Data Processing Addendum (DPA)

This Loopify Data Processing Addendum ("Addendum" or “DPA”) forms an integral part of the agreement relating to the provision of services as governed by the Loopify Terms of Service (https://loopify.com/legal/terms) (the "Agreement") between the Customer ("Controller") and Loopify AS, Ruseløkkveien 6, 0251 Oslo, Norway ("Loopify" or "Data Processor").

Any capitalized terms used in this DPA shall, in addition to the terms defined in the Agreement, have the same understanding as in the EU General Data Protection Regulation (2016/679) (“GDPR”).

1. Definitions

The following capitalized terms used in this DPA shall be defined as follows;

1. "Customer" means the party having entered into the Agreement for the provision of services from Loopify.
2. "Customer Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (as defined in the GDPR) and any other personal data that Loopify Processes on behalf of the Customer in connection with the provision of the Loopify App.
3. "Data Protection Laws" means the "GDPR, any applicable national implementing legislation including, and in each case as amended, replaced or superseded from time to time, and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Customer Personal Data.
4. "Security Incident" means a breach of security leading to the accidental or unlawful alteration, loss, unauthorized disclosure of, destruction, or access to, any Customer Personal Data transmitted, stored, or otherwise processed.
5. "Sub-processor" means any Processor engaged by Loopify, who agrees to receive from and process Loopify Customer Personal Data.
6. "Parties" means "Loopify" and the "Controller" jointly.

2. Data Processing

1. Instructions for Data Processing. Loopify will only Process Customer Personal Data in accordance with the Customer's written instructions unless Processing is required by the European Union or Member State to which Loopify may be subject, in which case Loopify shall, to the extent permitted by law, inform the Customer of that legal requirement before Processing that Customer Personal Data. The Agreement (subject to any changes to the Loopify Services agreed between the Parties) and this Addendum constitute Customers instructions to Loopify in relation to the Processing of Customer Personal Data.
2. Processing outside the scope of this Addendum or the Agreement will require a prior written agreement between the Customer and Loopify on additional instructions for Processing.

3. The Processor has no reason to believe that legislation applicable to it prevents the Processor from fulfilling the instructions mentioned above. The Processor shall, upon becoming aware of it, notify the Controller of instructions or other Processing activities by the Controller, which in the opinion of the Processor, infringes applicable privacy legislation.
4. The categories of Data Subject's and Personal Data subject to Processing according to this Agreement are outlined in Annex 1.
5. Required legal basis for the processing of personal data. Where required by applicable Data Protection Laws, the Customer will ensure that it has a legal basis to process and disclose to the Processor (including any Sub-processors) the Personal Data for the Processing of Customer Personal Data in Loopify in accordance with the Agreement.

3. Transfers of Customer Personal Data

1. Authorized Sub-processors. The Customer agrees that Loopify may use Sub-processors to Process Customer Personal Data The data processor has the data controller's general authorization for the engagement of Sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of Sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The list of Sub-processors already authorized by the data controller can be found in Annex 3.
2. If the Customer objects to a new Sub-processor Loopify shall make commercially reasonable efforts to make a change in the Services, or if Loopify is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, the Customer may terminate the applicable part of the Services which cannot be provided by Loopify without the use of the new Sub-processor. Loopify shall enter into a written agreement with the Sub-processor, which imposes equivalent obligations on the Sub-processor with regard to their Processing of Customer Personal Data, as are imposed on Loopify under this DPA. Loopify shall at all times remain responsible for compliance with our obligations under the DPA and will be liable to Customer for the acts and omissions of any Sub-processor as if they were Loopify's acts and omissions.
3. Transfers of Customer Personal Data to third countries. To the extent that the Processing of Customer Personal Data by Loopify involves the export of such Customer Personal Data to a country or territory outside the EEA, other than to a country or territory that is ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of personal data as determined by the European Commission (an "International Transfer"), such transfer shall be governed by this DPA. In addition, any transfer of personal data to third countries shall always take place in compliance with Chapter V GDPR. Loopify has the authorization to sign applicable EU Model Clauses on behalf of the Customer when so required to allow for the transfer of personal data to a third country.

4. Data Security, Audits, and Security Incident Notifications

1. Upon the Customer's reasonable request, Loopify will make available all information reasonably necessary to demonstrate compliance with this DPA.
    a. Security Incident Notification. If Loopify becomes aware of a Security Incident, Loopify will notify the Customer of the Security Incident without undue delay; and
    b. investigate the Security Incident and provide the Customer (and any law enforcement or regulatory official) with reasonable assistance as required to investigate the Security Incident and enable the Customer to notify to authorities or Data Subjects in accordance with GDPR Art. 33.

2. Employees and Personnel. Loopify will treat the Customer Personal Data as confidential and shall ensure that any employees or other personnel have agreed to protect the confidentiality and security of Customer Personal Data.
3. Audits. Loopify will, upon reasonable request from the Customer, allow for and contribute to audits, including inspections, conducted by the Customer (or a third party auditor on behalf of, and mandated by, the Customer) provided (i) such audits or inspections are not conducted more than once per year (unless requested by a Supervisory Authority); (ii) are conducted only during business hours; and (iii) are conducted in a manner that causes minimal disruption to Loopify's operations and business.
4. Loopify shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to Loopify's physical facilities on presentation of appropriate identification.

5. Access Requests and Data Subject Rights

1. Government Disclosure. Loopify will notify the Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency having judicial power over Loopify.
2. Data Subject Rights. Where applicable, and taking into account the nature of the Processing, Loopify will use reasonable endeavors to assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject rights laid down in the Data Protection Laws including in Chapter III GDPR. All-access requests shall be forwarded to the Customer with undue delay. Loopify will not respond to any Data Subject requests unless instructed to do so by the Customer. Assistance provided by Loopify will be charged at hourly rates.

6. Assessment and Prior Consultation

1. To the extent required under applicable Data Protection Laws, Loopify will provide Customer with reasonably requested information regarding the Loopify Services to enable the Customer to carry out data protection impact assessments or prior consultations with any Supervisory Authority, in each case solely in relation to the Processing of Customer Personal Data and taking into account the nature of the Processing and information available to Loopify.

7. Termination

1. Deletion of data. Loopify will, within 90 (ninety) days of the date of termination of the Agreement, securely delete the Customer Personal Data Processed by Loopify.
2. Loopify and its Sub-processors may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that Loopify ensures the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8. Choice Legal Venue and Place of Jurisdiction

1. This DPA is governed by Norwegian law. Any dispute arising out of or in connection with this DPA that cannot be resolved by negotiations shall be solved by ordinary court proceedings with Oslo District Court (Oslo tingrett) as the competent legal venue.

Contact person Data Controller	
Name	
Mobile	
Email	

Contact person Data Processor	
Name	Stig Sætre
Mobile	+4790109670
Email	stig.saetre@loopify.com

Date: _____

_____
For Data Controller

Date: 18th of December 2023

_____
For Data Processor

This Agreement is prepared in two –2– copies, one –1– of which is to be kept by each of the parties.

Annex 1: Details of Processing of Personal Data

This Annex includes certain details of the processing of Personal Data:

1. Subject Matter and Duration of the Processing of Personal Data

- The subject matter and duration of the processing of the Personal Data are set out in the Agreement.

2. The Nature and Purpose of the Processing of Personal Data

- Under the Agreement, Loopify provides certain marketing automation services, including email services to the Customer.

3. The Types of Personal Data to Be Processed

- The personal data transferred includes name, email, IP address, and personal data included in the message content.
- The categories of data subjects to whom the Personal Data relates to are senders and recipients of email messages and SMS.

Annex 2: Information Security

For the purpose of securing the personal data processed, Loopify uses the industry best practices.

1. Information Systems and Software Access Controls

- All information systems and services have formal user registration and deregistration process for granting and withdrawing access authorizations.
- The complexity of passwords and PINs is subject to minimum requirements that meet the current state of the art.
- Password procedures (e.g., the prohibition of disclosure, storage) are regulated in written form. Access to sensitive data is restricted to senior developers and senior management located inside of the EU.
- Other employees, like customer support and consultants, have to be invited by the customer to have access to the data.
- We use an authentication process with OAuth2 security level to prevent unauthorized use of access tokens.

2. Communication and Operations Management

- **Separation of development, test, and operational facilities**
  - Loopify has separated environments for software development, testing, and live operations.
  - To prevent inappropriate developer access, front-end developers do not have access to sensitive customer data.
  - We do not use operational databases containing personal information or any other sensitive information for testing purposes
- **Third-party service delivery management**
  - We work with third-party suppliers for server hosting, email, and SMS delivery.
  - Third-party suppliers must have satisfying data processing agreements as well as privacy policies in place.
  - There are procedures in place for how to deal with a security breach experienced by a third-party supplier.
- **System capacity management**
  - We have chosen to outsource all scalable operational elements to reliable third-party suppliers.
  - We use Cloudflare which provides DDoS mitigation against incoming attacks.
  - We use AWS for secure cloud computing services and database storage.
- **Backup**
  - Backup copies of code are taken regularly enabling us to restore any earlier versions of the software.
- **Management of removable media.**
  - Employees are not allowed to store any sensitive data on non-password-protected media.
  - Employees are not allowed to print out any sensitive customer data.
- **Payment systems and online transactions**
  - We work with a reliable third-party supplier for credit card invoicing. We do not access any sensitive cardholder data, like credit card numbers or CVC.

3. User Password Security

- User passwords are stored encrypted. Passwords cannot be restored by us, only by the user.

4. Device Access Controls

- All devices used to log in to the software must be password-protected.
- Employees are allowed to log in to the software from their personal computers and devices as long as they do not leave them unlocked and supervised and log out immediately after use.

5. Network Access Controls

- The wireless network in our offices is secured against unauthorized access. Only employees have the password to access these networks.
- None of the wireless networks provides access to any shared information because we have chosen SaaS as a way of storing all shared documents.

Annex 3: List of Data Processors

Sub-processor	Processing activity	Location
Mailgun Technologies, Inc.	This data processor manages the delivery of emails.	United States
Amazon Web Services	This data processor is used for secure cloud computing services and database storage.	Ireland
MongoDB	This data processor is used to store, retrieve, and support huge volumes of both data and traffic.	United States
Sinch UK	Sinch is used to manage the sending of SMS and verification via text messages.	United Kingdom
Google	Google services are used for web analytics, marketing, and advertising purposes.	United States
Cloudflare, Inc	Cloudflare is used to provide secure, fast, reliable network services.	United States
ExaVault, Inc	This data processor is used for secure business file transfer via a cloud SFTP Service.	United States
Sentry (Functional Software, Inc)	Sentry is used for error tracking and application monitoring.	United States