Data Protection Agreement

This Data Protection Agreement (« Agreement ») is entered into between Privacyboard and the undersigned Customer identified in the applicable Appendix I at Controller section and the signature block below (« Customer ») as of the last date beneath Customer's and Privacyboard's signature blocks below (« Addendum Effective Date »). This Agreement forms part of the agreement between Customer and Privacyboard covering Customer's use of the Services (as defined below).

Clause 1: Purpose and scope

(a) The purpose of this Agreement is to ensure compliance with Article 28(3) and (4) of 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.

(b) The controllers and processors listed in Appendix I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Appendix II.

(d) Appendixes I to III are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the Customer is subject by virtue of Regulation (EU) 2016/679.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679. They are herein completed by Standard Contractual Clauses for personal data transfers outside the European Union/European Economic Area (EU/EEA) if needed.

Clause 2: Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Appendixes or updating information in them.

(b) This does not prevent the Parties from including these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms have the same meaning as in that Regulation.

(b) These Clauses must be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses are not to be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses will prevail.

Clause 5: Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Appendixes and signing Appendix I.

(b) Once the Appendixes in (a) are completed and signed, the acceding entity will be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Appendix I.

(c) The acceding entity will have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Clause 6: Description of processing(s)
The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Customer, are specified in Appendix II.

Clause 7: Roles of the Parties
7.1. Instructions

(a) Privacyboard processes personal data only on documented instructions from the Customer, unless required to do so by Union or Member State law to which Privacyboard is subject. In this case, Privacyboard will inform the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Customer throughout the duration of the processing of personal data. These instructions are always to be documented.

(b) Privacyboard immediately informs the Customer if, in Privacyboard's opinion, instructions given by the Customer infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

Privacyboard processes the personal data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further instructions from the Customer.

7.3. Duration of the processing of personal data

Processing by Privacyboard only takes place for the duration specified in Appendix II.

7.4. Security of processing

(a) Privacyboard implements the technical and organizational measures specified in Appendix III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) No provision of this Agreement includes the right to, and Customer may not, directly or indirectly, enable any person or entity other than authorized users to access or use the Services, or use (or permit others to use) the Services other than as described in the applicable Agreement.

(c) Privacyboard grants access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring the contract. Privacyboard ensures that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

(a) If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), Privacyboard applies specific restrictions and/or additional safeguards.

(b) Without limiting its responsibilities under this Agreement, Customer is responsible for ensuring that no sensitive data is submitted

to Privacyboard when not necessary for the processing activities available in Appendix II.

7.6 Compliance with documented instructions

(a) The Parties are able to demonstrate compliance with these Clauses.

(b) Privacyboard deals promptly and adequately with inquiries from the Customer about the processing of data in accordance with these Clauses.

7.7 Audit

(a) Upon request, Privacyboard makes available to the Customer all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the Customer's request, Privacyboard also permits and contributes to audits of the processing activities covered by these Clauses.

(b) For any intended audit or inspection, the Customer undertakes to notify Privacyboard by providing a reasonable prior written notice at least fourteen (14) business days before the audit or the inspection.

(c) The Customer may choose to conduct the audit by itself or mandate an independent auditor. In deciding on a review or an audit, the Customer may take into account relevant certifications held by Privacyboard.

(d) The Parties makes the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.8. General authorization for the use of sub-processors

(a) Privacyboard has the Customer's general authorization for the engagement of sub-processors from an agreed list available below in Appendix II.

(b) Privacyboard will endeavor to give the Customer written notice of any intended changes of that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the Customer fifteen (15) days to object on reasonable grounds to such changes prior to the engagement of the concerned sub-processor(s) by sending an email to hello@privacyboard.co.

(c) The Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Privacyboard from offering the Services to the Customer. If the Customer does not object to the engagement of a sub-processor in accordance within fifteen (15) days of notice by Privacyboard, that sub-processor will be deemed an authorised sub-processor for the purposes of this Agreement.

(d) Where Privacyboard engages a sub-processor for carrying out specific processing activities (on behalf of the Customer), it will do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on Privacyboard in accordance with these Clauses. Privacyboard will ensure that the sub-processor complies with the obligations to which Privacyboard is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(e) At the Customer's request, Privacyboard provides a copy of such a sub-processor agreement and any subsequent amendments to the Customer. To the extent necessary to protect business secret or other confidential information, including personal data, Privacyboard may redact the text of the agreement prior to sharing the copy.

(f) Privacyboard remains fully responsible to the Customer for the performance of the sub-processor's obligations in accordance with its contract with Privacyboard. Privacyboard will notify the Customer of any failure by the sub-processor to fulfill its contractual obligations.

7.9. Personal data transfers outside the EU/EEA

(a) Any transfer of personal data to a country or an international organization outside the EU/EEA by Privacyboard is operated only on the basis of performing the services for and to the Customer or in order to fulfill a specific requirement under Union or Member State law to which Privacyboard is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) If the storage and/or processing of Personal Data as described in Appendix II involves a transfer of personal data to Privacyboard outside of the EU/EEA, and Regulation (EU) 2016/679 applies to the transfer, then Standard Contractual Clauses for the transfer of personal data to third countries (hereinafter "SCCs") are to be incorporated into and form a part of this Agreement in accordance.

(c) The Customer agrees that where Privacyboard engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Customer) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, Privacyboard and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by, in particular:

implementing appropriate safeguards such as SCCs adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those SCCs are met, or

being subject to binding corporate rules in accordance with Article 47 of Regulation (EU) 2016/679, or

ensuring that such transfer is covered by a decision of adequacy by the European Commission in accordance with Article 45 of Regulation (EU) 2016/679, or

complying to the derogations for specific situations in accordance with Article 49 of Regulation (EU) 2016/679.

Clause 8: Assistance to the Customer

8.1 Data subjects rights

(a) Privacyboard promptly notifies the Customer of any request it has received from the data subject. It will not respond to the request itself, unless authorized to do so by the Customer.

(b) Privacyboard assists the Customer in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), Privacyboard complies with the Customer's instructions.

8.2 Cooperation with the Customer

Privacyboard furthermore assists the Customer in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to Privacyboard:

(a) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(b) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk;

(c) the obligation to ensure that personal data is accurate and up to date, by informing the Customer without delay if Privacyboard becomes aware that the personal data it is processing is inaccurate or has become outdated;

(d) the obligations under Article 32 Regulation (EU) 2016/679.

Clause 9: Notification of personal data breach
In the event of a personal data breach concerning data processed by Privacyboard, Privacyboard notifies the Customer without undue delay

after having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification will contain the information then available and further information will, as it becomes available, subsequently be provided without undue delay.

Privacyboard cooperates with and assists the Customer for the Customer to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to Privacyboard.

Clause 10: Non-compliance with the Clauses and termination

10.1 Suspension of the processing activity

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that Privacyboard is in breach of its obligations under these Clauses, the Customer may instruct Privacyboard to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. Privacyboard promptly informs the Customer in case it is unable to comply with these Clauses, for whatever reason.

(b) The Customer shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these

Clauses if:

(1) the processing of personal data by Privacyboard has been suspended by the Customer pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) Privacyboard is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 ;

(3) Privacyboard fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) Privacyboard shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Customer that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the Customer insists on compliance with the instructions.

10.2 Destruction or return of the Customer's personal data

Following termination of the Services, Privacyboard, at the choice of the Customer, deletes all personal data processed on behalf of the Customer and certify to the Customer that it has done so on request, or, returns all the personal data to the Customer and deletes existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, Privacyboard shall continue to ensure compliance with these Clauses.

Appendix I: List of parties

Controller(s): [Identity and contact details of the Customer(s), and, where applicable, of the Customer's data protection officer]

1. Name: _____

Address: _____

Contact person's name, position and contact details: _____

Signature: _____

Accession date: _____

Processor(s):

1. Name: Privacyboard

Address: 12 Boulevard Voltaire, 75011 Paris, France

Contact person's name, position and contact details: Antoine Milkoff, CEO (hello@privacyboard.co)

Signature: _____

Accession date: _____

Appendix II: Description of the processing

Categories of data subjects whose personal data is processed:

Users
Customers

Categories of personal data processed:

Identification data
Professional data
Connection data
Internet data
Economic and financial data

Nature of the processing:

Send transactional email
Creation and management of your account

Purpose(s) for which the personal data is processed on behalf of the Customer:

To inform users and help them use Privacyboard.
To grant users access to the service
administer and manage their accounts

Duration of the processing:

Processing activity	Retention period
Send transactional email	As long as necessary for the performance of the service
Creation and management of your account	As long as necessary for the performance of the service

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:

Subprocessor	Processing	Country	Privacy contact
Sendinblue	Mass emailing platform	European Union	privacy@sendinblue.com
Formagrid Inc dba Airtable	Database solution	USA	privacy@airtable.com
Wized	Web app builder	USA	

Appendix III: Technical and organizational measures including technical and organizational measures to ensure the security of the data and assistance to the customer

A: Security measures taken by Privacyboard
Measures for user identification and authorisation
Unique identifier per user
Strong password policy
SSO authentication
Multi-factor authentication

Measures for certification/assurance of processes and products
Antivirus on systems
Antivirus on devices
Software security updates

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Frequent data backup

Measures of pseudonymisation and encryption of personal data
HTTPS encryption in transit
TLS 1.2 or 1.3 used in transit
AES encryption at rest

Measures for ensuring the continuity of the protection of personal data when transferred to other organizations
Security assessment process
Security clauses and contractual obligations

Measures for ensuring system configuration, including default configuration
Privacy by design and by default

Measures for allowing data portability and ensuring erasure

Right request management process

Privacyboard may update or modify such measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Service.

B: Security measures taken by sub-processors

Subprocessor	**Security commitment**
Sendinblue	https://www.sendinblue.com/enterprise/security/
Formagrid Inc dba Airtable	https://www.airtable.com/security
Wized	

Standard Contractual Clauses

For the purposes of these Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 (hereinafter "SCCs") available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, the Customer is the controller of the personal data received and Privacyboard is the processor of such data.

For the purposes of the SCCs, the following shall apply:

(a) Module Two (Controller to Processor) will apply;

(b) Each Party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the SCCs;

(c) Clause 7 (Docking clause) shall be deemed as included;

(d) Clause 9 (a) (Use of sub-processors): Option 2 "General written authorization" will apply as set out in Clause 7.7 of this Agreement.

(e) Clause 11 (Redress: optional clause of redress mechanism before an independent dispute resolution body) shall be deemed as not included;

(f) Clause 13 (a) (Supervision): The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority;

(g) Clause 17 (Governing law): The Parties agree that this shall be the law to which the data exporter is subject.

(h) Clause 18 (b) (Choice of forum and jurisdiction): The Parties agree that any dispute between them arising from the SCCs shall be resolved by the courts of the country where the data exporter is established.

Annex I

A. List of parties

Privacyboard is the “data importer” and the Customer is the “data exporter” as set out in this Agreement.

B. Description of transfer

As described in the Appendix II of this Agreement.

C. Competent Supervisory Authority

The SCCs shall be governed by the law of the EU Member State in which the Customer is established.

Annex II - Technical and organizational measures including technical and organizational measures to ensure the security of the data

As listed in the Appendix III of this Agreement.

Annex III – List of sub-processors

As listed in the Appendix II of this Agreement.