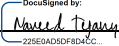


ALERT MEDIA, INC. DATA PROTECTION ADDENDUM TO THE MASTER SERVICES AGREEMENT

This Data Protection Addendum (“**DPA**”) is entered into as of the date of the last signature below, (the “**Effective Date**”), by and between the customer specified in the table below (“**Customer**”) and Alert Media, Inc. (“**Supplier**”), each a “**Party**” and together the “**Parties**” to this DPA.

SIGNATORY INFORMATION

Supplier: Alert Media, Inc.	Customer:
Signature:  <small>DocuSigned by: Naveed Tejany 2256A0D5DF8D4C...</small>	Signature:
Name: Naveed Tejany	Name:
Title: CFO	Title:
Date Signed: 6/30/2025	Date Signed:
Address: 401 S. 1st St., Suite 1400 Austin, TX 78704, USA	Address:
DPO/Privacy Contact: Privacy Team Legal@alertmedia.com	DPO/Privacy Contact:
Supervisory Authority (for purposes of Annex 1.C of the SCCs, which is forth in Exhibit 2, Part 2-C of this DPA):	

RECITALS

- (A) Supplier provides certain communication services (“**Supplier Services**”) to Customer under an agreement between Supplier and Customer (“**Main Agreement**”).
- (B) In connection with the Supplier Services, Supplier may process certain personal data on behalf of Customer.
- (C) The Customer and Supplier have agreed to enter into this DPA, which sets forth the obligations and requirements applicable to the Processing of personal data pursuant to the Supplier Services, in order to comply with applicable Data Protection Laws (defined below).

TERMS

1. Definitions

1.1. The following definitions are used in this DPA:

- (a) “**Common Control**” means, with respect to two entities, that one entity either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity; for purpose of this definition and the DPA, an entity “**controls**” another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract.
- (b) “**Controller**” means an entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data

- (c) **“Customer Personal Data”** means any Personal Data that is processed by Supplier (or any Sub-processor) on behalf of Customer, pursuant to Supplier’s performance of the Supplier Services under the Main Agreement;
- (d) **“Customer Group”** means Customer and any corporate entities which are from time to time under Common Control with Customer;
- (e) **“Data Subject”** means any identified or identifiable natural person about whom the Personal Data relates;
- (f) **“Data Subject Request”** means a request from or on behalf of a Data Subject as permitted under Data Protection Laws, including those relating to access to, rectification, erasure, or data portability in respect of that person’s Personal Data or an objection from or on behalf of a Data Subject to the Processing of its Personal Data;
- (g) **“Data Protection Laws”** means the applicable data protection, privacy and cyber security laws or regulations, including but not limited to the following to the extent applicable: EU Data Protection Laws and US Privacy Laws;
- (h) **“Deidentified Data”** means data that (a) has been “deidentified” pursuant to applicable Data Protection Laws such that it cannot longer reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject, and (b) is subject to reasonable measures to ensure that it cannot be associated with a particular Data Subject or household.
- (i) **“EU Data Protection Laws”** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the Processing of Personal Data under the Main Agreement, including the GDPR and UK Data Protection Laws, to the extent applicable;
- (j) **“GDPR”** means 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 (known as the General Data Protection Regulation);
- (k) **“Personal Data”** means information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, as well as other information defined as personal data or personal information under applicable Data Protection Laws;
- (l) **“Process”** or **“Processing”** means any operation or set of operations performed on Personal Data, whether or not by automated means, including but not limited to 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 of the data.
- (m) **“Processor”** means a person or entity that Processes Personal Data on behalf of and under the instructions of the Controller;
- (n) **“Restricted Transfer”** means a transfer of Customer Personal Data to, by or between Supplier and any Sub-processor (including Supplier Group members), to the extent such transfer would be prohibited by applicable Data Protection Laws in the absence of the SCCs;
- (o) **“Standard Contractual Clauses”** or **“SCCs”** means the EU Standard Contractual Clauses (Modules One to Four), as set out and approved in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including the Annexes thereto, which are currently posted at http://data.europa.eu/eli/dec_impl/2021/914/oj and are hereby incorporated by reference into this DPA, (including the Annexes thereto), subject to the terms of Section 6 and Exhibit 2 of this DPA (as applicable), together with and as amended by the UK Addendum (as applicable), as well as any alternative or successor clauses thereto, which are recognized by the European Commission or a relevant Supervisory Authority and which may be adopted by one of the Parties hereunder;

- (p) **“Sub-processors”** means any entity engaged by Supplier to provide any portion of the Supplier Services or that who will otherwise process any Customer Personal Data;
- (q) **“Supervisory Authority”** means a data protection or other regulatory body or public agency with the jurisdiction to enforce applicable Data Protection Laws;
- (r) **“Supplier Group”** means Supplier, its subsidiaries, and any affiliate entities that are under Common Control with Supplier;
- (s) **“Swiss Data Protection Laws”** means the applicable Data Protection Laws of Switzerland, including the (revised) Swiss Federal Act on Data Protection of 25 September 2020;
- (t) **“UK Data Protection Laws”** means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (**“UK GDPR”**), together with the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (as amended), each as further amended. In this DPA, in circumstances where and solely to the extent that the UK GDPR applies, references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions, and references to “EU or Member State laws” shall be construed as references to UK laws; and
- (u) **“UK Addendum”** means the International Data Transfer Addendum (current version B.1.0) to the Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, which is currently posted at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf> and is hereby incorporated by reference into this DPA.
- (v) **“US Privacy Laws”** means the California Consumer Privacy Act (**“CCPA”**) and U.S. state laws similar to the CCPA, including, but not limited to, the Colorado Privacy Act and related regulations, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Florida Digital Bill of Rights, the Indiana Consumer Data Protection Act, the Iowa Consumer Privacy Act, the Montana Consumer Data Privacy Act, the New Hampshire Privacy Act, the New Jersey Privacy Act, the Oregon Consumer Privacy Act, the Texas Data Privacy and Security Act, the Tennessee Information Protection Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act, each including any implementing regulations and each as it becomes effective.

1.2. Capitalized terms used but not otherwise defined in this DPA will have the meaning otherwise set forth in the Main Agreement.

2. Processing of Personal Data

2.1. The type of Customer Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the Processing, and the categories of Data Subjects, are as described in Exhibit 1 of this DPA.

2.2. Each of the Customer and Supplier in relation to Customer Personal Data will (and will assure that any of its staff and/or Sub-processors) comply with applicable Data Protection Laws. As between the Parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data. Customer will ensure that all required notices are provided to, and all required consents obtained from individuals related to the Processing of their Personal Data pursuant to the Supplier Services.

2.3. In respect of the Parties' rights and obligations under this DPA regarding the Customer Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller and Supplier is the Processor. Accordingly, with respect to the Processing of Customer Personal Data:

- 2.3.1. The Parties will comply with their respective obligations under the applicable Data Protection Laws; and
- 2.3.2. Supplier will process Customer Personal Data in accordance with its obligations under this DPA and the Main Agreement.
- 2.4. Customer agrees that Supplier may, unless prohibited by applicable laws, retain, use and otherwise process aggregate and non-identifiable data derived from or related to the Supplier Services, which does not directly or indirectly identify, and is not otherwise linked or linkable, to a particular Data Subject, subject to the following:
 - (a) Supplier may use such data for the purposes of improving the Supplier Services and Supplier's internal business operations, developing new services, products, and offerings, and detecting and preventing misuse, and for security, fraud protection and quality control purposes;
 - (b) Such data shall be Supplier's own information or data and shall not be Customer Personal Data pursuant to this DPA, provided Supplier complies with Section 2.4(c) (to the extent applicable); and
 - (c) To the extent Supplier processes Deidentified Data (as defined under applicable Data Protection Laws), Supplier will (i) follow reasonable measures to prevent such data from being associated with a particular individual or household, including by any recipient of such data; and (ii) otherwise comply with the requirements under applicable Data Protection Laws with respect to Deidentified Data.

3. **Supplier obligations**

- 3.1. With respect to Customer Personal Data, Supplier will:
 - (a) only process the Customer Personal Data in order to provide the Supplier Services and in accordance with this DPA and the Customer's written instructions, as represented by the Main Agreement and this DPA;
 - (b) in the unlikely event that applicable law requires Supplier to Process Customer Personal Data other than pursuant to the Customer's instruction, Supplier will notify the Customer (unless prohibited from so doing by applicable law);
 - (c) as soon as reasonably practicable upon becoming aware, inform the Customer if, in Supplier's opinion, any instructions provided by the Customer infringe the EU Data Protection Laws;
 - (d) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the Processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. Such measures include, without limitation, the security measures set out in Exhibit 3 below.
 - (e) take reasonable steps to ensure that only authorized personnel have access to such Customer Personal Data and that any persons whom it authorizes to have access to the Customer Personal Data are under obligations of confidentiality;
 - (f) in the event of any unauthorized or accidental disclosure of or access to Customer Personal Data (a "**Security Breach**"), Supplier will:
 - (i) notify Customer as soon as reasonably practicable upon becoming aware of a Security Breach;
 - (ii) promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach;
 - (iii) provide Customer with relevant information in Supplier's possession concerning the Security Breach, including, to the extent known: (a) the possible cause and consequences of the Security Breach; (b) the categories of Customer Personal Data involved; (c) a summary of the possible

consequences for the relevant Data Subjects; (d) a summary of the unauthorized recipients of the Customer Personal Data; and (e) the measures taken by Supplier to mitigate any damage;

- (iv) except to the extent required by applicable law, not make any announcement about a Security Breach (a “**Breach Notice**”) without: (a) the prior written consent from the Customer; and (b) prior written approval by the Customer of the content, media, and timing of the Breach Notice;
 - (g) if Supplier receives a Data Subject Request involving Customer Personal Data, Supplier will:
 - (i) promptly notify the Customer; and
 - (ii) not respond to such a Data Subject Request without the Customer’s prior written consent, except to confirm that such request relates to the Customer, such confirmation to which the Customer hereby agrees;
 - (h) upon the Customer’s request, Supplier will provide reasonable assistance as necessary to enable Customer to respond to a Data Subject Request as required by Data Protection Laws, provided the Customer shall pay the Supplier’s charges for providing such assistance, at the Supplier’s standard consultancy rates set out in the Main Agreement. Customer as Controller is responsible for deciding whether a Data Subject Request involving Customer Personal Data should be actioned or not and is responsible for any Customer Personal Data Processed by Customer or the Supplier after a Data Subject Request has been received by Customer (and whether Customer decides to act on the request or not).
 - (i) as soon as reasonably practicable following, and in any event within thirty (30) days of, termination or expiry of the Main Agreement or completion of the Supplier Services, Supplier will delete or return to the Customer (at the Customer’s direction) all Customer Personal Data (including copies thereof) Processed pursuant to this DPA.
 - (j) upon request, provide reasonable assistance (taking into account the nature of Processing and the information available to Supplier) as necessary to enable the Customer to comply with its requirements under applicable Data Protection Laws with respect to data protection impact assessments and notifications to a Supervisory Authority, such assistance to be at the cost of Customer, billed at Supplier’s standard consultancy rates.
- 3.2. To the extent the CCPA applies to the Processing of Customer Personal Data, without limiting its other obligations herein, Supplier will:
- (a) not use, retain, or disclose Customer Personal Data except in order to perform the Supplier Services and as set forth in this DPA;
 - (b) not “sell” or “share,” any Customer Personal Data as those terms are defined under the CCPA;
 - (c) not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Supplier, except as expressly permitted by the CCPA;
 - (d) not combine Personal Data that it receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person, except as expressly permitted by the CCPA;
 - (e) comply with its obligations under the CCPA and provide the same level of privacy protection as required by the CCPA;
 - (f) notify Customer without undue delay if it can no longer meet its obligations under the CCPA; and
 - (g) grant Customer the right to take reasonable and appropriate steps upon prior written notice to Supplier to (i) ensure Supplier utilizes Customer Personal Data in a manner

consistent with the CCPA as applicable, and (ii) stop and remediate any unauthorized use of Customer Personal Data.

- 3.3. With respect to any request, enquiry, or complaint received by Supplier or any Sub-processor from a Supervisory Authority or other third-party regarding Customer Personal Data, including any request to exercise rights under the Data Protection Laws, (hereafter, a “**Third-Party Request**”), Supplier will, unless prohibited from doing so by applicable laws: (a) promptly notify Customer of such Third-Party Request; and (b) not respond to such Third-Party Request, except on the documented instructions of Customer or as required by applicable laws, in which case Supplier will to the extent permitted by such applicable laws provide prior notice to Customer of such legal requirement prior to responding to such Third-Party Request. Upon request, Supplier will provide reasonable assistance to enable Customer to seek to limit, quash or respond to such Third-Party Request.

4. **Sub-processing**

- 4.1. The Customer grants a general authorization to Supplier to (a) appoint other members of the Supplier Group as Sub-processors, (b) continue to use other members of the Supplier Group, as well as those other Sub-processors currently in use as of the Effective Date, and (c) engage other members of the Supplier Group, Sub-processors, and/or other third parties where the engagement of such third party (or its services) supports the performance of the Supplier Services, including but not limited to, third party data center operators, enterprise data storage providers, and communication providers.
- 4.2. Supplier will maintain the list of Sub-processors through the Supplier admin portal at <https://www.alertmedia.com/subprocessors/> and will add the names of new and replacement Sub-processors to the list prior to them starting sub-processing of Customer Personal Data. If the Customer has a reasonable objection to any new or replacement Sub-processor, it shall notify Supplier of such objections in writing within ten (10) days of the notification and the Parties will seek to resolve the matter in good faith. If Supplier is able to provide the Supplier Services to the Customer in accordance with the Main Agreement without using the Sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.2 in respect of the proposed use of the Sub-processor. If Supplier requires to use the Sub-processor and is unable to satisfy the Customer as to the suitability of the Sub-processor or the documentation and protections in place between Supplier and the Sub-processor within thirty (30) days from the Customer's notification of objections, the Customer may within thirty (30) days of the end of the 30-day period referred to above terminate the Main Agreement by providing written notice to Supplier having effect thirty (30) days after receipt by Supplier. Supplier will refund to the Customer any prepaid fees covering the remainder of the term of the Main Agreement following the date of termination. Supplier may use a new or replacement Sub-processor whilst the objection procedure in this clause 4.2 is in process.
- 4.3. Supplier will ensure that any Sub-processor it engages to provide the services on its behalf in connection with this Agreement does so only on the basis of a written contract which imposes on such Sub-processor terms substantially no less protective of Customer Personal Data than those imposed on Supplier in this DPA (the “**Relevant Terms**”). Supplier shall procure the performance by such Sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such Sub-processor of any of the Relevant Terms.

5. **Audit and records**

- 5.1. To satisfy the Customer's right of audit under applicable Data Protection Laws, Supplier may provide:
 - (a) an audit report not older than 12 months by an independent external auditor demonstrating that Supplier's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard such as ISO 27001 or SSAE 16 II SOC1 or SOC2; and
 - (b) as applicable, additional relevant information in Supplier's possession or control to an EU Supervisory Authority when such authority requests or requires additional information from Customer in relation to the Processing activities carried out by Supplier under this DPA.

To the extent the information provided in subsections (a) and (b) are not sufficient to meet Customer's obligations under Data Protection Laws, Customer may seek additional information through an audit as set forth in section 5.2 below.

- 5.2. To the extent the audit rights set forth in Section 5.1 are not sufficient, Supplier shall, in accordance with applicable Data Protection Laws, as necessary, make available to the Customer such information in Supplier's possession or control as the Customer may reasonably request to demonstrate Supplier's compliance with applicable obligations of data processors under Data Protection Laws in relation to its Processing of Customer Personal Data. Customer will give Supplier reasonable written notice of any audit or inspection to be conducted under this section and Customer and Supplier shall agree in writing to the scope of access to personnel, written materials, and any other information Customer shall have in conducting the audit. Except as otherwise required by applicable law or a relevant Supervisory Authority, any audit or inspection will be conducted within normal business hours, no more than once in any calendar year. Any information Customer obtains under such audit shall be subject to all confidentiality obligations as set forth in the Main Agreement. Customer shall pay Supplier for any time personnel expend in responding to any audit requests, billed at Supplier's standard consultancy rates.

6. Cross-border transfers of Personal Data

- 6.1. Customer consents to the Processing and transfer of Customer Personal Data outside the jurisdiction in which it was collected, including Restricted Transfers of Customer Personal Data, subject to Supplier's compliance with the obligations set out in this Section 6.
- 6.2. The SCCs and the UK Addendum are hereby incorporated by reference into this DPA and shall apply, subject to the terms of this Section 6 and Exhibit 2 to the DPA, as applicable.
- 6.3. With respect to Restricted Transfers by Customer to Supplier, by executing this DPA, Customer (as the "data exporter" and a Controller) and Supplier (as the "data importer" and a Processor), hereby enter into the SCCs and the UK Addendum, which will take effect upon the commencement of, and apply, subject to Exhibit 2, to the extent of a Restricted Transfer of Customer Personal Data by Customer to Supplier as follows:
 - 6.3.1. For Restricted Transfers that are subject to EU Data Protection Laws, UK Data Protection Laws, or Swiss Data Protection Laws ("**European Data Protection Laws**"), the SCCs (including the Annexes thereto) shall apply subject to, and as set forth in, Exhibit 2 of this DPA; and
 - 6.3.2. For Restricted Transfers of Personal Data not subject to European Data Protection Laws ("**Other Restricted Transfers**"), (Module 2 of) the SCCs will apply, subject to Section 6.4 of this DPA, and a description of the Processing of Customer Personal Data is set forth in Annex 1 to this DPA.
- 6.4. For Other Restricted Transfers: (a) the terms of the SCCs (including the Annexes thereto) will apply *mutatis mutandis*; (b) the terms "Member State" and "State" will be replaced throughout by the word "jurisdiction;" (c) "supervisory authority" means the relevant data protection regulator or other government body with authority to enforce the applicable Data Protection Laws in the jurisdiction in which the data exporter is established (the "**Local Data Protection Law**"); (d) with respect to disputes arising under the SCCs, except to the extent prohibited by the Local Data Protection Law, the governing law and the choice of forum and jurisdiction (venue) shall be the same as specified in the Main Agreement and where required by the Local Data Protection Law, as an alternative place of jurisdiction (venue), a Data Subject may bring a claim in the local courts in which the Data Subject habitually resides.
- 6.5. Prior to any Restricted Transfer by Supplier to a Sub-processor, Supplier will ensure that its written agreement with such Sub-processor incorporates the applicable Standard Contractual Clauses in respect of such Restricted Transfers.
- 6.6. To the extent applicable, the Parties agree that transfers of Customer Personal Data to a data importer (including Supplier, a Supplier Group member or a Sub-processor) in the United States who is certified, and complies with its obligations, under the Data Privacy Framework is not a Restricted Transfer pursuant to the European Data Protection Laws and the SCCs shall not

apply to such transfers of Customer Personal Data, to the extent they meet the foregoing requirements. Such SCCs shall apply if the Data Privacy Framework is no longer applicable for any reason.

- 6.7. Customer agrees that a data importer may provide a copy or summary of the relevant terms of the written agreement with Customer to an applicable Supervisory Authority upon request.

7. Changes in Data Protection Laws

- 7.1. If any amendment to this DPA is required as a result of a change in Data Protection Laws, then either Party may provide written notice to the other Party of that change in law. The Parties will discuss and negotiate in good faith any necessary variations to this DPA to address such changes. The Parties will not unreasonably withhold consent or approval to amend this DPA, pursuant to this Section 7.1 or otherwise.
- 7.2. Without limitation to Section 7.1, in the event the SCCs are replaced, amended, supplemented or superseded with a new version ("**New Clauses**"), Customer agrees that Supplier may amend this DPA in order to incorporate the New Clauses, by providing written notice to Customer of such amendment (the "**Amendment**") at least thirty (30) days prior to such amendment taking effect (the "**Amendment Effective Date**"). Notice of such Amendment may be provided by Supplier to Customer electronically, by emailing the Privacy Contact identified in the Signatory Information section of this DPA, or by providing legal notice to the Customer in accordance with the terms of the Main Agreement.

8. General

- 8.1. This DPA is without prejudice to the rights and obligations of the Parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the Processing of Customer Personal Data, except the in the event of a conflict between the SCCs and another term of this DPA, the SCCs will prevail.
- 8.2. Supplier's liability to Customer under or in connection with this DPA (including under the SCCs and UK Addendum) shall be subject to the exclusions and limitations of liability set out in the Main Agreement as if liability under this DPA arose under the Main Agreement. For purposes of the foregoing, references to "Supplier's liability to Customer" includes, collectively, Customer and any Customer Group member authorized to use the Supplier Services under the Main Agreement.
- 8.3. This DPA sets out all of the terms that have been agreed between the Parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.
- 8.4. A person who is not a Party to this DPA shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this DPA.
- 8.5. This DPA shall be governed by and construed in accordance with the laws of the country or territory which govern the DPA, and subject to the dispute resolution procedures and jurisdiction provisions set out in the Main Agreement.
- 8.6. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA will remain valid and in force. The invalid or unenforceable provision will be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Exhibit 1

Details of the Personal Data and Processing activities

1. **Categories of Customer Personal Data:** names, email address, phone numbers, and other contact information of Customer's employees and other authorized users; contact preferences for employees and end users; and records of communications sent to employees and end users
2. **Duration of the Processing of Customer Personal Data:** until the earliest of (i) expiry/termination of the Main Agreement (pursuant to Section 9 of the Main Agreement) or (ii) the date upon which Processing is no longer necessary for the purposes of either Party performing its obligations under the Main Agreement (to the extent applicable);
3. **Nature of the Processing of Customer Personal Data:** The Supplier Services provide Customer a platform for sending emergency and urgent mass communications to employees and other end users; Customer may elect to upload Data Subjects' contact information so Customer can use Supplier Services to send messages to those people over SMS, phone, email, and other communication channels;
4. **The purpose(s) of the Processing of Customer Personal Data:** to provide the Supplier Services, in particular:
 - to maintain current contact information and contact preferences for customer end users;
 - to send and facilitate the sending of (email, phone and text) messages to Customer's employees and other end users; and
 - to maintain records and logs of communications sent via the Supplier Services.
5. **Categories of Data Subjects:** end users of Customer, which may include employees, members, or other Data Subjects to whom Customer wants to send a message.
6. **Sub-processors:** The Sub-processors engaged by Supplier as of the Effective Date are available through the Supplier admin portal at: <https://www.alertmedia.com/subprocessors/>.

Exhibit 2**Standard Contractual Clauses**

Pursuant to Section 6 of the DPA, where applicable, the Parties agree to be bound by and comply with the applicable terms of the SCCs, including the Clauses and the Annexes thereto, the UK Addendum (as applicable), and any applicable additional terms, subject to the terms of this Exhibit 2 and Section 6 of the DPA.

Contents:

Part 2-A	Identifies the relevant Module and certain selections applicable to the SCCs.
Part 2-B	Sets forth additional terms applicable to Restricted Transfers governed by UK Data Protection Laws and Swiss Data Protection Laws.
Part 2-C	Contains the Appendix (Annex I and Annex 2) to the Clauses and forms an integral part of the SCCs.

Part 2-A: Applicable Module and Selections

Module Two (Controller to Processor) of the Clauses (including Annexes I and II) shall apply, subject to and with reference to the following selections:

1. Clause 9 (Use of Sub-Processors): Option 2 (General Written Authorization) will apply and the specific time period for notice by the data importer of intended changes to its Sub-processors is the time period set forth in Section 4 (Subprocessing) of the DPA.
2. Clause 7 (Docking): the (optional) Clause 7 does apply.
3. Clause 11(a) (Redress): the optional paragraph of Clause 11(a) does not apply.
4. Clause 13 (Supervision): for purposes of Clause 13, the relevant supervisory authority as specified in Annex I.C will be as follows:
 - 4.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
 - 4.2. Where Customer 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 shall act as competent supervisory authority.
 - 4.3. Where Customer 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, shall be the Irish Data Protection Commission.
 - 4.4. Where Customer is established in Switzerland or falls within the territorial scope of application of the Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority for Restricted Transfers governed by the Swiss Data Protection Laws (in accordance with Part 2-B, Paragraph 1 of this Exhibit 2).

- 4.5. Where Customer is established in the United Kingdom or falls within the territorial scope of UK Data Protection Laws, the Information Commissioner's Office ("ICO") shall act as competent supervisory authority for Restricted Transfers governed by UK Data Protection Laws (in accordance with Part 2-B, Paragraph 2 of this Exhibit 2).
- 4.6. For Other Restricted Transfers, the relevant supervisory authority will be the relevant data protection regulator or other government body with authority to enforce the applicable Data Protection Laws of the jurisdiction in which the data exporter is established (in accordance with Section 6.4 of the DPA).
5. Clause 17 (Governing Law): Option 1 shall apply and the Parties specify the law of the Republic of Ireland except that:
 - 5.1. For Other Restricted Transfers, the governing law is as specified in Section 6.4 of the DPA; and
 - 5.2. For Restricted Transfers governed by Swiss Data Protection Laws or UK Data Protection laws, the governing law is as specified in Paragraphs 1 and 2, respectively, of Part 2-B of this Exhibit 2.
6. Clause 18 (Choice of Forum and Jurisdiction): For purposes of paragraph b) of Clause 18, the parties select the law and courts of the Republic of Ireland, except that:
 - 6.1. For Other Restricted Transfers, the choice of forum and jurisdiction is as specified in Section 6.4 of the DPA; and
 - 6.2. For Restricted Transfers governed by Swiss Data Protection Laws or UK Data Protection laws, the governing law will be as specified in Paragraphs 1 and 2, respectively, of Part 2-B of this Exhibit 2.
7. Annexes: Annex 1 and Annex 2 of the SCCs are completed with reference Part 2-C herein. Annex 3 does not apply.

Part 2-B: Additional Terms for Swiss, UK and Other Restricted Transfers

1. For Restricted Transfers of Customer Personal Data from Switzerland, governed by Swiss Data Protection Laws:
 - 1.1. General and specific references in the Clauses to the GDPR, Regulation (EU) 2016/679, EU Member State Law, or any provisions thereof, shall be interpreted as references to Swiss Data Protection Laws or the equivalent reference in the Swiss Data Protection Laws, as applicable;
 - 1.2. Any other obligation in the Clauses determined by the Member State in which the Data Subject is established shall refer to an obligation under Swiss Data Protection Laws, as applicable;
 - 1.3. For purposes of the Clauses, the relevant supervisory authority will be the Swiss Data Protection and Information Commissioner, the governing law will be the law of Switzerland, and the applicable forum will be the federal courts of Switzerland; and
 - 1.4. The term "Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18.

2. For Restricted Transfers of Customer Personal Data from the United Kingdom, which are governed by UK Data Protection Laws:
 - 2.1. The Clauses shall be read, apply in accordance with, and be deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum;
 - 2.2. For purposes of the Clauses, the relevant supervisory authority is the UK Information Commissioner's Office, the governing law will be the laws of England and Wales, and the applicable forum for disputes will be the courts of England and Wales;
 - 2.3. The information required to complete Part 1 (Tables) of the UK Addendum is set out in this Exhibit 2:
 - 2.3.1. The information required to complete Table 1 is specified in Part 2-C (Annex 1.A) of this Exhibit 2;
 - 2.3.2. The information required to complete Table 2 is specified in Part 2-A of this Exhibit 2;
 - 2.3.3. The information required to complete Table 3 is specified in Part 2-C (Annexes 1 and 2) of this Exhibit 2; and
 - 2.3.4. For purposes of Table 4, the Importer and the Exporter may end the UK Addendum as set forth in Section 19 of the UK Addendum.

Part 2-C: Annexes I and II to the SCCs

APPENDIX

ANNEX 1

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the EU.*

- Name:** As set forth in the Signatory Information section of the DPA

Address: As set forth in the Signatory Information section of the DPA

Contact person's name, position and contact details: As set forth in the Signatory Information section of the DPA

Activities relevant to the data transferred under these Clauses: Use of Supplier's communication service, primarily offered in the form of web and mobile applications and a related API.

Role (controller/processor): Controller

Signature and date: The SCCs are signed and executed by the data exporter, as of the Effective Date of the DPA (as set forth in the Signatory Information section of the DPA).

Data importer(s): *Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the EU.*

- Name:** Alert Media, Inc.

Address: 401 S. 1st St., Suite 1400, Austin, Texas, 78704, USA

Contact person's name, position and contact details: Naveed Tejany, CFO

Activities relevant to the data transferred under these Clauses: To provide a communication service, primarily offered in the form of web and mobile applications and a related API

Role (controller/processor): Processor

Signature and date: The SCCs are signed and executed by the data importer, as of the Effective Date of the DPA (as set forth in the Signatory Information section of the DPA)

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data is transferred

End users of Customer, which may include employees, members, or other Data Subjects to whom Customer wants to send a message.

Categories of personal data transferred

- Names, email address, phone numbers, and other contact information of Customer's employees and other end users
- Contact preferences for employees and end users
- Records of communications sent to employees and end users

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.

None.

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

☐ One-off

☒ Continuous

☐ Other: [...]

Nature of the processing

The Supplier Services provide Customer a platform for sending emergency and urgent mass communications to employees and other end users; Customer may upload the contact information for such users so that Customer can use Supplier Services to send messages to them over SMS, phone, email, and other communication channels

Purpose(s) of the data transfer and further processing

To provide the Supplier Services, in particular:

- to maintain current contact information and contact preferences for customer end users;
- to send and facilitate the sending of (email, phone and text) messages to Customer's employees and other end users; and
- to maintain records and logs of communications sent via the Supplier Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Services, unless otherwise set forth in the DPA.

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

The sub-processors engaged as of the Effective Date and the subject matter and nature of their processing are specified in Exhibit 1 to the DPA. The duration of processing is generally the duration of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

- The competent supervisory authority is (a) specified in the Signatory Information section of the DPA, or, (b) if no competent supervisory authority is specified in the Signatory Information section of the DPA, the competent supervisory authority will be The Data Protection Commission of Ireland, except that:
- For Restricted Transfers governed by Swiss Data Protection Laws, UK Data Protection Laws or Other Data Protection Laws, the competent supervisory authority is as specified in Sections 4.4, 4.5 and 4.6, respectively, of Part 2-A of this Exhibit 2.

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

Data importer will implement and maintain technical and organizational measures for the security of the Customer Personal Data, as set forth in the admin portal at <https://www.alertmedia.com/security-measures/>.