Data Processing Agreement

This Data Processing Agreement (“Agreement“) forms part of the Agreement for the Services (“Principal Agreement“) between Stormly (as a “Data Processor”) and the Client (as a “Data Controller”) (and together as the “Parties”).

This Data Processing Agreement together with the “Data Processing Terms”” apply applies to all data sent from Client to Stormly; not only that part of data that would fall under the GDPR. While implemented with the GDPR in mind, it should be compatible with other potential data legislation as well, such as the new CCPA (California Consumer Privacy Act) that goes into effect on the 1st of January 2020.

Stormly has a dedicated Data Protection Officer: Maurice Sikkink, which can be reached by email at dpo@stormly.com.

Effective date: 6 September 2023

WHEREAS:

a. The Client acts as a Data Controller.
b. The Client wishes to subcontract certain Services, which imply the processing of personal data, to Stormly.
c. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
d. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

Article 1. Definitions and Interpretation

1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
    a. **Agreement:** this Data Processing Agreement.
    b. **Client Personal Data:** any Personal Data Processed by a Contracted Processor on behalf of Client pursuant to or in connection with the Principal Agreement.
    c. **Contracted Processor:** a Subprocessor.
    d. **Data Protection Laws:** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.
    e. **EEA:** means the European Economic Area.
    f. **EU Data Protection Laws:** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
    g. **GDPR:** EU General Data Protection Regulation 2016/679.
    h. **Data Transfer:** (i) a transfer of Client Personal Data from the Client to a Contracted Processor; or (ii) an onward transfer of Client Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).
    i. **Services:** the SaaS services that Stormly provides.
    j. **Subprocessor:** any person appointed by or on behalf of Stormly to process Personal Data on behalf of the Client in connection with the Agreement.
    k. **Sensitive Data:** (a) social security number, passport number, driver's license number or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under the GDPR or any other applicable Data Protection Laws.
    l. The terms, **“Commission”**, **“Controller”**, **“Data Subject”**, **“Member State”**, **“Personal Data”**, **“Personal Data Breach”**, **“Processing”** and **“Supervisory Authority”** shall have the same meaning as in the GDPR, and their

cognate terms shall be construed accordingly.

Article 2. Processing of Client Personal Data

1. Stormly shall:
    a. comply with all applicable Data Protection Laws in the Processing of Client Personal Data; and
    b. not Process Client Personal Data other than on the relevant Client's documented instructions.
2. The Client instructs Stormly to process Client Personal Data.

Article 3. Details of Data Processing

1. Stormly processes data of Client to provide Services to the Client as agreed upon in the Principal Agreement.
2. Information is processed which is sent by Clients' end-user to Stormly, via different programmatic integrations, such as, but not limited to: Stormly's Javascript website integration library, import functionality, custom tracking end-points and 3rd party data sources. The following is a list of Personal Data properties that may be processed due to integrations as described above.

    Automatically tracked general properties for all integrations:

    - Timestamp of action
    - User created timestamp
    - User last active at
    - Previous user id (in case of identifying an anonymous user)
    - Referred by user id (in case share codes are used to track invites)
    - IP (not stored and anonymized by removing the last octet. Only used temporarily to generate other properties like Geolocation and timezone)
    - The timezone of request, based on anonymized IP
    - Anonymized Geo coordinates, country, city and connection type, based on IP anonymized address

    For Web integrations the following is tracked automatically:

    - User Identifier (using a first-party cookie)
    - Browser User Agent, version and name
    - Page URL and title
    - HTTP referrer
    - UTM campaign properties
    - Screen width and height
    - Operating System name and version
    - Locale
    - Share code

    For App integrations the following properties are tracked only if set by the developer of the App, or using 3rd party data sources like Segment.com:

    - User Identifier (implementation is up to Client or 3rd party data source used)
    - Screen width, height and density
    - App name, version and build
    - Device id, name, model, manufacturer
    - Device advertising id, and if ad is tracking enabled
    - If device network is using bluetooth, cellular, wifi, and the network in case of cellular
    - Referrer id, name and type
    - Custom Campaign properties
    - Operating System name and version
    - Locale
    - Share code

Article 4. Categories of Data Subjects

The categories of Data Subject are Clients' End-User, such as but not limited to users of web and mobile applications, or any custom imported data containing users and their actions.

Article 5. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Client Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Article 6. Security

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Stormly shall in relation to the Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
2. In assessing the appropriate level of security, Stormly shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
3. To see what third-party service providers Stormly uses and that may be used to process Personal Data and their compatibility with the GDPR and other data regulation frameworks, see "Security Architecture Document".

Article 7. Subprocessing

1. Stormly may engage another processor (sub-processor) without prior specific authorization of the Data Controller. Stormly shall inform the Client of any intended changes concerning the addition or replacement of other processors (sub-processors), thereby giving the Client the opportunity to object to such changes.
2. Where Stormly engages another processor (sub-processor) for carrying out specific processing activities on behalf of the Client, the same data protection obligations as set out this processor agreement or other legal act between the Client and Stormly as referred to in article 28, paragraph 3, of the GDPR, shall be imposed on that other processor (sub-processor) by way of contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.
3. Stormly uses the sub-processors as identified on Stormly's website here, which list may be updated by Stormly from time to time. By using the Services, the Client hereby provides authorization to engage such sub-processors. For a list of Sub-processors appointed by Stormly see: "Security Architecture Document".

Article 8. Data Subject Rights

1. Taking into account the nature of the Processing, Stormly shall assist the Client by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client obligations, as reasonably understood by Client, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
2. Stormly shall:
    a. promptly notify Client if it receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data; and
    b. ensure that it does not respond to that request except on the documented instructions of Client or as required by Applicable Laws to which Stormly is subject, in which case Stormly shall to the extent permitted by Applicable Laws inform Client of that legal requirement before the Contracted Processor responds to the request.
3. Stormly provides programmatic and online tools so that Client can comply with user removal and user data retrieval requests. See "Data Processing Terms" for more information.

Article 9. Personal Data Breach

1. Stormly shall notify Client without undue delay upon Stormly becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow the Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
2. Stormly shall co-operate with the Client and take reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

Article 10. Data Protection Impact Assessment and Prior Consultation

Stormly shall provide reasonable assistance to the Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

Article 11. Deletion or return of Client Personal Data

Subject to this section 9, Stormly shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Client Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those Client Personal Data.

Article 12. Audit rights

1. Subject to this section 10, Stormly shall make available to the Client on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Client or an auditor mandated by the Client in relation to the Processing of the Client Personal Data by the Contracted Processors.
2. Information and audit rights of the Client only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

Article 13. Data Transfer

Any transfers of Personal Data under the Principal Agreement from the EU, EEA, Member States and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws or which transfer is not otherwise governed by a framework approved by the European Commission (such as the EU-US and Switzerland-US Privacy Shield framework) to which Stormly is officially certified, shall be subject to the Standard Contractual Clauses (SCC) of the European Commission. The Standard Contractual Clauses shall come into effect and be deemed executed upon execution of this Agreement and shall apply pursuant to the order of precedence described in the preceding sentence.

Article 14. Confidentiality

1. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that: (i) disclosure is required by law; (ii) the relevant information is already in the public domain.
2. In case it is required by comply with relevant laws, Client’s and/or End-User data might be released to the authorities.

Article 15. Notices

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

Article 16. Governing Law and Jurisdiction

1. This Agreement is governed by the laws of the Netherlands.
2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Amsterdam.

Article 17. Utilizing Chat GPT by Microsoft Azure

1. Engagement with Chat GPT by Microsoft Azure: When utilizing the AI assistant, Chat GPT by Microsoft Azure, within the Stormly platform, users consent that each query made to the AI, and its respective aggregate report results, will be stored on Microsoft Azure OpenAI platforms for a span of 30 days.
2. Nature of Data Shared with Chat GPT: Interactions with Chat GPT involve the transmission of event names, event property names and contents, user property names and contents. It's crucial to note that this data, in its standard form, doesn't encompass personally identifiable information (PII). However, if a company tailors its setup to capture specific PII such as email addresses, this action would contravene Stormly's terms of service.

3. Omitted Properties for Enhanced Privacy:
4. User Properties: "user id", "device advertising id", "device_id", "referrer id", "referrer url", "user agent", "referred by user id", "previous user id (once identified)", "share code"
5. Event Properties: "id", "user id", "device advertising id", "device id", "referrer id", "ip", "referrer url", "user agent", "referred by user id", "share code"
6. Aggregate Data Sharing: While specific contents of user properties, such as countries, are shared, the information is presented in an aggregate manner. For example, instead of user-level specifics, data may indicate a distinct summarization of all tracked country or device types, without pinpointing individual users.
7. Liability Stipulation: Stormly is not accountable for any repercussions, including damages or losses, resulting from the usage of the Chat GPT service powered by Microsoft Azure.
8. Emphasis on Data Security: Stormly prioritizes data security and privacy. Users are earnestly cautioned against transmitting any sensitive or personal data within the chat interface. Adhering to Stormly's guidelines is paramount to ensure a secure and privacy-conscious platform experience.
9. By electing to interact with Chat GPT by Microsoft Azure on Stormly, users affirm their agreement to the stipulated terms and conditions.