Back4App, Inc. Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is made and entered into by and between Back4App, Inc. ("**Back4App**") and the customer specified in the table below ("**Customer**").

Back4App, Inc. **By:** Alex Kusmenkovsky **Name: Alex Kusmenkovsky** **Title: Data Protection Officer** **Signature Date: May,17th 2018** **Address:** 440 N Wolf Road Sunnyvale, CA, 94085 USA **Attention:** General Counsel	**Customer Name (Required):** _____ (full legal entity name) **By (Signature Required):** _____ **Your Printed Name (Required):** _____ **Your Title (Optional):** _____ **Signature Date (Required):** _____ **Customer Address (Required):** _____ _____ **Attention:** _____

This Addendum includes the Data Processing Terms and the attached Annexes A–B (including Appendices) and supplements Back4App's Terms of Service available at https://www.back4app.com/terms-of-service.pdf (as updated from time to time) (the "**Agreement**") between Customer and Back4App (collectively, the "**Parties**"). This Addendum will be effective as of the day Back4App receives a complete and executed Addendum from Customer in accordance with the instructions under Sections 1 and 2 below (the "**Addendum Effective Date**").

1. **Instructions.** This Addendum (including the Standard Contractual Clauses in Annex B) has been pre-signed on behalf of Back4App, Inc. To enter this Addendum, Customer must:
   - **a)** Complete the table above by signing and providing the Customer's full legal entity name, address and signatory information; and
   - **b)** Submit the completed and signed Addendum to Back4App via email to gdpr@back4app.com.
2. **Effectiveness.**
   - **a)** This Addendum will be effective only if it is executed and submitted to Back4App in accordance with Section 1 above and this Section 2, and all items identified as "Required" in the table are completed accurately and in full. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void.
   - **b)** Customer signatory represents to Back4App that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g., is not a minor).
   - **c)** This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of the Addendum.
3. **Subject Matter and Duration.**
   - **a) Scope and Rules.** The Addendum applies when Customer Data is Processed by Back4App. In this context, Customer may act as a "Controller or "Processor", and Back4App may act as "Processor" or "Sub-Processor" with respect to Customer Data.
   - **b) Subject Matter.** This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Data under the terms of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings

given to them in the Agreement. If and to the extent language in this Addendum or any of its Annexes conflicts with the Agreement, this Addendum shall control.

c) **Duration and Survival.** This Addendum will become legally binding upon the Addendum Effective Date. Back4App will Process Customer Data until the relationship terminates as specified in the Agreement. Back4App's obligations and Customer's rights under this Addendum will continue in effect so long as Back4App Processes Customer Data.

4. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules and regulations to which the Customer Data are subject. "Applicable Data Protections Law(s)" shall include, but not be limited to, the EU General Data Protection Regulation 2016/679 ("**GDPR**").

b) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Data.

c) "**Customer Data**" shall: (i) have the meaning assigned to the terms "Personal Data" or "personal information" under Applicable Data Protection Law(s) and (ii) mean Personal Data or personal information pertaining to Customer's users or employees located in the European Economic Area Processed by Back4App. The Customer Data and the specific purposes of Processing the Customer Data are detailed in **Annex A** attached hereto, as required by the GDPR.

d) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Data or on sets of Customer 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.

e) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Customer Data on behalf of Customer subject to this Addendum.

f) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data Processed by Back4App.

g) "**Services**" means any and all services that Back4App performs under the Agreement or any Statement of Work that Process Customer Data.

h) "**Third Party(ies)**" means Back4App's authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Customer Data.

5. Data Use and Processing.

a) Compliance with Laws. Customer Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

b) Documented Instructions. Back4App and its Third Parties will process Customer Data in accordance with Customer's instructions. The Parties agree that this Addendum is Customer's complete and final instructions to Back4App in relation to Processing of Customer Data. Processing outside the scope of this Addendum (if any) will require prior written agreement between Customer and Back4App regarding additional instructions for Processing, including agreement on any additional fees Customer will pay Back4App for carrying out such instructions. Customer may terminate this Addendum if Back4App declines to follow instructions requested by Customer that are outside the scope of this Addendum. Back4App will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Data in a manner that is inconsistent with Customer's instructions.

c) Authorization to Use Third Parties. To the extent necessary to fulfill Back4App's contractual obligations under the Agreement or any Statement of Work, or to provide certain Services on its behalf, such as providing support services, Customer hereby authorizes (i) Back4App to engage Third Parties and (ii) Third Parties to engage sub-processors. Any Third Party Processing of, or access to, Customer Data shall be consistent with Customer's documented instructions and comply with all Applicable Data Protection Law(s).

d) Back4App and Third Party Compliance. Back4App agrees to (i) enter into written agreements with Third Parties regarding such Third Parties' Processing of, or access to, Customer Data that imposes on such Third Parties (and their sub-processors) data protection and security requirements for Customer Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Back4App's Third Parties' (and their sub-processors, if applicable) failure to perform their obligations with respect to the Processing of Customer Data.

e) Right to Object to Third Parties. Prior to engaging any new Third Parties that may Process or access Customer Data, Back4App will notify Customer by updating its list of Third Parties found at https://www.back4app.com/product/parse-gdpr/thrid-parties at least fifteen (15) days before it authorizes and permits such Third Parties to Process or access Customer Data. It is Customer's responsibility to check this website for updates. If Customer has legitimate objections to the appointment of any new Third Party, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Customer may terminate the part of the Service performed under the Agreement that cannot be performed by Back4App without use of the objectionable Third Party.

f) Confidentiality. Any person or Third Party authorized to Process Customer Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

g) Data Inquiries and Requests. Back4App agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising the rights granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). At Customer's request, Back4App agrees to assist Customer in answering or complying with any Privacy Request in so far as it is possible. Customer shall be responsible for any costs arising from Back4App's provision of such assistance.

h) Data Protection Impact Assessment and Prior Consultation. Back4App agrees to provide reasonable assistance at Customer's sole expense to Customer where, in Customer's judgement, the type of Processing performed by Back4App is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Company Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

i) Demonstrable Compliance. Back4App agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide any necessary records to Customer to demonstrate compliance upon reasonable request.

6. Cross-Border Transfers of Data.

a) Cross-Border Transfers of Data. Customer authorizes Back4App and its Third Parties to transfer Customer Data across international borders, including from the European Economic Area to the United States. Any cross-border transfer of Customer Data must be supported by an approved adequacy mechanism.

b) Standard Contractual Clauses. Back4App and Customer will use the Standard Contractual Clauses in **Annex B** as the adequacy mechanism supporting the transfer and Processing of Customer Data.

7. Information Security Program.

a) Taking into account the state of the art, the costs of implementation and the nature, scope,

context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Back4App shall implement and maintain appropriate technical and organizational measures in such a manner that its Processing of Data will meet the requirements of Applicable Data Protection Law(s), ensure the protection of the rights of the data subjects, and ensure a level of security appropriate to the risk (an "**Information Security Program**").

8. Security Incidents.

a) Security Incident Procedure. Upon becoming aware of a Security Incident, Back4App shall without undue delay inform Customer and provide written details of the Security Incident reasonably required to fulfill Customer's Security Incident reporting obligations under Applicable Data Protection Law(s). Where possible, such details shall include, the nature of the Security Incident, the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Data records concerned, the likely consequences of the Security Incident, and the measures taken or proposed to be taken to mitigate the Security Incident's possible adverse effects.

9. Audits.

a) Back4App Audit. The Parties acknowledge that Back4App will conduct an internal audit to verify the adequacy of its Processing of Customer 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**").

b) Audit Results. At Customer's written request, Back4App will provide Customer with a copy of its Report so that Customer can reasonably verify Back4App's compliance with the security and audit obligations under this Addendum. Any provision of such Report to Customer shall be subject to Back4App's security and confidentiality terms and guidelines.

c) Customer Audit. In the event that Customer demonstrates the Report does not provide sufficient information, Customer and Back4App may designate an independent auditor to, no more than once annually, carry out an inspection of Back4App's operations and facilities with respect to the Processing of Customer Data. Customer must provide Back4App forty-five (45) days written notice of such intention to audit, conduct its audit during normal business hours, and take reasonable measures necessary to prevent unnecessary disruption to Back4App's operations. Any such audit shall be subject to Back4App's security and confidentiality terms and guidelines. Customer shall be solely responsible for any costs arising from such audit (including any costs incurred by Back4App).

d) Third Parties. In the event that Customer conducts an audit through a third party independent auditor, such third tarty shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Back4App's and Back4App's customers' confidential and proprietary information.

e) Audit Results. After conducting an audit, Customer shall notify Back4App of the manner in which Back4App does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein.

10. Data Deletion.

a) Data Deletion. Upon termination of the Agreement, Back4App will delete all Customer Data to Customer, except where Back4App is required to retain copies under applicable laws, in which case Back4App will isolate and protect that Customer Data from any further Processing except to the extent required by applicable laws.

Annex A

1.1 Subject Matter of Processing	The Processing will involve Processing for: Compute, Storage and Content Delivery on the Back4App Network.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	Includes the following: • Data exporter's customers and end-users • Prospects, customers, business partners and vendors of Customer (who are natural persons) • Employees or contact persons of Customer's prospects, customers, business partners and vendors • Employees, agents, advisors, freelancers of Customer (who are natural persons) • Customer's users authorized by Customer to use the Services
1.4 Nature and Purpose of Processing	Includes the following: Back4App will process Customer Data in accordance with Customer's instructions. The parties agree that this Addendum is Customer's complete and final instructions to Back4App in relation to processing of Customer Data. Processing outside the scope of this Addendum (if any) will require prior written agreement between Back4App and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Back4App for carrying out such instructions. Customer may terminate this Addendum if Back4App declines to follow instructions requested by Customer that are outside the scope of this Addendum.
1.5 Types of Personal Information	Includes the following: The personal data relating to individuals which is uploaded onto the Back4App Services by the data exporter.

Annex B

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The entity identified as "**Customer**" in the Addendum
(the "**data exporter**")

And

Back4App, Inc.
440 N Wolf Road, Sunnyvale, CA, 94085, USA

(the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of

processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is: Customer.

Data importer
The data importer is: Back4App, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:

- Data exporter's customers and end-users
- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's users authorized by data exporter to use the Back4App Services

Categories of data
The personal data transferred concern the following categories of data:
Personal data relating to individuals which is uploaded onto the Back4App Services by the data exporter.
Data can include, but not limited to:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
Data exporter may submit special categories of data to the Services, and which is for the sake of clarity personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations
The personal data transferred will be subject to the following basic processing activities:
The objective of processing of personal data by data importer is the performance of the Services pursuant to the Agreement and any Statements of Work.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of this Addendum, the parties will be deemed to have signed Appendix 2.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Data Processing Addendum. Data importer will not materially decrease the overall security of the Services during the term of the Agreement.