which are deleted on set intervals.

7. Third-Party Risk Management

7.1. Prior to engaging a new third-party service provider who will have access to Personal Data, Company conducts a risk assessment of its information security practices.

8. Law Enforcement Request Policy

8.1. One of the most prominent Company's core values is respecting human rights. As such, the Company ensures that all data requests received from law enforcement agencies, governmental, regulatory, and judicial bodies are valid and made in accordance with the applicable legal procedures.

8.2. All disclosure of Personal Data to authorities shall be in accordance with this DPA

Exhibit C
Sub-processors

Provider	Description of the Services Provided by the Provider	Country
Mongo	Data storage and hosting	US
SendGrid	Email transmission and external communication	US
Langfuse	LLM logging	Germany
Logfire	General logging purposes	UK
Render	Server services	US
GCP - Google cloud	Analytics services	US
OpenAI	API calls to LLM	US
Anthropic	API calls to LLM	US
Wix.com Ltd.	Providing and improving the services	Israel