DATA PROCESSING ADDENDUM

Last Updated: June 16, 2025

This Data Processing Addendum (including its Exhibits) ("**DPA**") forms part of and is subject to the terms and conditions of the Back4app Terms of Service (the "**Agreement**") by and between you ("**Customer**") and Back4app Inc. ("**Back4app**"). All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its Exhibits conflicts with the Agreement, this DPA shall control.

1. **Definitions.** For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

1.1. "**Customer Personal Data**" means User Content that is Personal Data about end users of Customer's Application Processed by Back4app on behalf of Customer under the Agreement.

1.2. "**Data Protection Laws**" means the privacy and data protection laws, rules and regulations applicable to a party's Processing of Customer Personal Data under the Agreement. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; other comprehensive US state privacy laws; the Swiss Federal Act on Data Protection; and the United Kingdom General Data Protection Regulation; the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

1.3. "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws.

1.4. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated 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.

1.5. "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Back4app.

1.6. "**Services**" means the services that Back4app performs under the Agreement.

1.7. "**Subprocessor**" means a vendor that Back4app has engaged to Process Customer Personal Data.

2. **Processing Terms for Customer Personal Data.**

2.1. Documented Instructions. Back4app shall Process Customer Personal Data to provide the Services in accordance with the Agreement, this DPA, and any instructions agreed upon by the parties. If applicable law requires that Back4app Process Customer Personal Data for other purposes, Back4app shall inform Customer of that legal requirement before engaging in such Processing, unless that law prohibits such information on important grounds of public interest.

2.2. Authorization to Use Subprocessors. Customer authorizes Back4app to engage Subprocessors. Customer acknowledges that Subprocessors may further engage vendors.

2.3. Back4app and Subprocessor Compliance. Back4app shall (i) enter into a written agreement with Subprocessors that imposes data protection requirements for Customer Personal Data on such Subprocessors that are consistent with this DPA; and (ii) remain responsible to Customer for the Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data.

2.4. Right to Object to Subprocessors. Back4app shall notify Customer prior to engaging any new Subprocessors by updating its list of Subprocessors found at https://www.back4app.com/product/parse-gdpr/gdpr-third-parties, and allow Customer ten (10) days to object after the list has been updated. It is Customer's responsibility to check this website for updates. If Customer has legitimate objections to the appointment of any new Subprocessor that are raised in accordance with this Section 2.4, the parties shall work together in good faith to resolve the grounds for the objection.

2.5. Confidentiality. Any person authorized to Process Customer Personal Data shall be subject to a duty of confidentiality, contractually agree to maintain the confidentiality of such information, or be under an appropriate statutory obligation of confidentiality.

2.6. Personal Data Inquiries and Requests. Back4app shall provide reasonable assistance to Customer as required by applicable Data Protection Laws in response to any requests from individuals exercising their rights in Customer Personal Data granted to them under applicable Data Protection Laws.

2.7. Data Protection Assessment, Data Protection Impact Assessment, and Prior Consultation. Back4app shall provide reasonable assistance and information to Customer as required by applicable Data Protection Laws where, in Customer's judgement, the type of Processing performed by Back4app requires a data protection assessment, data protection impact assessment, and/or prior consultation with the relevant data protection authorities. Customer shall reimburse Back4app for all non-negligible costs Back4app incurs in performing its obligations under this Section.

2.8. Demonstrable Compliance. Back4app shall provide information reasonably necessary to demonstrate compliance with this DPA as required by applicable Data Protection Laws upon Customer's reasonable request.

2.9. California Specific Terms. To the extent that Back4app's Processing of Customer Personal Data is subject to the CCPA, this Section also applies. Customer discloses or otherwise makes available Customer Personal Data to Back4app for the limited and specific purpose of Back4app providing the Services to Customer in accordance with the Agreement and this DPA. Back4app shall: (i) comply with its applicable obligations under the CCPA; (ii) provide the same level of protection as required under the CCPA; (iii) notify Customer if it can no longer meet its obligations under the CCPA; (iv) not "sell" or "share" (as such terms are defined by the CCPA) Customer Personal Data; (v) not retain, use, or disclose Customer Personal Data for any purpose (including any commercial purpose) other than to provide the Services under the Agreement or as otherwise permitted under the CCPA; (vi) not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Back4app; and (vii) unless otherwise permitted by the CCPA, not combine Customer Personal Data with Personal Data that Back4app (a) receives from, or on behalf of, another person, or (b) collects from its own, independent consumer interaction. Back4app will permit Customer, upon reasonable request, to take reasonable and appropriate steps to ensure that Back4app Processes Customer Personal Data that is subject to this Section 2.9 in a manner consistent with the obligations of a "business" under the CCPA by requesting that Back4app attest to its compliance with this Section 2.9. Following any such request, Back4app will promptly provide that attestation or notice about why it cannot provide it. If Customer reasonably believes that Back4app is engaged in unauthorized Processing of Customer Personal Data that is subject to this Section 2.9, Customer will notify Back4app of such belief, and the parties will work together in good faith to remediate the allegedly violative Processing activities, if necessary.

2.10. Security & Fraud Prevention. Where permitted by Data Protection Laws, Back4app may Process Customer Personal Data: (i) to prevent, detect, or investigate Security Incidents; or (ii) to protect against malicious, deceptive, fraudulent or illegal activity.

2.11. Aggregation and De-Identification. Back4app may: (i) compile aggregated and/or de-identified information in connection with providing the Services provided that such information cannot reasonably be used to identify Customer or any data subject to whom Customer Personal Data relates ("**Aggregated and/or De-Identified Data**"); and (ii) use Aggregated and/or De-Identified Data for its lawful business purposes.

3. Information Security Program. Back4app shall implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data.

4. Security Incidents. Upon becoming aware of a Security Incident, Back4app shall provide written notice without undue delay and within the time frame required under applicable Data Protection Laws to Back4app's primary contact at Customer's organization, or the email address that is listed as Customer's account owner or administrator. Where possible, such notice will include all available details required under applicable Data Protection Laws for Customer to comply with its own notification obligations to government authorities and/or individuals affected by the Security Incident.

5. Cross-Border Transfers of Customer Personal Data.

5.1. Cross-Border Transfers of Customer Personal Data. Customer authorizes Back4app and its Subprocessors to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to jurisdictions outside those regions.

5.2. EEA, Swiss, and UK Standard Contractual Clauses. If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Back4app in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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 ("**Standard Contractual Clauses**") as supplemented by **Exhibit A** attached hereto, the terms of which are incorporated herein by reference. Where the Standard Contractual Clauses are applicable and Customer acts as a controller of Customer Personal Data with Back4app acting as a processor of Customer Personal Data, each party shall comply with its obligations under Module Two of the Standard Contractual Clauses. Where the Standard Contractual Clauses are applicable and Customer acts as a processor of Customer Personal Data with Back4app acting as a (sub)processor of Customer Personal Data, each party shall comply with its obligations under Module Three of the Standard Contractual Clauses. Each party's execution of this Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

6. **Audits and Assessments.**

6.1. Back4app Audit. Back4app shall conduct an internal audit to verify the adequacy of its Processing of Customer Personal Data in accordance with this Addendum. This audit: (i) will be performed at least annually; (ii) will be performed against an industry recognized framework; (iii) will be performed by Back4app; and (iv) will result in the generation of an executive level summary of the audit report affirming that Back4app's security controls are consistent with industry standards ("**Report**").

6.2. Audit Results. Upon Customer's written request, Back4app shall provide Customer with a copy of its most recent Report so that Customer can reasonably verify Back4app's compliance with the security obligations under this Addendum. Any provision of such Report to Customer shall be subject to Back4app's security and confidentiality terms and guidelines.

6.3. Follow Up Audit or Assessment. To the extent that Customer can demonstrate that the Report does not provide sufficient information to verify Back4app's compliance with its security obligations set forth herein, and applicable Data Protection Laws afford Customer an audit or assessment right, Customer (or its appointed representative) may carry out an audit or assessment of Back4app's policies, procedures, and records with respect to the Processing of Customer Personal Data. Any audit or assessment must be: (i) conducted during Back4app's regular business hours; (ii) with reasonable advance notice to Back4app; (iii) carried out in a manner that prevents unnecessary disruption to Back4app's operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit or assessment will be limited to once per year, unless an audit or assessment is carried out at the direction of a government authority with jurisdiction over the Processing of Customer Personal Data.

6.4. Where Data Protection Laws afford Customer an audit or assessment right, Customer (or its appointed representative) may carry out an audit or assessment of Back4app's policies, procedures, and records relevant to the Processing of Customer Personal Data. Any audit or assessment must be: (i) conducted during Back4app's regular business hours; (ii) with reasonable advance notice to Back4app of at least 45 days; (iii) carried out in a manner that prevents unnecessary disruption to Back4app's operations; and (iv) subject to reasonable confidentiality procedures and execution of Back4app's non-disclosure agreement. In addition, any audit or assessment shall be limited to once per year, unless an audit or assessment is carried out at the direction of a government authority with jurisdiction over the Processing of Customer Personal Data. (v) Customer shall be solely responsible for any costs arising from such audit (including any costs incurred by Back4app).

7. **Customer Personal Data Deletion.** At the expiry or termination of the Agreement, Back4app shall delete all Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Back4app's data retention schedule), except where Back4app is required to retain copies under applicable laws, in which case Back4app will isolate and restrict that Customer Personal Data from any further Processing except to the extent required by applicable laws.

8. **Customer's Obligations.** Customer represents and warrants that: (i) it has complied and will comply with Data Protection Laws; (ii) it has obtained and will obtain and continue to have, during the term, all necessary rights, lawful bases, authorizations, consents, and licenses for the Processing of Customer Personal Data as contemplated by the Agreement; and (iii) Back4app's Processing of Customer Personal Data in accordance with the Agreement will not violate Data Protection Laws or cause a breach of any agreement or obligations between Customer and any third party.

9. **Processing Details.**

9.1. Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

9.2. Duration. The Processing will continue until the expiration or termination of the Agreement.

9.3. Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement.

9.4. Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Back4app is the performance of the Services.

9.5. Types of Customer Personal Data. Customer Personal Data that is Processed pursuant to the Agreement.

EXHIBIT A TO THE DATA PROCESSING ADDENDUM

This Exhibit A forms part of the DPA and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Exhibit A have the meaning set forth in the DPA.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III)."; (iii) the optional text in Clause 7 is deleted; (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must notify data exporter of any new subprocessors in accordance with Section 2.4 of the DPA; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

   A. List of Parties

   Data Exporter: Customer.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Controller (Module Two); Processor (Module Three).

   Data Importer: Back4app.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Processor.

   B. Description of the Transfer:

   Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data is transferred under the Clauses including, but not limited to, end users of data exporter's Application.

   Categories of personal data transferred: The categories of personal data transferred under the Clauses is determined and controlled by data importer in its sole discretion. This personal data, may include, but is not limited to personal data such as name, email address, phone number, and Application usage data.

   Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: To the parties' knowledge, no sensitive data is transferred.

   The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the Services, or as otherwise agreed upon by the parties.

   Nature of the processing: The Services.

   Purpose(s) of the data transfer and further processing: The Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For the subject matter, nature, and duration as identified above.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

D. Clarifying Terms: The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 6 of the DPA; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Clauses will be limited to the termination of the Clauses; (v) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Clauses; (vi) the information required under Clause 15.1(c) of the Clauses will be provided upon data exporter's written request; and (vii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Clauses without regard for any limitation of liability set forth in the Agreement.

3. **Annex II.** Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain technical and organisational measures designed to protect personal data in accordance with the DPA. Such measures shall include:

- Measures of pseudonymisation and encryption of personal data (as appropriate);
- Measures designed to ensure ongoing confidentiality, integrity, availability and resilience of the Services that process personal data;
- Measures designed to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in an effort to ensure the security of the processing of personal data;
- Measures for user identification and authorization;
- Measures designed to protect personal data during transmission;
- Measures designed to protect personal data during storage;
- Measures designed to ensure the physical security of locations at which personal data are processed (as appropriate);
- Measures for events logging (as appropriate);
- Measures regarding system configuration, including default configuration (as appropriate);
- Measures regarding internal IT and IT security governance and management;
- Measures regarding certification/assurance of the Services (as appropriate);
- Measures designed to ensure data minimization for personal data (as appropriate);
- Measures designed to ensure data quality (as appropriate, and to the extent within data importer's control);
- Measures for data retention of personal data;
- Measures for accountability regarding the processing of personal data; and
- Measures for allowing data portability and ensuring erasure of personal data.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

4. **Annex III.** A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the DPA. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the DPA.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The parties agree that Importer may end the UK Addendum as set out in Section 19.