COMPANY DATA PROCESSING AGREEMENT

The terms of this Data Processing Agreement ("**DPA**") shall apply to any Processing of Personal Data carried out by the Parties under an applicable Company Master Services **Agreement** accepted or executed by Client (the "Agreement"). Capitalized terms used in this DPA but not defined below are defined in the Agreement.

1. Definitions

(a) **"Client Personal Data"** means any Personal Data contained within the Client Data.

(b) **"Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processor",** and **"Processing"** are each as defined in the GDPR (and **"Processes", "Processed",** and **"Process"** shall be interpreted accordingly).

(c) **"Documentation"** means the applicable documentation for the services made available to Client by Company from time to time and which sets out a description of the services and the user instructions for the Services.

(d) **"GDPR"** means, as applicable, the European Union General Data Protection Regulation 2016/679 and/or the UK GDPR, as defined in section 3(10) (as supplemented by section 205(4)) of the United Kingdom's Data Protection Act 2018 (the **"DPA 2018"**).

(e) **"Losses"** means losses, damages, claims, liabilities, costs (including costs of investigation, litigation, settlement, and judgment), claims, demands, disbursements, expenses (including legal costs on a solicitor and own-client basis), fees, interest, and penalties (including fines imposed by regulatory bodies or supervisory authorities).

(f) **"Privacy Laws"** means all applicable laws, treaties, and regulations regarding the Parties' respective Processing of Client Personal Data, including without limitation the GDPR, the United Kingdom's DPA 2018, the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100, et seq. and its implementing regulations, as amended by the California Privacy Rights Act (the **"CCPA/CPRA"**), and Canada's Personal Information Protection and Electronic Documents Act (the **"PIPEDA"**).

(g) **"Security Incident"** means as defined at clause 6.

(h) **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 2021 **("EU SCCs")** and the UK International Transfer Addendum to the EU SCCs **("UK Addendum").**

2. Compliance with Privacy Laws. Each Party shall comply with its respective obligations under all applicable Privacy Laws in relation to any and all Client Personal Data that it Processes under or in connection with the Agreement.

3. Status of the Parties. To the extent that the GDPR applies to the activities of either Party under or in connection with the Agreement, the Parties hereby acknowledge and agree that (unless otherwise expressly stated in Everbridge's Privacy Notice): Client is a Controller and Company is a Processor in connection with the Solutions.

4. Client responsibilities. Client warrants, represents, and undertakes that:

(a) it has and shall, throughout the term of the Agreement, maintain (at its own cost and expense) all relevant regulatory registrations and notifications as required from time to time under applicable Privacy Laws;

(b) all data or information provided by Client to Company under or in connection with the Agreement shall comply in all respects with applicable Privacy Laws (including, for example, by providing all required notices to, and obtaining all required consents from, Users and Contacts);

(c) it has all necessary appropriate consents and notices in place to enable the lawful transfer of the Client Personal Data to Company for the duration of the Agreement;

(d) all instructions that Client gives to Company in respect of the Client Personal Data shall at all times fully comply with applicable Privacy Laws;

(e) it shall not unreasonably withhold, delay, or make conditional its agreement to any change or amendment to this DPA requested by Company to ensure that the Processing complies with applicable Privacy Laws;

(f) it shall establish and maintain adequate security measures to safeguard the Client Personal Data in its possession or control from unauthorized or unlawful destruction, corruption, Processing or disclosure, and shall maintain complete and accurate back-ups of all Client Personal Data provided to Company (or anyone acting on Company's behalf) so as to be immediately able to recover and reconstitute such Client Personal Data in the event of loss, damage, or corruption thereof or thereto;

(g) it has undertaken appropriate due diligence in relation to Company's Processing operations, and it is satisfied that: (i) Company's Processing operations are suitable for the purposes for which the Client proposes to use the Services and engage Company to Process the Client Personal Data; and (ii) Company has sufficient expertise, reliability, and resources to implement technical and organizational measures that meet the requirements of applicable Privacy Laws.

5. **Scope and confidentiality of Processing.** Company shall ensure that any person that it authorizes to Process the Client Personal Data, including Company's staff, agents and subcontractors (an **"Authorized Person"),** shall be subject to a legally binding duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to Process the Client Personal Data who is not under such a duty of confidentiality by applying the Technical and Organizational Security Measures of this DPA. Company shall ensure that all Authorized Persons Process the Client Personal Data only as necessary for the purposes permitted under the Agreement. Company shall only Process (and shall ensure that its Authorized Persons shall only Process) the Client Personal Data in accordance with this DPA and (subject to the remainder of this clause 5) with Client's reasonable prior written instructions to Company (and not otherwise unless alternative Processing instructions are agreed beforehand between the Parties in writing), except where otherwise required by applicable laws to which Company is subject. Company shall inform Client if Company believes that any instruction received by it from Client infringes or may infringe applicable Privacy Laws, and Company shall be entitled to cease performing the relevant services under the Agreement until the Parties have agreed appropriate amended instructions which are not infringing (but, where Company does not cease performing the relevant services, then, to the maximum extent permitted by law and subject to the terms of the Agreement, Company shall have no liability (howsoever arising) for any Losses suffered or incurred by Client and which arise directly or indirectly from or in connection with any Processing in accordance with such instruction following Company's having informed Client of the relevant infringement or potential infringement in accordance with this clause 5. Client acknowledges and agrees that the execution of any computer command to Process (including deletion of) any Client Personal Data made in the use of any of the services by the Client's personnel or a third party instructed by the Client will constitute a Processing instruction (other than to the extent such command is not fulfilled due to technical, operational, or other reasons, including as set out in the Documentation). Client shall ensure that its personnel or a third party instructed by the Client do not execute any such command unless expressly and specifically authorized by Client (and by all other relevant Controller(s)) and acknowledges and accepts that, if any Client Personal Data is deleted pursuant to any such

command, Company is under no obligation to seek to restore it. For clarity, and subject to the terms of the Agreement, Company shall have no liability for any Losses suffered or incurred by Client arising out of any breach of the Privacy Laws or this DPA to the extent that such Losses (or the circumstances giving rise to them) are contributed to or caused by Client.

6. **Security.** Company shall implement appropriate technical and organizational measures to protect the Client Personal Data from loss, alteration, unpermitted disclosure of, or unpermitted access to the Client Personal Data (a **"Security Incident").** Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing (as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) and (as appropriate):

   (a) the pseudonymization and encryption of the Client Personal Data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems;

   (c) the ability to restore the availability and access to the Client Personal Data in a timely manner in the event of a physical or technical incident; and

   (d) a procedure for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

7. **Subprocessing.** You consent to Company's use of its existing Sub-processors, which is provided at www.everbridge.com/about/legal/everbridge-sub-processors/, and grant Company a general written authorization to engage Sub-processors as necessary to perform the Services. Company will notify you if it intends to add one or more Sub-processors to that list at least 30 days before the changes take effect, using the email address you provide when subscribing to email notifications on the identified Sub-processor webpage or the email address we use to provide you service messages. You may reasonably object to a change on legitimate grounds within 30 days after you receive notice of the change. You acknowledge that Company's Sub-processors are essential to provide the Services and that if you object to Company's use of a Sub-processor, then notwithstanding anything to the contrary in the Agreement and this DPA, you can choose not to use the parts of the Services that the Subprocessor supports (for example, by choosing not to use a communication path supported by that Subprocessor.)

8. **Data Transfer.** To the extent that the activities of either Party pursuant to the Agreement are subject to the GDPR, Client agrees that Company may transfer Client Personal Data Processed by or on behalf of Company in connection with the provision of the services to countries outside the European Economic Area **("EEA")** and the United Kingdom **("UK")** provided all such transfers by Company shall (to the extent required under Privacy Laws) be: (i) to a country, territory, or jurisdiction deemed, at the time of such transfer, by both the European Commission and the U.K. to have an adequate level of protection pursuant to Article 45 of the GDPR (an **"Adequate Country")**; (ii) to an entity that is based in a country, jurisdiction, or territory that is not an Adequate Country (a **"Non-Adequate Country"**) but which is certified under a framework deemed adequate and approved by the European Commission (such as the EU-US Data Privacy Framework, the UK Extension established thereto pursuant to the UK's Data Protection (Adequacy) (United States Of America) Regulations 2023, and the Swiss-US Data Privacy Framework); or (ii) to any other entity located in a Non-Adequate Country provided always that: (x) either Party has provided appropriate safeguards in relation to such transfer; (y) the relevant Data Subjects have enforceable rights and effective legal remedies; and (z) Company complies with its obligations under the Privacy Laws by providing an adequate level of protection to any Client Personal Data that is thus transferred. The provisions of this clause 8 shall constitute Client's instructions with respect to transfers in accordance with clause 5 of this DPA. Client acknowledges that, due to the nature of cloud services, the Client Personal Data may be transferred to other geographical locations in connection with use of the services further to access and/or computerized instructions initiated by the Client's

personnel or third parties instructed by the Client, and Client acknowledges that Company does not control such Processing and Client shall ensure that its personnel (and all others acting on its behalf) only initiate the transfer of Client Personal Data to other geographical locations if appropriate safeguards are in place and that such transfer is in compliance with all applicable Privacy Laws. If an adequate protection measure for the international transfer of Personal Data is required under the Privacy Laws (and has not otherwise been arranged by the parties) the Data Transfer Provisions shall be incorporated into this DPA in Schedules 1 and 2 as if they had been set out in full.

9. **Cooperation and Data Subjects' rights.** Company shall, at Client's own cost (and always taking into account the nature of Processing by, and information available to, Company) provide to Client such reasonable and timely assistance to Client as Client may reasonably require to enable Client to respond to: (i) any request from a Data Subject to exercise any of its rights under applicable Privacy Laws (including its rights of access, correction, objection, erasure and data portability and right to prohibit sale or resale, as applicable); and (ii) any other correspondence, inquiry, or complaint received from a Data Subject, regulator or supervisory authority, or other third party in connection with the Processing of the Client Personal Data. If any such request, correspondence, inquiry, or complaint is made directly to Company, Company shall promptly inform Client, providing full details of the same. Notwithstanding anything to the contrary in the Agreement, Company reserves the right to disclose the identity of Client to any relevant Data Subject following Company's receipt of any such request, correspondence, inquiry, or complaint.

10. **Data protection impact assessments.** If Company believes or becomes aware that its Processing of the Client Personal Data is likely to result in a high risk to the data protection rights and freedoms of relevant Data Subjects, it shall promptly inform Client and shall, at Client's own cost (and always taking into account the nature of Processing by, and information available to, Company), provide Client with such reasonable and timely assistance as Client may reasonably require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

11. **CCPA/CPRA Compliance.** Company is a service provider under the CCPA/**CPRA.** Company shall not sell, rent, lease, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, personal information of California residents (referred to as "consumers" under the CCPA/**CPRA**) to another business, person, or third party for monetary or other valuable consideration. Company shall not disclose personal information of California residents to another business, person, or a third party, except for the purpose of performing Services specified in the Agreement or to the extent such disclosure is permitted hereunder or required by applicable law. Company may disclose personal information of California residents required by applicable law only after: (i) notifying Client of the legal requirement prior to disclosing any the information (unless otherwise prohibited by applicable law); and (ii) taking steps to ensure that only the information that is legally required is disclosed. Company shall notify Client of any verifiable consumer request within two (2) working days of receiving it and shall, at Client's cost, provide reasonable assistance to Client with meeting its CCPA/**CPRA** compliance obligations and responding to CCPA/**CPRA** -related inquiries. Company certifies that it understands and will comply with the restrictions of this clause 11.

12. **Security Incidents.** Upon becoming aware of a Security Incident, Company shall inform Client without undue delay (48 hours) and shall provide all such timely information and cooperation as Client may reasonably require in order for Client to fulfill its data breach reporting obligations under (and in accordance with the timescales required by) applicable Privacy Laws. Company shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident for which Company is responsible and shall keep Client informed of all material developments in connection with the Security Incident.

13. **Demonstration of Compliance and Audit.** Company shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Client information to demonstrate such compliance, including those obligations required by applicable Privacy Laws. Client acknowledge and agrees that Client will exercise its audit rights under this DPA by instructing Company to comply with the audit measures described in this 'Demonstration of Compliance' section. Client acknowledge that the Solutions are hosted by Company's hosting sub-processors (e.g., AWS, Azure) who maintain independently validated security programs (including SOC 2 and ISO 27001) and that Company's systems are audited annually and regularly tested by independent third party penetration testing firms. Where Company has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service, Company agrees to provide these certifications or standards, on request, for the duration of the Agreement so that Client can verify

    Company's compliance with this DPA. Company will further cooperate with reasonable requests by Client for documentary audits of Company's security and privacy practices by completing a security questionnaire no more than once per year unless Client has reasonable grounds to suspect non-compliance with the DPA. Company will provide Client with any information necessary to enable Client to comply with a request from a regulatory body or to demonstrate compliance with law, provided that Company will not release any confidential information of other customers. If a regulator wishes to carry out an audit of Company or its activities under this Agreement, Client will provide Company with no less than 30 days' notice, unless the regulator has given less notice.

    Without prejudice to the above Client audit rights, if a requested documentary audit scope is addressed in (a) a SOC, ISO or similar audit report issued by a qualified third-party auditor within the prior twelve months; or (b) the detailed materials available at trust.everbridge.com (including an industry standard questionnaire such as SIG Lite), and Company provides the Client with such report and materials confirming there are no known material changes to the controls described, Client agrees to accept such findings and materials in lieu of requesting completion of a questionnaire describing the same controls covered by such a report and detailed materials.

14. **Disclosure to authorities.** Company acknowledges that Client may disclose these terms and the data privacy provisions of this DPA and the Agreement to the US Department of Commerce, the Federal Trade Commission, recognized EEA or UK supervisory authority, or any other US or EEA judicial or regulatory body upon their request and that any such disclosure shall not be deemed a breach of confidentiality.

15. **Deletion of Client Personal Data.** Unless Company is required to continue Processing the relevant Client Personal Data under or in connection with a separate order made under the Agreement, following the expiration or termination of a particular order under the Agreement , Company shall (at Client's election) return or flag all Client Personal Data Processed by or on behalf of Company under or in connection with such terminated or expired order for purging and shall delete such Client Personal Data from its active systems. Client shall make such election by using self-service features in the platform to delete or return/download its data.

16. **Processing particulars.**

    (a) *Subject matter and purpose of the Processing of Client Personal Data:* Company's performance of its obligations under the Agreement.

    (b) *The nature of the Processing of Client Personal Data:* The collection, recording, hosting, organization, alteration, correction, consultation, retrieval, disclosure by transmission, erasure, and destruction thereof (in each case for the purposes of providing the relevant Services to Client as set forth in the Agreement, including any specific order to the Agreement).

    (c) *The types of Client Data to be Processed:* As specified in the Agreement or relevant order to the Agreement and that client uploads while using the applicable Services. The personal data transferred includes the following categories of data such as: employee/contractor name, business email address, business telephone and mobile numbers. Certain services process geo-location and travel information.

(d) *The categories of data subject to whom the Client Data relates:* As specified in the Agreement or relevant order to the Agreement. The Categories of Data Subjects include Client's employees, contractors, and Contacts.

(e) *The duration of the Processing of Client Personal Data:* Company's Processing of the Client Personal Data shall continue for the duration of the Agreement.

SCHEDULE 1: EU SCCS

1. Incorporation of the EU SCCs

1.1. To the extent clause 8 applies and the transfer is made pursuant to the GDPR, this Schedule 1 and the following terms shall apply:

1.1.1. *Where clause 3 applies and the Client is located in an Adequate Country and Company is located in a Non-Adequate Country:* Module 2 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 1 as if they had been set out in full in the case where the exporter is a Controller, the importer is a Processor and the transfer requires such additional protection;

1.1.2. *Where clause 3 applies and the Client is itself a Processor, with one party located in an Adequate Country and the other in a Non-Adequate Country:* Module 3 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 1 as if they had been set out in full in the case where the exporter is a Processor, the importer is a subprocessor and the transfer requires such additional protection; and

1.1.3. *Where clause 3 applies and Company is located in an Adequate Country and the Client is located in a Non-Adequate Country:* Module 4 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 1 as if they had been set out in full in the case where the exporter is a Processor, the importer is a Controller and the transfer requires such additional protection.

2. Clarifications to the EU SCCs

2.1. To the extent Module 2 and Module 3 of the EU SCCs apply:

2.1.1. Deletion of data. For the purposes of clause 8.5 of the EU SCCs (Duration of processing and erasure or return of data), the parties agree as follows: At the end of the provision of the processing services the importer shall delete all Personal Data and shall certify to the exporter that it has done so, if requested to provide such certification by the exporter in writing.

2.1.2. Auditing. The parties acknowledge that the importer complies with its obligations under clause 8.9 of the EU SCCs (Documentation and compliance)

2.1.3. by exercising its contractual audit rights it has agreed with its subprocessors.

2.1.4. Subprocessors. For the purposes of clause 9 of the EU SCCs (Use of subprocessors), option 2 (general) applies and the parties agree that the process for appointing subprocessors set out in clause 7 applies.

2.2. To the extent Module 2 and Module 3 of the EU SCCs apply:

2.2.1. Competent Supervisory Authority. For the purposes of clause 13 of the EU SCCs, the competent Supervisory Authority shall be:

- if the exporter is established in an EU Member State: The Irish Data Protection Commissioner;
- where the exporter is not established in an EU Member State and has appointed a representative pursuant to Article 27(1) GDPR, it shall notify the importer of this and the EU Member State in which the exporter's representative is appointed shall be the competent Supervisory Authority; and
- where the exporter is not established in an EU Member State, but falls within the territorial scope of Article 3(2) GDPR but has not appointed a representative pursuant to

Article 27(1) GDPR: the exporter shall notify the importer of its chosen competent supervisory authority, which must be the Supervisory Authority of an EU Member State in which the Data Subjects whose personal data is transferred under the EU SCCs in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

2.3. To the extent Module 1, Module 2, Module 3 and Module 4 of the EU SCCs apply:

2.3.1. International Transfer Assessments. For the purposes of clause 14(c) of the EU SCCs (Local laws and practices affecting compliance with the Clauses) the exporter has been provided with a transfer impact assessment by the importer which the exporter accepts as sufficient to fulfil the importer's obligations pursuant to clause 14(c) and 14(a). The exporter acknowledges that it has been provided with the security measures applied to the Personal Data and approves such measures as being in compliance with the EU SCCs.

2.3.2. Best Efforts Obligations. For the purposes of clauses 14(c), 15.1(b) and 15.2 of the EU SCCs (Local laws and practices affecting compliance with the clauses) the parties agree that "best efforts" and the obligations of the importer under clause 15.2 shall mean exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a leading practice engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2.3.3. Governing Law & Jurisdiction. For the purposes of clauses 17 and 18 of the EU SCCs, the parties agree that the governing law and choice of jurisdiction shall be where the exporter is established. If those laws do not allow for third party rights, the law of Netherlands shall apply and the courts of Netherlands will have exclusive jurisdiction.

2.4. To the extent Module 3 of the EU SCCs applies:

2.4.1. the exporter warrants that it has the rights necessary to transfer the personal data to the importer; and

2.4.2. any request received from a data subject in connection with the personal data being processed by the importer shall be forwarded to the exporter to facilitate with the controller of such personal data; and (iv) for the purposes of clause 8.6(c) and (d) of the EU SCCs, the importer shall notify the exporter of any personal data breach.

2.5. To the extent Module 4 of the EU SCCs applies, for the purposes of clause 8.1(d) of the EU SCCs, at the end of the provision of the processing services the importer shall delete all Personal Data and shall certify to the exporter that it has done so, if requested to provide such certification by the exporter in writing.

3. Processing Particulars for the EU SCCs

The Parties

Module 2:

- **Exporter (Controller):** The Client
- **Importer (Processor):** Company

Module 3:

- **Exporter (Processor):** Company where Company is located in an Adequate Country / the Client where the Client is located in an Adequate Country

- **Importer (Processor):** The Client where Company is located in a Non-Adequate Country / Company where the Client is located in a Non-Adequate Country

Module 4:

- **Exporter (Processor):** Company
- **Importer (Controller):** The Client

Description Of Data Processing

- **Categories of data subjects:** As set out at clause 16(d).
- **Categories of personal data transferred:** As set out at clause 16(c).
- **Sensitive data transferred:** As set out at clause 16(c).
- **Frequency of the transfer:** Continuous.
- **Nature of the processing:** As set out at clause 16(b).
- **Purpose of the processing:** As set out at clause 16(a).
- **Duration of the processing:** For the duration of the Agreement.
- **Subprocessor Transfers:** As set out at clause 7.
- **Competent Supervisory Authority:** As set out at paragraph 2.3.1.
- **Technical and Organisational Security Measures.** The Company Technical and Organizational Security Measures available at the Services & Compliance Policies Page: https://www.everbridge.com/company-policies

SCHEDULE 2: UK ADDENDUM

1. Parties

As set out in Schedule 1.

2. Selected SCCs, Modules and Clauses

2.1. Module 2, Module 3 and Module 4 of the EU SCCs and no other optional clauses unless explicitly specified, and as amended by the clarifications in Schedule 1, paragraph 2, but subject to any further amendments detailed in this Schedule

2.2. Personal data received from the importer is not combined with personal data collected by the exporter.

3. Appendix Information

The processing details required by the UK Addendum are as set out in Schedule 1, paragraph 3.

4. Termination of the UK Addendum

In the event the template UK Addendum issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the DPA 2018 on 2 February 2022, as it is revised under Section 18 is amended, either party may terminate this Schedule 2 on written notice to the other in accordance with Table 4 and paragraph 19 of the UK Addendum and replace it with a mutually acceptable alternative.