flipsnack

DPA

Flipsnack 2024

Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the Agreement between the party identified in the Agreement ("**Customer**") and Flipsnack and applies to the extent that Flipsnack processes Personal Data on behalf of Customer in the course of providing the Services. This DPA is entered into as of the later of the dates beneath the parties' signature below.

1. Definitions and interpretation

1.1. "**Agreement**" means the written or electronic agreement between Customer and Flipsnack for the provision of Services to Customer.

1.2. "**Controller**" is the party that determines the purposes and means of the Processing of Personal data.

1.3. "**Processor**" the party that Processes Personal Data on behalf of the Controller.

1.4. "**Personal data**" means any information relating to an identified or identifiable natural person within the meaning of GDPR.

1.5. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6. "**Data subject**" the identified or identifiable natural person that the Personal Data is related to.

1.7. "**Data Protection Law**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

1.8. "**GDPR**" means 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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9. "**Flipsnack**" means the Flipsnack entity that is a party to the Agreement and this DPA, Flipsnack LLC, a company incorporated in the State of Michigan.

1.10. "**Sub-processor**" means any entity engaged by Flipsnack to Process Personal Data in connection with the Services.

1.11. "**Services**" means the marketing services provided by Flipsnack to Customer pursuant to the Agreement.

1.12. "**Supervisory Authority**" means an independent public authority that is established by an EU Member State pursuant to GDPR.

2. Processing of Customer Personal Data

2.1. The Parties acknowledge and agree that with regard to the processing of Personal Data, Customer is the Controller, and Flipsnack is the Processor. In some circumstances, Customer may be a Processor, in which case Customer appoints Flipsnack as Customer's sub-processor, which shall not change the obligations of either Customer or Flipsnack under this Data Processing Addendum, as Flipsnack will remain a Processor with respect to the Customer in such event.

2.2. Flipsnack shall process Personal Data for the purposes set forth in the Agreement and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. The Agreement and this Data Processing Addendum set out Customer's complete instructions to Flipsnack in relation to the Processing of Personal Data, and any Processing required outside the scope of these instructions will require prior written agreement of the parties.

2.3. Flipsnack ensures that: (a) only employees who must have access to the Personal Data in order to meet Flipsnack's obligations under the Agreement have access to Personal Data, (b) such employees have received appropriate training regarding their responsibilities and obligations with respect to the Processing, protection, and confidentiality of Personal Data.

2.4. Flipsnack, as Processor, has complied and will continue to comply with all applicable requirements of the GDPR, CCPA, and if to the extent agreed between parties in writing, Data Protection Legislation in other jurisdictions to the extent Customer and Flipsnack have agreed such legislation is applicable, and the Service is able to comply.

2.5. Customer, as a Controller, shall be responsible for ensuring that, in connection with Customer Data and Subscription Services: (a) it has complied, and will continue to comply, with all applicable privacy and data protection laws, including EU Data Protection Legislation; and (b) it has, and will continue to have, the right to transfer or provide access to, the Personal Data to Flipsnack for Processing in accordance with the terms of the Agreement and this Data Processing Addendum.

3. Data Breach

3.1. Upon becoming aware of a Security Incident, Flipsnack shall notify the Customer no later than 24 hours and will provide information relating to the Personal Data Breach as reasonably requested by the Customer. Flipsnack will take steps to immediately identify

and remediate the cause of such Security Incidents.

4. Security

4.1. Flipsnack will implement and maintain appropriate technical and organizational measures (TOMs) to protect against Personal Data Breaches and to preserve the security and confidentiality of Personal Data processed by Flipsnack on behalf of the Customer in the provision of the Service. TOMs are subject to technical progress and development. Accordingly, Flipsnack may update or modify the TOMs provided that the functionality and security of the Services are not degraded.

5. Audit Reports; Privacy Impact Assessment

5.1. On written request from Customer, Flipsnack shall provide necessary information to demonstrate compliance with this DPA and shall allow for and contribute to audits by the Customer or a reputable auditor mandated by Customer in relation to the Processing of the Customer Personal Data by Flipsnack, provided that Customer shall not exercise this right more than once in any 12 months rolling period.

5.2. Customer and Flipsnack will discuss and agree in advance on the reasonable start date, scope, and duration of security and confidentiality obligations applicable to any audits.

5.3. Where required by Data Protection Laws, Flipsnack will reasonably cooperate with Customer, at Customer's expense, where Customer is conducting a data protection impact assessment. Such assistance shall be solely in relation to the processing of Customer Personal Data by Flipsnack.

5.4. If the Customer is subject to inspection by supervisory authorities or other bodies, or if data subjects assert their rights against it under Chapter III of the GDPR, the Contractor undertakes to support the Customer to the extent necessary insofar as the commissioned processing is concerned. The Contractor may provide information to third parties or the data subjects only with the prior consent of the Customer. It shall immediately forward requests addressed directly to the Customer.

5.5. The Contractor undertakes to assist the Customer in its obligations under Articles 32 to 36 of the GDPR to the extent necessary.

6. Confidentiality

6.1. Confidentiality of Processing. Flipsnack shall ensure that any person that it authorizes to Process the Personal Data (including its staff, agents, subcontractors, and Sub-processors) shall be subject to a duty of confidentiality (whether a contractual or statutory duty) that shall survive the

termination of their employment and/or contractual relationship.

7. Return or Deletion of Customer Personal Data

7.1. Upon termination or expiration of the Agreement, Flipsnack shall, in accordance with the terms of the Agreement, delete or make available to Customer for retrieval all relevant Personal Data (including copies) in Flipsnack's possession, save to the extent that Flipsnack is required by any applicable law to retain some or all of the Personal Data. In such event, Flipsnack shall extend the protections of the Agreement and this DPA to such Personal Data and limit any further Processing of such Personal Data to only those limited purposes that require the retention, for so long as Flipsnack maintains the Personal Data. Flipsnack shall furnish verification of proper destruction and submit such verification to the Controller without delay.

8. Data Transfers

8.1. Any transfer of Personal Data under this Data Processing Agreement from the European Union, where GDPR applies, to countries outside of the EU shall be conducted in accordance with the Data Privacy Framework. Flipsnack participates in the EU-US Data Privacy Framework, UK Extension to Data Privacy Framework and Swiss-U.S Data Privacy Framework and adheres to Data Privacy Framework Principles regarding the collection, use, sharing, and retention of Personal Data from the European Union.

9. Sub-processors

9.1. Flipsnack will enter into an agreement with each Sub-processor that obligates the Sub-processor to process Personal Data in a manner consistent with the standards set forth in the DPA and, at minimum, at the level of data protection required by Data Protection Law.

9.2. Flipsnack engages Sub-processors to provide certain services on its behalf. The customer consents to Flipsnack engaging Sub-processors to process Personal Data under the Agreement. Flipsnack will be responsible for any act, errors, or omissions of its sub-processes that cause Flipsnack to breach any of its obligations under this DPA.

9.3. Flipsnack will provide a list of sub-processors that it engages in to process Personal

Data upon written request by the customer or as otherwise made available by Flipsnack on its website: https://legal.flipsnack.com/flipsnack-sub-processors.

9.4. Flipsnack agrees to (i) to provide prior notice to Customer, add or make changes to the Sub-processors; and (ii) if Customer has a reasonable objection to any new or replacement Sub-processor, it shall notify Flipsnack of such objections in writing within ten (10) days of the notification, and the parties will seek to resolve the matter in good faith.

10. Governing Law

10.1. This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and in accordance with the laws of the State of Michigan.

11. Termination

11.1. This DPA shall terminate automatically upon termination of the Agreement.

12. Miscellaneous

12.1. Except as amended by this DPA, the Agreement will remain in full force and effect.
12.2. In the event of any conflict between this DPA and any privacy-related provisions in the Agreement, the terms of this DPA will prevail.

The parties' authorized signatories have duly executed this DPA.

On behalf of _____ (Customer):

Name (written out in full): _____
Position:_____
Address:_____
Signature: _____

On behalf of Flipsnack LLC

Name: Emanuil Nagy
Position: Legal Counsel
Address: 37310 Ruth Dr, Sterling Heights, Michigan, 48312-1977, USA.
Signature: 

ANNEX A

TECHNICAL AND ORGANISATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Details of Flipsnack's technical and organizational security measures to protect customers' data are available at:

- https://www.flipsnack.com/security
- https://player.flipsnack.com/?hash=Qjc1NUI4NTU2OUIrem44MmNodWJkYw==
- https://player.flipsnack.com/?hash=Qjc1NUI4NTU2OUIrN2g5NjNtaGJkYw==
- https://legal.flipsnack.com/privacy-policy

Further information regarding the technical and organizational security measures is set forth below:

1. Information Security Program.

Flipsnack has developed a set of security policies covering a range of topics, and they are periodically updated.

2. Information Security Unit.

Flipsnack has a dedicated security team to enforce security practices and respond to security incidents quickly.

3. Security Certifications.

An independent third party has audited Flipsanck for the following security-related certifications: ISO270001:2013, ISO9001:2015, ISO20000-1, CSA Star Level 1, and Cyber Essentials.

4. Data Hosting and Storage.

Flipsnack services and data are hosted in Amazon Web Services (AWS) facilities in the USA. Further details regarding the security controls implemented by AWS for their data centers can be found at https://aws.amazon.com/compliance/data-center/controls/ .

5. Encryption.

For data at rest, we use AWS Key Management Service (AWS KMS) to store and manage encryption keys and the Advanced Encryption Standard algorithm with 256-bit keys (AES-256) to perform the encryption

With regard to data in transit, we use SSL for every request between our customers and Flipsnack. Please check TLSv1.2_2018 on https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html#secure-connections-supported-ciphers for a complete list regarding our algorithms and protocols. Key size: 2,048 bits Algorithm: SHA-256 with RSA Encryption

6. Data back-up.

All data within Flipsnack is replicated across multiple database servers to prevent a single failure from causing data loss.

7. Password and Credential Storage.

Flipsnack credentials are stored encrypted using bcrypt algorithm.

8. Two-factor Authentication.

We have 2-factor authentication enforced (2FA) and strong password policies on Google, AWS, and other tools required for our daily tasks to ensure access to cloud services is protected.

9. Virtual Private Cloud.

All of Flipsnack's servers are within our virtual private cloud (VPC) with network access control lists (ACLs) that prevent unauthorized requests from getting to our internal network.

10. Failover and Disaster Recovery.

Flipsnack was built with disaster recovery in mind. Our infrastructure and data are spread across 3 AWS availability zones and will continue to work should any of those data centers fail.

11. Incident Response.

Flipsnack uses an internal protocol for handling security events, including escalation procedures, rapid mitigation, and post-mortem. All employees are informed of our policies.

12. Quality Assurance.

All changes to the Flipsnack application are subject to peer review and testing before being merged.

13. On-Site Security.

Flipsnack offices are secured by keycard access and biometrics and monitored with infrared cameras throughout.

14. Zero trust.

Flipsnack runs a zero-trust corporate network, meaning every employee must authenticate to access any of Flipsnack's resources.

15. Least privileged access.

Access to customer data is limited to authorized employees who absolutely need it for their jobs.