ONESIGNAL DATA PROCESSING ADDENDUM

This OneSignal Data Processing Addendum (the “DPA”) is incorporated into the agreement under which OneSignal has agreed to provide customer messaging services to Customer. This DPA applies to and takes precedence over that agreement and any associated contractual document between the parties, such as an order form, or statement of work (collectively, the “Agreement”), to the extent of any conflict. OneSignal may reasonably revise and update this DPA from time to time when required by Applicable Law (as defined below). All changes are effective within 30 days after being posted online and will apply to all access to and use of the Services (as defined below) thereafter.

Definitions

1. In this DPA:
   - “Applicable Law” means the following, as applicable: (i) GDPR; (ii) all national implementations of (i); (iii) the Swiss Federal Act on Data Protection, as revised, and its corresponding ordinances; (iv) in respect of the United Kingdom, the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, and the Data Protection Act 2018 (the "UK GDPR") and any applicable national legislation that replaces or converts the GDPR in domestic law or that relates to data and privacy and is enacted as a consequence of the United Kingdom leaving the European Union; in each case, as may be amended, superseded or replaced from time to time; and (v) any other laws, rules, and regulations applicable to the European Economic Area, the United Kingdom or Switzerland relating to the processing, privacy, or use of personal data. For the avoidance of doubt, each partyis only responsible for the Applicable Law applicable to it.
   - "GDPR" means the General Data Protection 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.
   - “Personal Data” means any information relating to an identified or identifiable individual, within the meaning of the GDPR or equivalent under Applicable Law, in respect of which Customer is the data controller and OneSignal is the data processor on Customer’s behalf.
   - “Personal Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, and a personal data breach (or equivalent term) as defined under Applicable Law.
   - “Process” and “Processing” mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "SCCs" means: (i) where GDPR or the Swiss Federal Act on Data Protection applies, the standard contractual clauses for data controller to data processor transfers attached hereto as Annex A ("EU SCCs"); and (ii) where the UK GDPR applies, the EU SCCs, and the International Data Transfer Addendum to the EU SCCs ("UK SCCs").
- “Subprocessor” means any OneSignal affiliate or subcontractor engaged by OneSignal for the Processing of Personal Data.

Scope

2. This DPA applies to the Personal Data that OneSignal receives from Customer, or otherwise Processes for or on behalf of Customer, through the services that OneSignal provides under the Agreement for which Customer is an administrator (the “Services”).

Customer Responsibilities

3. Customer acknowledges that it is the administrator for the account(s) specified in the Agreement and, therefore, is considered to be a “controller” under the GDPR or Applicable Law and that OneSignal is a “processor.”
4. Customer will comply with all Applicable Laws. Customer will establish legal bases for its and OneSignal’s Processing of Personal Data and obtain any consents from data subjects required under Applicable Laws for OneSignal to provide the Services, in each case prior to any Processing by OneSignal and its Subprocessors. Customer will provide all disclosures and notices to data subjects as required by Applicable Law for it to share Personal Data with OneSignal and its Subprocessors and for OneSignal and its Subprocessors to Process Personal Data in accordance with this DPA, in each case prior to any Processing by OneSignal and its Subprocessors. Customer will not share any sensitive information or special categories of data with OneSignal.

Customer Instructions to OneSignal

5. OneSignal will Process the Personal Data only as described under the Agreement, unless obligated to do otherwise by Applicable Law. In such case, OneSignal shall inform Customer of that legal requirement before Processing, unless that legal requirement prohibits providing such information on important grounds of public interest. For the avoidance of doubt, the details of the Processing are as set forth in Annex I to the attached Standard Contractual Clauses:

6. The Agreement and this DPA (each as may be amended from time to time), along with Customer's configuration of any settings or options in the Services (as Customer may be able to modify from time to time, depending on the Services), constitute Customer's complete and final instructions to OneSignal regarding the Processing of Personal Data, including for purposes of the SCCs. Customer shall not instruct OneSignal to Process Personal Data in violation of Applicable Law, and OneSignal shall promptly inform Customer if, in OneSignal's opinion, an instruction from Customer infringes Applicable Law.

Subprocessors

7. OneSignal may subcontract the collection or other Processing of Personal Data only in compliance with Applicable Law and any additional conditions for subcontracting set forth in the Agreement. OneSignal's current list of Subprocessors are set forth on this web page and are hereby approved by Customer: https://media.onesignal.com/cms/Files/Annex_III_Sub-processors.pdf. Prior to a Subprocessor's Processing of Personal Data, OneSignal will impose contractual obligations on the Subprocessor as required by Applicable Law. OneSignall will notify Customer of new Subprocessors at least 10 days in advance by updating its Subprocessor web page. Customer

must object in writing within such 10-day notice period. OneSignal may address the objection (such as by finding a suitable work around) or allow Customer to terminate the Agreement for the affected Service. If OneSignal allows Customer to terminate the Agreement, Customer has 5 days following OneSignal's determination to notify OneSignal of Customer's election to terminate the Agreement effective upon written notice to OneSignal. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. OneSignal remains responsible for its Subprocessors and liable for their performance. This paragraph constitutes Customer's consent to both OneSignal's use of the Subprocessors and its subprocessing under the SCCs, as applicable.

Security

8. OneSignal will assist Customer in ensuring Customer's compliance with the security obligations of the GDPR and other Applicable Law, as relevant to OneSignal's role in Processing the Personal Data, taking into account the nature of Processing and the information available to OneSignal, by complying with the following paragraph and, if available in the Services, by providing configurable security options.
9. To protect the Personal Data OneSignal shall implement all appropriate technical and organisational measures to ensure that the requirements of the GDPR and other Applicable Law.
10. Customer is solely responsible for reviewing the available security documentation and evaluating for itself whether the Services and related security will meet Customer's needs, including Customer's security obligations under Applicable Law. Customer agrees that the security commitments in this DPA will provide a level of security appropriate to the risk in respect of the Personal Data.
11. OneSignal will ensure that the persons OneSignal authorizes to Process the Personal Data are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality.

Personal Data Breach Notification

12. OneSignal will comply with the Personal Data Breach related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to OneSignal, OneSignal will assist Customer in complying with those applicable to Customer by informing Customer of a confirmed Personal Data Breach without undue delay.

Assistance Responding to Data Subjects

13. Taking into account the nature of the Processing, OneSignal will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to honor requests by individuals (or their representatives) to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data).

Assistance with DPIAs and Consultation with Supervisory Authorities

14. Taking into account the nature of the Processing and the information available to OneSignal, OneSignal will provide reasonable assistance to and cooperation with Customer for Customer's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving OneSignal and related consultation with supervisory authorities by providing Customer with access to documentation for the Services. Additional support for data protection impact assessments or relations with regulators is available at Customer expense and will require a statement of work and mutual agreement on fees, the scope of OneSignal's involvement, and any other terms that the parties deem appropriate.

Data Transfers

15. Customer agrees and will ensure that Customer and its affiliates are entitled to transfer the Personal Data to OneSignal so that OneSignal and its Subprocessors may lawfully Process the Personal Data in accordance with the Agreement and this DPA.
16. The SCCs form part of this DPA, as applicable, and take precedence over the rest of this DPA to the extent of any conflict, with respect to Personal Data that is transferred to any country not recognized by the European Commission as providing an adequate level of protection for personal data. The SCCs will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the European Economic Area, the United Kingdom or Switzerland.
17. In connection with the performance of the Agreement, Customer authorizes OneSignal to transfer Personal Data from the European Economic Area, the United Kingdom and Switzerland to the United States of America in accordance with this DPA and as follows:
    - With respect to Personal Data that is protected by GDPR or the Swiss Federal Act on Data Protection, the EU SCCs attached hereto as Annex A and incorporated herein will apply; provided, that with respect to the Swiss Federal Act on Data Protection, the competent supervisory authority will be the Swiss Federal Data Protection and Information Commission, the governing law will be Switzerland, and references to member states will

refer to Switzerland, and data subjects in Switzerland will be entitled to exercise and enforce their rights under the EU SCCs in Switzerland and references to GDPR refer to the Swiss Federal Act on Data Protection; and

- With respect to Personal Data that is protected by the UK GDPR, the UK SCCs are incorporated herein and will apply; provided, that the competent supervisory authority will be the Information Commissioner's Office, the governing law will be the laws of England and Whales, references to members states will refer to the United Kingdom, data subjects in the United Kingdom will be entitled to exercise and enforce their rights under the UK SCCs in the United Kingdom. For purposes of Part I of the International Data Transfer Addendum, the terms of this Addendum, including the roles of the parties set out in Annex I to the EU SCCs and the technical measures set out in Annex II to the EU SCCs, shall apply. Both parties shall be allowed to end subscription to the International Data Transfer Addendum as set out in its Section 19. For purposes of Part 2 of the International Data Transfer Addendum, the EU SCCs shall apply.

OneSignal commits to comply with its obligations under the applicable SCCs with respect to the transfer of Personal Data.

For the purposes of the SCCs: (i) Customer will act as the "data exporter," (ii) OneSignal will act as the "data importer," and (iii) any sub-Processors, will act as "sub-processors" pursuant to the SCCs.

Return or Destruction

18. OneSignal will, at the choice of Customer, make available to Customer and/or destroy all Personal Data after the end of the provision of Services relating to Processing except to the extent Applicable Law requires storage of the Personal Data.
19. Nothing will oblige OneSignal to delete Personal Data from files created for security, backup and business continuity purposes sooner than required by OneSignal's data retention processes. If Customer requires earlier deletion of such Personal Data, and such deletion is commercially feasible, Customer must first pay OneSignal's reasonable charges for such deletion, which may include costs for business interruptions associated with such a request.

Audits

20. OneSignal will allow for and contribute to audits, including inspections, conducted by Customer or agreed upon third party auditor mandated by Customer, as follows:
    - If the requested audit scope is addressed in an ISO or similar audit report issued by a third party auditor within the prior twelve (12) months and OneSignal provides such report to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.
    - If an audit report is not provided, any audit, must be requested at least 30 days in advance, and must be limited to no more than once per twelve (12) month period, and Customer will conduct the audit only on an agreed date during OneSignal's normal business hours.
    - Any third-party auditor must execute a written confidentiality agreement acceptable to OneSignal.
    - Customer must promptly provide OneSignal with the results of any audit, including any third-party audit report. All such results and reports, and any other information obtained during the audit (other than Customer's Personal Data) is confidential information of OneSignal.
    - Nothing herein will require OneSignal to disclose or make available:
        i. any data of any other customer of OneSignal;
        ii. OneSignal's internal accounting or financial information;
        iii. any trade secret of OneSignal;
        iv. any information that, in OneSignal' reasonable opinion, could (i) compromise the security of OneSignal systems or premises; or (ii) cause OneSignal to breach its obligations under Applicable Law or its security and/or privacy obligations to Customer or any third party; or
        v. any information sought for any reason other than the good faith fulfilment of Customer's obligations under the Standard Contractual Clauses or Applicable Law.
21. In addition, to the extent required by Applicable Law, including where mandated by Customer's Supervisory Authority, Customer of Customer's Supervisory Authority may perform, at Customer's expense, a broader audit, including inspections of the data center facility that Processes Personal Data. OneSignal will contribute to such audits by providing Customer or Customer's Supervisory Authority with the information and assistance reasonably necessary to

conduct the audit, including any relevant records of Processing activities applicable to the Services.

22. Customer must provide OneSignal with any audit reports generated in connection with this DPA, unless prohibited by Applicable Law. Customer may use the audit reports only for the purposes of meeting Customer’s regulatory audit requirements and/or confirming compliance with the terms of this DPA.
23. Customer agrees that any audit conducted in accordance with Sections 20-22 above satisfies OneSignal’s audit obligations under the SCCs.

General

Each party’s liability towards the other party under, in connection with or arising from this DPA will be limited in accordance with the provisions of the applicable Agreement.

ANNEX A

STANDARD CONTRACTUAL CLAUSES

SECTION 1

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) : Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) - Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy itsobligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data

subject

with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and upon exporter’s request, certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation,
or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward Transfers

The data importer shall only disclose the personal data to a third party on documented instructions from
the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice, provided that data importer may make such inspections subject to additional reasonable privacy and security restrictions that (in importer's judgment) are necessary to protect any personal or entity's privacy, security, or proprietary rights, including those of importer.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a)

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

that contract that materially harms data exporter or results in the loss, unauthorized acquisition or other material breach of data exporter's personal data.

(e) The data importer shall agree to a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

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

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the Member State in which the date Exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer set forth in Order.

Address: The Customer's address set forth in the Addendum or the Agreement if no address is set forth in the Addendum.

Contact person's name, position and contact details: The contact information set forth in the Addendum or the Agreement if no contact information is set forth in the Addendum.

Activities relevant to the data transferred under these Clauses: The activities related to the services provided by the data importer pursuant to the Agreement.

Signature and date: Execution of the Order is deemed execution of this Addendum.
Role (controller/processor): controller

Data importer(s):

Name: OneSignal, Inc.
Address: 2850 S. Delaware St., Suite 201, San Mateo, CA 94403
Contact person's name, position and contact details: Long Vo, Chief Operating Officer, long@onesignal.com
Activities relevant to the data transferred under these Clauses: The services provided by data importer to the data exporter pursuant to the Agreement.
Signature and date: Execution of the Order is deemed execution of this Addendum.
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer's employees who use the Services
End users of Customer's mobile applications and/or websites

Categories of personal data transferred

The types and extent of Personal Data Processed aredetermined and controlled by the Customer in its sole discretion; provided that no sensitive information or special categories of data will be shared with OneSignal. Personal Data may include name, email, and IP address.

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.

Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Collecting, organizing, structuring, storing, altering, using, disclosing, combining, deleting and destroying

Purpose(s) of the data transfer and further processing

For OneSignal to provide the Services to Customer, including, specifically, delivering push notifications, in-app messaging, email messaging, and SMS messaging to the Customer's intended recipients; and supporting and communicating with Customer's employees who use 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

The duration of the main agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See above

C. COMPETENT SUPERVISORY AUTHORITY

The applicable competent supervisory authority in the EU Member State as contemplated by Clause 13 (Supervision).

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

Data importer is responsible for implementing and maintaining technical and organisational measures to help data importer secure data exporter's personal data against unauthorised data processing and accidental or unlawful loss, access or disclosure. It shall minimise security risks, including through risk assessment and regular testing.

Data importer shall designate one or more employees to coordinate and be accountable for the information security programme. The information security programme will include the following measures:

- Network Security: the computer network (servers, networking equipment, software systems etc. that are within data importer's control) through which the Services are provided will be accessible to employees, contractors and any other person, all only to the extent necessary. Data importer will maintain access controls and policies to manage what access is allowed (on a need to access basis) to the computer network, including the use of firewalls or functionally equivalent technology and authentication controls. Data importer will maintain corrective action and incident response plans to respond to potential security threats.

- Physical Security: physical components of the computer network are housed in facilities (the "**Facilities**"). Access to the Facilities is managed via:

- Implementation and maintenance of technical measures (e.g. to protect from the introduction of malicious computer programmes) to maintain the security of data exporter personal data.

- Implementation and maintenance of management and organisation measures, e.g. the appointment of an individual whose responsibility it is to look after such data; training staff as to their obligations; ensuring business continuity; ensuring periodic checks to ensure the organisation's security measures remain appropriate and up to date; relevant policies to limit the personal use of equipment.

- Separation of Data: Data exporter's data shall be kept separate from third party data to minimise the risk of unauthorised disclosure.

Security is a major focus for OneSignal and our clients. OneSignal clients can leverage most OneSignal features without ever transferring personally identifiable information (PII) or other sensitiveinformation. Nevertheless, we have paid careful attention to ensure that we go above and beyond bestpractices to protect our systems and client data.

Authentication (SSO)

OneSignal supports logging in to our service using e-mail and password authentication. We also support single sign-on through Github or Google Apps (GSuite). Accounts are automatically protected from weak passwords, and 2-Factor Authentication is supported.

Physical Security

OneSignal's servers are controlled by our cloud hosting provider Google Cloud and are housed in the Netherlands. This data center is highly secure, including ISO 27001, 27017, 27018 certifications and is SOC audited.

Network Security

OneSignal's servers are connected to each other via a private local network. All internal servers have strict firewalls in place to prevent access from non-OneSignal hosts both within our datacenter and externally. Servers that do allow remote connections (our load-balancers, for instance) also have strict firewall rules and are closely monitored.

All connections to OneSignal's public-facing services require TLS (HTTPS) encryption. Access to internal services is managed using Public-Private key authentication and is limited to key personnel.

Software Security

OneSignal regularly reviews our infrastructure to ensure that we are running up to date software across our infrastructure and that any CVEs or other software vulnerabilities are rapidly patched.

Modifications to OneSignal's software or infrastructure undergo review by at least one senior engineer on OneSignal's team to ensure best practices are followed and security vulnerabilities are not introduced. OneSignal also leverages thorough code testing and continuous integration to ensure that software security rules are working properly and regressions are not introduced.

Multi-Tenancy

OneSignal's servers leverage multi-tenancy to maximize the efficiency of hardware utilization. To mitigate the possibility of data ever being leaked across clients, OneSignal employs multiple levels of security and safeguards:

First, OneSignal's dashboard and API build upon a user permissions system that restricts access to data that users should not be able to reach. Next, OneSignal's database leverages partitioning to separate client data across multiple tables on each database server. Finally, OneSignal has a strong code review process and automated testing in place to minimize the possibility of deploying code changes that could negatively affect the safeguards we have in place or overall system security.

For additional security, OneSignal recommends that clients do not pass personally identifiable information (PII) to our system. PII is not required to utilize any features of OneSignal.

Incident Response

OneSignal has detailed monitoring in place across all of its infrastructure. In the event of a service disruption or unusual activity, a senior member of OneSignal's engineering and infrastructure team is immediately paged to investigate and resolve the problem.

OneSignal backs up customer data at a frequency of at least once every 24 hours. In the event of a hardware failure that affects a database server, recovery can be performed in 3-4 hours. OneSignal also maintains detailed logs on system activity to identify infrastructure or security issues.

In the unlikely event of a security incident, OneSignal will immediately notify affected clients and work with them to provide details on the incident and necessary follow-up steps.

Certifications

OneSignal itself does not have SOC or SSAE 16 certifications, however, our data center does have these certifications. You can learn more about this from them here:
https://cloud.google.com/security/compliance

Security Audits
OneSignal completes an annual comprehensive security assessment performed by Cherry Bekhaert.
https://www.cbh.com/

Data Retention

API and automated message data is kept for 30 days and then deleted from our servers. Data stored on our dashboard is kept for the lifetime of the application.