DATA PROCESSING ADDENDUM

(Revision July 2024)

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement or other written or electronic agreement between Braze, Inc. and Customer (the "**Agreement**") for the purchase of online services from Braze (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as **"Services"** or **"Braze Services**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Braze processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Braze Services to Customer pursuant to the Agreement, Braze will Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules. This DPA supersedes all prior and contemporaneous data processing agreements or data processing terms in any agreements, proposals or representations, written or oral, concerning the Processing of Personal Data.

1. DEFINITIONS

"Authorized Affiliate" means any of Customer's Affiliate(s) which (i) is subject to the Data Protection Laws and Regulations of any jurisdiction that requires a data processing agreement between a Controller and a Processor for the Processing of Personal Data under this Agreement , and (ii) is permitted to use the Braze Services pursuant to the Agreement between Customer and Braze but has not signed its own Order Form with Braze.

"CCPA" means the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100 et seq., as it is amended by the California Privacy Rights Act of 2020 ("**CPRA"**), their implementing regulations, as further amended from time to time.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data, including equivalent terms under Data Protection Laws and Regulations such as "**Business**".

"Customer Data" means what is defined in the Agreement as "Customer Data".

"Dashboard User" means an individual who is authorized by Customer to use the Braze Services (whether defined as Dashboard User or User in the Agreement).

"**Data Protection Laws and Regulations"** means all laws and regulations applicable to a party in its use or provision of the Braze Services, in connection with the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates, including equivalent terms under Data Protection Laws and Regulations such as "**Consumer**".

"Data Subject Right" means any right afforded to a Data Subject under Data Protection Laws and Regulations.

"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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and/or the UK GDPR as applicable.

"Personal Data" means any information relating to an identified or identifiable End-User, including equivalent terms under Data Protection Laws and Regulations such as "**Personal Information**", where such data is Customer Data.

"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, retention, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including equivalent terms under Data Protection Laws and Regulations such as "**Service Provider**".

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Braze or its Sub-processors of which Braze becomes aware.

"**Sell**" or "**Share**" have the definitions ascribed to them in the CCPA or as similarly defined in U.S. Data Protection Laws and Regulations.

"**UK Addendum**" means the International Data Transfer Addendum to the SCCs, issued by the Information Commissioner under S119A(1) Data Protection Act 2018, Version B1.0, that Customer and Braze, Inc. may enter into, and that Braze makes available at www.braze.com/legal.

"**2021 EU SCCs**" or "**SCCs**" means the "Controller to Processor" modules of the 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, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, that Customer and Braze, Inc. may enter into and that Braze makes available at www.braze.com/legal.

"P2P SCCs" means the "Processor to Processor" modules of the 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, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 that Braze may enter into with its Sub-processors.

"Sub-processor" means any processor engaged by Braze or its Affiliates engaged in the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1 Details of the Processing. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Braze is the Processor and that Braze or its Affiliates engaged in the Processing of Personal Data will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below. The subjectmatter of Processing of Personal Data by Braze is the performance of the Braze Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA. The parties shall exercise their rights hereunder acting in good faith and in a reasonable manner.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Braze Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Upon entering into this DPA, this DPA, the Agreement and any applicable Order Form(s) are Customer's documented instructions to Braze for the Processing of Personal Data. Any additional or alternate instructions must be reasonable and consistent with the terms of this DPA and the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data.

2.3 Braze's Processing of Personal Data. Braze shall only Process Personal Data in accordance with Customer's documented instructions pursuant to Section 2.2 above, and for the following purposes: (i) Processing in accordance with the Agreement, applicable Order Form(s) and Data Protection Laws and Regulations; and (ii) Processing initiated by Dashboard Users in their use of the Braze Services (collectively the "**Business Purpose**"). Braze shall not Process Personal Data for any purpose other than the Business Purpose or outside of the direct business relationship with Customer. Braze shall, in its provision of the Braze Services, Process Personal Data in accordance with Data Protection Laws and Regulations, provided that Braze shall not be in violation of this contractual obligation in the event that Braze's Processing of Personal Data in non-compliance with Data Protection Laws and Regulations arises from Customer's use of the Braze Services in violation of the Agreement. Braze shall not Sell or Share Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Requests. Braze shall, to the extent legally permitted and to the extent Braze has been able to identify that the request comes from a Data Subject whose Personal Data was submitted to the Braze Services by Customer, promptly notify Customer if Braze receives a request from a Data Subject in relation to the exercise of any Data Subject Right ("**Data Subject Request**"). Braze will confirm to the Data Subject that it has passed the request to the Customer, but Braze shall not handle or execute the Data Subject Request.

3.2 Taking into account the nature of the Processing, Braze shall assist Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

4. BRAZE PERSONNEL

4.1 Confidentiality. Braze shall 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 on their responsibilities and have executed

written confidentiality agreements. Braze shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Braze shall treat Personal Data as Confidential Information.

4.2 Reliability. Braze shall take commercially reasonable steps to ensure the reliability of any Braze personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Braze shall ensure that Braze's access to Personal Data is limited to those personnel performing Braze Services in accordance with the Agreement.

4.4 Data Protection Officer. Braze has appointed a data protection officer for Braze and its Affiliates. The appointed person may be reached at privacy@braze.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Braze's Affiliates may be retained as Subprocessors; and (b) Braze and Braze's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Braze Services. Braze or a Braze Affiliate has entered into a written agreement with each Sub-processor containing, in substance, the same data protection obligations as in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Attached hereto as Schedule 3 is a current list of Sub-processors for the Braze Services. Such Sub-processor list shall include the identities of those Sub-processors, their country of location as well as a description of the processing they perform. Braze will notify Customer of a new Subprocessor(s) at least thirty (30) calendar days before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Braze Services. The notification shall include an updated Sub-processor list which is the information necessary to enable the Customer to exercise its right to object.

5.3 Objection Right for New Sub-processors. Customer may object to Braze's use of a new Sub-processor by notifying Braze promptly in writing within ten (10) calendar days after receipt of Braze's notice in accordance with Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Braze will use reasonable efforts to make available to Customer a change in the Braze Services or recommend a commercially reasonable change to Customer's configuration or use of the Braze Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Braze is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Braze Services which cannot be provided by Braze without the use of the objected-to new Sub-processor, by providing written notice to Braze. Braze will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Braze Services, without imposing a penalty for such termination on Customer.

5.4 Liability for Sub-processors. Braze shall be liable for the acts and omissions of its Sub-processors to the same extent Braze would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Braze shall maintain appropriate technical and organizational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Datasheet attached hereto as Schedule 2. Braze regularly monitors compliance with these measures. Customer is responsible for reviewing the information made available by Braze relating to data security and making an independent determination as to whether the Braze Services meet Customer's requirements and legal obligations under Data Protection Laws and Regulations. Customer acknowledges that the security measures described within the Security, Privacy and Architecture Datasheet are subject to technical progress and development and that Braze may update or modify such document from time to time provided that such updates and modifications do not result in a material decrease of the overall security of the Braze Services during a Subscription Term.

6.2 Personal Data Incident Management and Notification. Braze maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Datasheet and shall notify Customer without undue delay after becoming aware of a Personal Data Breach. Braze shall provide information to Customer necessary to enable Customer to comply with its obligations under Data Protection Laws and Regulations in relation to such Personal Data Breach. The content of such communication to Customer will (i) include the nature of Processing and the information available to Braze, and (ii) take into account that under applicable Data Protection Laws and Regulations, Customer may need to notify regulators or individuals of the following: (a) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Data records concerned; (b) a description of the likely consequences of the Personal Data Breach; and (c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. As between the parties, Customer is responsible for any required notification to Data Subjects and/or regulators of a Personal Data Breach. Braze shall make commercially reasonable efforts, based on its expertise, to identify the cause of such Personal Data Breach and take those steps as Braze deems

necessary and reasonable in order to remediate the cause of such Personal Data Breach to the extent the remediation is within Braze's reasonable control. The obligation to remediate the cause of a Personal Data Breach shall not apply to Personal Data Breaches that are caused by Customer or Customer's Dashboard Users.

7. RETURN AND DELETION OF PERSONAL DATA

At the termination or expiration of the Agreement, Braze shall return Personal Data by enabling Customer to export its Personal Data as set forth in the Agreement and shall delete Personal Data, in accordance with this DPA, the Agreement, applicable Data Protection Laws and Regulations and the Documentation. Upon request from the Customer, Braze will provide a certificate of deletion once Personal Data has been deleted from the Braze Services.

8. AFFILIATES

8.1 Relationship between Braze and Customer's Authorized Affiliates. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing an independent DPA between Braze and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 8 and Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For sake of clarity, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access to and use of the Braze Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

8.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Braze under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates and Authorized Affiliates.

8.3 Data Controller Rights of Affiliates and Authorized Affiliates. Any Affiliate or Authorized Affiliate shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

Except where applicable Data Protection Laws and Regulations require the Affiliate or Authorized Affiliate to exercise a right or seek any remedy under this DPA against Braze directly by itself, the parties agree that:

(i) solely the Customer that is the contracting party to the Agreement shall exercise any such right (including any Audit right) or seek any such remedy on behalf of such Affiliate or Authorized Affiliate,

(ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Affiliate or Authorized Affiliate individually but in a combined manner for all of its Affiliates and Authorized Affiliates together, and

(iii) when carrying out an On-site Audit, Customer shall take all reasonable measures to limit any impact on Braze and its Sub-processors by combining, to the extent reasonably possible, several Audit requests carried out on behalf of different Affiliates and Authorized Affiliates in one single Audit.

For the purpose of this Section 8.3, an Affiliate signing an Order Form with Braze is not deemed "Customer".

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Braze, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

10. COOPERATION

10.1 Upon Customer's request, Braze shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligations under Data Protection Laws and Regulations, including with regards to data privacy impact assessments and consultations with supervisory authorities, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Braze. Cooperation may include the provision of appropriate technical and organizational measures, where possible, through the Braze Services and/or as outlined in the Documentation.

10.2 Braze shall immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Laws and Regulations.

10.3 Where required under Data Protection Laws and Regulations, Braze shall notify Customer if Braze is no longer able to comply with its Processing obligations under such Data Protection Laws and Regulations. Customer agrees to exercise any resulting remediation rights under Data Protection Laws and Regulations acting in good faith and in a proportionate manner, and where appropriate, taking into account Braze's expertise.

11. AUDIT RIGHT

Braze shall allow for and contribute to audits and inspections ("Audits"), not more than once per year. Braze's contribution shall consist of Braze's reasonable cooperation and making relevant Braze employees available to Customer. Such Audit may be conducted by Customer or Customer's independent, third-party auditor that is not a competitor of Braze and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement, at Customer's own cost:

(i) by Braze providing information regarding Braze's processing activities in the form of a copy of Braze's then most recent third-party audit or certification set forth in the Security, Privacy and Architecture Datasheet, as applicable, that Braze makes available to its customers generally and through its Documentation;

(ii) to the extent required by Data Protection Laws and Regulations, by Braze allowing Customer to perform an On-Site Audit. "**On-site Audits**" shall be performed as follows: (a) an Audit of facilities operated by Braze, carried out during normal business hours, (b) such Audit shall not exceed one (1) business day; (c) Customer will provide Braze with at least three-weeks' written notice prior to such Audit, (d) before the commencement of any such Audit, Customer and Braze shall mutually agree upon the scope, cost and timing of the Audit; (e) Customer shall promptly notify Braze with information regarding any non-compliance discovered during the course of an Audit; and (f) Customer may perform an On-site Audit up to once per year.

12. CCPA PROVISIONS

The following shall apply for Customers subject to the CCPA: (i) Customer shall disclose Personal Information only for the limited and specified purposes described in Section 2, (ii) Braze will Process Personal Information with the same level of privacy protection as is required by the CCPA, (iii) Customer's rights to take reasonable and appropriate steps to help to ensure that Braze uses Personal Information transferred in a manner consistent with the Customer's obligations under the CCPA and to take, upon notice, reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, shall be exercised pursuant to Sections 10 Cooperation and 11 Audit Right and (iv) except for the limited purposes permitted by the CCPA, Braze will not combine Personal Information received from, or on behalf of, Customer with other Personal Information it receives from, or on behalf of, another party, or Personal Information that Braze has received from its own interactions with Consumers. Braze certifies that it understands the restrictions set forth in this DPA and will comply with them.

13. UK AND EU TRANSFER MECHANISM(S) FOR DATA TRANSFERS

The following provisions apply solely where Customer or an Authorized Affiliate is subject to the Data Protection Laws and Regulations of the United Kingdom ("UK") or the European Union ("EU"). As of the Effective Date of this DPA, with regard to any transfers of Personal Data under this DPA from the EU, or the UK to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of the foregoing territories, Braze makes available the following transfer mechanism(s) which shall apply, in the order of precedence as set out below, if applicable:

13.1 Any valid transfer mechanism pursuant to applicable EU and/or UK Data Protection Laws and Regulations (excluding the SCCs and the UK Addendum), to which Braze would subscribe, certify or participate in.

13.2 Standard contractual clauses, being either the SCCs and/or the UK Addendum, when they are an available and a valid transfer mechanism under applicable Data Protection Laws and Regulations, and the parties acknowledge and agree that they will comply with such standard contractual clauses as set out below:

a) Signing of this DPA, an agreement referencing this DPA, or an Order Form under an agreement referencing this DPA by any party shall be treated as signing of the SCCs by such party. Customer and any applicable Authorized Affiliates are each the data exporter. The SCCs shall be deemed incorporated into this DPA. Details required under Annexes 1, 2 and 3 of the SCCs are respectively available in Schedule 1, 2 and 3 to this DPA. In the event of any conflict or inconsistency between this DPA and the SCCs the SCCs shall prevail.

b) **General**. To the extent legally permitted, a "binding decision" is a final, non-appealable decision of a court or regulator. To the extent legally permitted, any and all communications, instructions, notifications, enquiries, requests, correspondence, co-operation, and assistance intended under the SCCs or P2P SCCs (i) between Braze and Data Subjects, shall be made exclusively via Customers; and (ii) between Customer and Sub-processors, shall be made exclusively via Braze.

c) **SCCs Clause 8.3 - SCCs Copy**. On request by a Data Subject, the Customer may make available to the Data Subject a copy of the SCCs, and for the avoidance of doubt, not the entirety of this DPA. Any business secrets or other Confidential Information shall be redacted out from such copy.

d) **SCCs Clause 8.9 - Audit Rights.** Audits pursuant to Clause 8.9 of the SCCs shall be carried out in accordance with Section 11 above. In addition, in case of demonstrable indications of material non-compliance by Braze of its processing obligations under the SCCs, Customer may perform an On-site Audit ("**Compliance Audit**"), in which case any On-site Audit performed pursuant to Section 11 (ii) shall not take place any earlier than twelve months from such Compliance Audit.

e) **SCCs Clause 9 - Sub-processors.** Section 5 of this DPA represents Customer's express consent regarding existing and new Sub-processors under Clause 9(a) of the SCCs. On request by Customer, Braze shall make available to Customer a copy of the applicable P2P SCCs with applicable Sub-processor(s), and for the avoidance of doubt, not

the entirety of the DPA with such Sub-processor(s). Any business secrets or other Confidential Information shall be redacted out from such copy. Braze shall in accordance with Clause 9(d) notify the Customer of any failure by the Sub-processor to fulfil its obligations under the P2P SCCs where such a failure leads to Braze being in material breach of this DPA.

f) **SCCs Clause 14 - Transfer Impact Assessments.** Upon Customer request, Braze will make available to Customer its documented assessment of its processing of Personal Data hereunder for the purpose of Clause 14 of the SCCs.

g) **SCCs Clauses 14 (f), 16 (b) and 16 (c) - Suspension and Termination.** Without prejudice to any other rights or remedies available to either party under this DPA, where Customer exercises any of its rights to suspend the processing of Personal Data within the Braze Services or its right to terminate any applicable Order Form(s) pursuant to Clauses 14 (f), 16 (b) or16 (c):

1. Customer shall notify Braze in writing setting forth in reasonable detail the alleged or actual material noncompliance with the requirements of the SCCs ("**Compliance Situation**"); ***and***
2. if within thirty (30) days after receipt of such notice by Braze, Braze does not: (x) demonstrate that the Compliance Situation does not lead to a violation of the SCCs, or (y) make available to Customer a change in the Braze Services, or recommend a commercially reasonable change in Customer's configuration of the Braze Services, that remedies such Compliance Situation without unreasonably burdening Customer; ***then***
3. Customer may terminate the relevant Order Form(s) pursuant to the SCCs and the Termination for Cause section of the Agreement.

List of Schedules:
Schedule 1: Details of the Processing
Schedule 2: Braze Security, Privacy and Architecture Datasheet
Schedule 3: List of Sub-processors Used in Connection with the Braze Services

The parties' authorized signatories have duly executed this DPA.

CUSTOMER: _____	**BRAZE, INC.** DocuSigned by: 9E73F64FBA9D411...
Signature: _____	Signature: _____
Printed: _____	Printed: Jon Hyman
Title: _____	Title: Chief Technology Officer
Date: _____	Date: July 22, 2024 | 1:52 PM PDT

SCHEDULE 1

DETAILS OF THE PROCESSING

1. Nature and Purpose of Processing

Braze will Process Personal Data as necessary to perform the Braze Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Braze Services. The Braze Services are a Software-asa-Service platform that includes customer relationship management and marketing automation tools and enables brands to drive user engagement and retention through multi-channel campaigns.

2. Duration of Processing

Subject to Section 7 of the DPA, Braze will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

3. Categories of Data Subjects

Customer may submit the following data to the Braze Services, the extent of which is determined and controlled by Customer in its sole discretion:

(i) Personal Data of End-Users

(ii) Personal Data of prospective or former End-Users

4. Type of Personal Data

Customer may submit Personal Data to the Braze Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

(i) Email address

(ii) Device data

(iii) ID data

SCHEDULE 2

BRAZE SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET

(effective as of July 2024; subject to change without notice)

Introduction

The goal of this document is to provide high-level information to our customers regarding Braze's commitment to security and data protection.

Braze's Corporate Trust Commitment

Braze is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

1. Policy Ownership

Braze has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the Braze Security Team.

2. Braze Infrastructure

Braze customers may elect US or European hosting options.

For US-hosted customers, Braze hosts the Braze Services with Amazon Web Services in their US-East-1 region, Virginia, USA, with some S3 backup storage containers in the US-East-2 region, Ohio, USA and US-West-2 region, Oregon, USA. Some Braze Services may also be hosted on Microsoft Azure in their East US region.

For Europe-hosted customers, Braze hosts the Braze Services with Amazon Web Services in their EU-Central-1 region, Frankfurt area, Germany, with some S3 backup storage containers in EU-West-1 in Ireland.

Certain databases are managed by ObjectRocket, a Rackspace company, which provides database support services in either the US or Germany based on data center needs.

3. Third-Party Architecture

Braze may use one or more third-party content delivery networks to provide the Braze Services and to optimize content delivery via the Braze Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Braze Services, may be cached with such content delivery networks to expedite transmission. Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

4. Audits, Certifications, and Regulatory Compliance

Braze is ISO 27001 certified and SOC 2 compliant. Braze also enters into the EU Standard Contractual Clauses with its Customers that require it, self-certifies to the EU-US and Swiss-US Data Privacy Frameworks and the UK Extension to the EU-US Data Privacy Framework, and is HIPAA-compliant.

Security Controls

5. Organization Security

Braze's CTO is responsible for the overall security of the Braze Services, including oversight and accountability. Braze's contracts with third-party hosting providers such as Rackspace and Amazon Web Services include industry-standard information protection requirements.

6. Asset Classification and Logical Access Control

Braze maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by Braze.

Braze adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. For example, Customer Success Managers only have access to the regions for which they are directly responsible. Braze maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.

Access to Braze's servers is controlled via revocable SSH keys managed via configuration management and rotated at least annually. All access to Braze's servers or Customer Data is logged and can only be accessed through Braze's VPN, which uses multi-factor authentication. Database access is controlled via 32 and 64-character passwords with IP whitelisting. Braze's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

7. Personnel Security and Training

All employees at Braze sign a non-disclosure agreement when their employment begins. In addition, Braze conducts background checks of its employees as part of its onboarding process. All employees are informed of, and agree to comply with, Braze's security policies and practices as a part of their initial onboarding. All Braze employees undergo annual security and privacy training.

System administrators, developers and other users with privileged access receive special and ongoing training and are subjected to additional background screening.

8. Physical and Environmental Security

Access to Braze facilities is controlled by 24-hour security. Additionally, all Braze offices are protected by locked access and are under 24-hour video surveillance. All Braze employee workstations are encrypted and password protected, and all Braze employee user accounts require two-factor authentication.

Data centers and servers are managed and controlled by our Cloud hosting providers, Rackspace, Microsoft, and Amazon Web Services. Braze employees have no access to any of these data centers.

Details regarding the security practices and controls applicable to these facilities can be found at their websites:

AWS: https://aws.amazon.com/security/

Rackspace: http://www.rackspace.com/security/

Microsoft: https://azure.microsoft.com/en-us/overview/security/

9. Policies and Logging

The Braze Services are operated in accordance with the following procedures to enhance security:

- Dashboard User passwords are never transmitted or stored in clear text
- Braze uses industry-standard methods to determine password validity
- API key information for third-party services provided by the customer are encrypted for storage
- Braze keeps audit logs for all access to production servers
- Server access is controlled via public key access, instead of passwords, and only permitted while on VPN that requires multi-factor authentication
- Logs are stored in a secure centralized host to prevent tampering
- Braze application and ssh audit logs are stored for one year
- Passwords are not logged under any circumstances
- Access to Braze mail and document services is only allowed on approved mobile devices that have automated security policies enforced, such as encryption, autolock and passwords
- All access to customer dashboard accounts by Braze Employees must be done through an internal service that is accessible via a 3-factor VPN only
- As part of Braze's Employee Information Security Policy, employees may not store any Customer Data on removable media

10. Intrusion Detection

Braze leverages Crowdstrike, an Endpoint Detection & Response solution (EDR). This solution is designed to review and conduct signature, heuristic, and behavioral analysis, granting the ability to detect advanced threats to both on our cloud infrastructure and corporate network. Logs from this system are centrally collected for further analysis and threat detection.

Additionally, Braze may analyze data collected by Dashboard Users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Braze Services function properly.

Braze's APIs and Dashboard use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and automatically alert Braze's engineering team.

11. Security Logs

All Braze systems used in the provision of the Braze Services, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis. Braze has automated alerts and searches on these logs.

12. System Patching and Configuration Management

Braze patches its servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that we "reset" back to a known, clean state. Braze's configuration management system regularly applies patches via Linux repositories. Braze uses the Chef configuration management tool and Kubernetes to automate this entire process, and our entire infrastructure.

Braze maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

13. Vulnerability Management

Braze's infrastructure and applications are continuously scanned by a Vulnerability Management System. Alerts are monitored by our Security Team and addressed at least monthly by the Braze Vulnerability Management Team. Braze also maintains a list membership to various CVE vulnerability mailing lists. Patches and 'critical' and 'high' vulnerabilities are remediated no later than 30 days following discovery.

Braze also uses static code analysis tools during the build process (such as Brakeman and bundler-audit) to perform static security analysis.

14. Third-Party Penetration Testing

Braze undergoes a third-party penetration test of the Braze Services on an annual basis.

15. Monitoring

For technical monitoring, maintenance and support processes, Braze uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- APM performance monitoring
- Error monitoring
- Office monitoring

16. Customer Access Control

The Braze Services employ a variety of security controls. These include, but are not limited to:

- API IP Whitelisting - Defines the range of IP addresses from which a customer's Dashboard Users can access the Braze API to prevent unauthorized third parties from accessing the Braze Services.
- Dashboard Account IP Whitelisting - Defines a range of IP addresses from which a customer's Dashboard Users can access the Braze Dashboard to prevent unauthorized parties from accessing the Braze Services.
- Single-sign on with a Google Account - Braze customers can access the Braze Services by means of a Google Account, which allows customers to configure such access to require two-factor authentication.
- Single-sign on via Okta - Braze customers can access the Braze Services via Okta, which allows customers to configure access via their Okta installation.
- Mobile Authenticator - Braze customers can enable two factor authentication via Authy which allows a mobile authenticator to be required for access to the Braze Dashboard.
- Customer-Configurable Roles and Permissions - Braze customers have the option to manage their Dashboard Users through selective and granular permissioning described in our documentation at https://www.braze.com/docs/user_guide/administrative/manage_your_braze_users/user_permissions/.
- All requests on the Braze Dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Braze does not use cookies for session storage to avoid replay attacks. Sessions expire after a few hours of inactivity.
- Dashboard User passwords on the Braze Dashboard must meet minimum password length requirements. At the customer's request, Braze can add password complexity requirements, such as lowercase, uppercase, numeral, and special characters, and set a password expiration policy such that Dashboard Users must change their passwords regularly.
- Dashboard User password history of the last six passwords prevents the reuse of Dashboard User passwords.
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

- Braze's REST APIs are accessed with separate API keys, which can only be provisioned by Braze Dashboard User accounts with administrative access. API keys are granted access to specific API endpoints when created.

17. Development and Maintenance

Braze uses tools such as GitHub and Jenkins to effectively manage the development lifecycle. During testing, Braze generates sandbox accounts and fake data for testing. Braze does not use production data in sandbox accounts.

Application source control is accomplished through private GitHub repositories. Braze has controls in place to ensure that all code must be approved before being merged to Braze's main code branch; only the CTO and approved employees are granted access to promote code to production.

Braze developers receive additional security training as part of their onboarding, and undergo regular and periodic security training during the term of their employment. Braze maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

18. Malware Prevention

As a mitigating factor against malware, all Braze servers run LTS editions of Operation Systems, as well as the endpoint detection and response(EDR) service, Crowdstrike.

Braze adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Braze employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

19. Information Security Incident Management Braze maintains written and regularly-audited security incident management policies and procedures, including an Incident Response Plan to be enacted in the event of an incident.

Braze has 24x7x365 on-call incident management staff. Braze uses tools such as PagerDuty to ensure complete coverage with defined escalation policies.

20. Data Encryption

The Braze Services use industry-accepted encryption practices to protect Customer Data and communications during transmissions between a customer's network and the Braze Services, including 256-bit TLS Certificates and 4096-bit RSA public keys at a minimum.

Braze audits the TLS ciphers used in connection with the provision of the Braze Services with third-party security auditors to ensure that anonymous or weak ciphers are not used. These audits also confirm that the Braze Services do not allow client renegotiation, support downgrade attack protection and forward secrecy.

Data shipped to Amazon Web Services is encrypted in transit and at-rest using AES-256 encryption via Amazon's managed encryption key process. Data shipped to Rackspace is encrypted in transit and at-rest using AES-256 encryption via Rackspace's managed encryption key process.

Where use of the Braze Services requires a customer to provide access to third party services (for example, AWS S3 credentials for data exports), Braze performs additional encryption of that information.

21. Return and Deletion of Customer Data

The Braze Services allow import, export, and deletion of Customer Data by authorized Dashboard Users at all times during the term of a customer's subscription. Following termination or expiration of the Braze Services, Braze shall securely overwrite or delete Customer Data within 60 days following any such termination in Braze's production instance, and in accordance with the Agreement, applicable laws and the Documentation.

22. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Braze Services is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

23. Business Continuity Management and Disaster Recovery

Braze has a written Business Continuity and Disaster Recovery Plan, which is tested annually. Braze tests database backups and failovers as part of our Business Continuity Plan. Backups are encrypted and stored in Amazon Web Services- and Rackspaceprovided backup services.

24. Mobile Device Management Policies

Braze uses Mobile Device Management ("MDM") platforms to control and secure access to Braze resources on mobile devices such as phones, tablets, and laptops. Braze uses Google for its phone and tablet MDM policy, and enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe. Braze uses JAMF for laptop and desktop management to enforce common security settings, including but not limited to, hard disk encryption, security patches, and remote location and remote wipe capabilities.

25. Blocking Third Party Access

The Braze Services have not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access Customer Data. We do not voluntarily provide any government or other third party with encryption keys, or any other way to break our encryption.

26. Forensics

Braze uses the CrowdStrike EDR solution to investigate and respond to security incidents involving Braze user endpoints. The solution allows the Security Team to collect valuable forensic information from affected systems to better understand what occurred in the system and to take steps to contain and/or remediate the threat.

For forensic disk acquisition, Braze uses Cellebrite's Digital Collector tool to collect a forensically-sound bit-by-bit copy of a storage device from a compromised asset.

To analyze forensic disk images, Braze uses Cellebrite Inspector. This tool allows the Security Team to recover deleted or hidden data and establish a complete picture of activity that occurred on a compromised asset.

27. Contacts

Braze's Security Team can be reached by emailing security@braze.com.

SCHEDULE 3
LIST OF SUB-PROCESSORS
USED IN CONNECTION WITH THE BRAZE SERVICES

This Schedule describes the Sub-processors material to Braze's provision of the Braze Services.
(effective as of the Effective Date; subject to change)

Last Modified: May 2024

Braze, Inc. ("Braze") uses certain Sub-processors, whether third parties or subsidiaries of Braze (as described below) who process Personal Data on behalf of Braze and in connection with Braze's provision of the Braze Services to its customers. Capitalized terms used herein without definition are used as defined in the Agreement.

Sub-processors are subject to written agreements that contain confidentiality and security commitments, in substance the same as those in the DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. Braze remains responsible for the acts and omissions of its Sub-processors pursuant to the DPA.

What follows is the list of Sub-processors that Braze uses in its provision of the Braze Services. Depending upon a Customer's use of the Braze Services e.g. geographical location of the Customer, not all Sub-Processors will be needed to deliver the Braze Services. Sub-processors receive, store, structure, categorize, analyze, handle, process and send Personal Data, as applicable and in accordance with the Agreement. The Sub-processors Process Personal Data until the earlier of (i) the completion of the Processing provided by such Sub-processor, and (ii) the duration of the Agreement, subject to the terms of the Agreement and the Documentation.

Customers shall provide appropriate contact details through Braze's applicable subscription mechanism in order to receive notice of new Sub-processors. More information on Sub-processors, including their contact details and available notification mechanisms, can be found at http://braze.com/subprocessors.

Storage and Analytics Services

Entity Name	Services Provided	Location of Processing
Amazon Web Services, Inc.	Third-party hosting provider.	United States
Amazon Web Services Germany GmbH	Third-party hosting provider.	European Union
Amazon Web Services Ireland Ltd.	Third-party hosting provider.	European Union
Rackspace US, Inc.	Provides ObjectRocket, a managed database service provider that hosts and stores End User profiles.	United States, European Union
Snowflake Computing Inc.	A managed database provider that hosts Personal Data to enable analytics reporting.	United States, European Union
Clickhouse, Inc.	A managed database provider that hosts Personal Data to enable analytics reporting.	United States, European Union
Google LLC	Provides Looker, a business intelligence software used to analyze Customer Data to identify trends and business outcomes.	United States
dbt Labs, Inc.	A tool that enables transformation, modelling and testing of data in the data warehouse for analytics purposes.	United States

SMS/MMS and Email Delivery Services

Entity Name	Services Provided	Location of Processing
MessageBird USA, Inc.	Provides Sparkpost, an email delivery provider.	European Union, United States

Twilio Inc.	Email delivery provider (via SendGrid) and SMS/MMS delivery provider.	United States
Infobip Inc.	SMS/MMS delivery provider.	United States, European Union

Content Delivery Networks

The Braze Services use content delivery networks ("CDNs") to provide the Braze Services, for security purposes, to support Dashboard User authentication, and to optimize content delivery. CDNs are commonly used systems of distributed services that deliver content based on the geographic location of the individual accessing the content and the origin of the content provider. Content items that are transmitted via CDNs tend to be high content data (videos, images) that have been uploaded to the Braze Services and may be cached by a CDN to expedite delivery of such content to End Users.

Entity Name	Services Provided	Location of Processing
Amazon Web Services, Inc.	Content delivery network used by Braze to optimize content delivery.	Global
Fastly, Inc.	Content delivery network used by Braze for the routing of encrypted API calls to Braze servers, and to optimize content delivery.	Global (https://www.fastly.com/network-map)
Cloudflare, Inc.	Content delivery network used by Braze for the routing of encrypted API calls to Braze servers, and to optimize content delivery.	Global (https://www.cloudflare.com/network/)

Monitoring, Diagnostic, and Support Services

The Braze Services use third-party vendors in connection with the delivery of the Braze Services. These third parties may process Personal Data in connection with monitoring, troubleshooting, log management and the provision of support or training to customers.

Entity Name	Services Provided	Location of Processing
DataDog, Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. Braze may provide End User metadata, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Braze Services.	United States
Functional Software, Inc. dba Sentry	Error tracking platform used by the Braze Services to capture errors that occur in the Braze Services. Braze may provide End User metadata such as user identifiers to Sentry for support and application troubleshooting and improving performance.	United States

Customer Success, Business Operations and Technical and Engineering Support Services

Entity Name	Services Provided	Location of Processing
Braze Australia Pty Ltd.	Subsidiaries providing customer success, business operations and support services.	Australia
Braze Canada Ltd.		Canada
Braze France SAS		France
Braze Germany GmbH		Germany
Braze Global Sales Ireland Limited		Ireland
Braze Ireland Procurement Limited		Ireland & Romania
Braze KK		Japan
Braze Limited		United Kingdom
Braze Pte Ltd.		Singapore
PT Braze Indonesia Technology		Indonesia