Data Processing Addendum

Updated on 12/31/2025

This Data Processing Addendum, including the Standard Contractual Clauses (as defined below) attached hereto (collectively, the "**DPA**" or "**Addendum**"), is made and entered into as of the effective date (the "**Effective Date**") of the applicable customer's ("**Customer**") acceptance of the Terms of Service between **Plus Five Five, Inc. ("Company" or "Resend")** and Customer to which this DPA is attached and incorporated (the "**Agreement**"). All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement.

This Addendum shall become legally binding upon Customer entering into the Agreement or upon execution of this Addendum.

1. Definitions

1.1. “**Affiliate**” means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2. "**Data Subject**" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by EU Data Protection Laws; or (ii) a "Consumer" as the term is defined in the CCPA.

1.3. "**Customer Data**" means any content, data, information or other materials (including Personal Information) submitted or shared by or for Customer to or through the Service.

1.4. "**Personal Information**" means information relating to a living individual or household who is, relates to, describes or can be, reasonably identified or linked, directly or indirectly from information, either alone or in conjunction with other information, within the Company's or Customer's control and which is stored, collected, Processed or submitted to or via the Service as Customer Data. Personal information includes Personal Data.

1.5. “**Authorized Sub-Processor**” means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is authorized under Section 4.2 of this DPA.

1.6. “**Company Account Data**” means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.7. “**Company Usage Data**” means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.8. “**Data Exporter**” means Customer.

1.9. “**Data Importer**” means Company.

1.10. “**Data Protection Laws**” means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act (“CCPA”), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”) and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “UK GDPR”) (together, collectively, the “GDPR”), (iii) the Swiss Federal Act on Data Protection, ; (iv) the UK Data Protection Act 2018; and (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms “Data Subject”, “Personal Data”, “Personal Data Breach”, “processing”, “processor,” “controller,” and “supervisory authority” shall have the meanings set forth in the GDPR.

1.11. “**ex-EEA Transfer**” means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the “EEA”), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.12. “**ex-UK Transfer**” means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the “UK”), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.13. “**Services**” shall have the meaning set forth in the Agreement.

1.14. “**Standard Contractual Clauses**” means the EU SCCs and the UK SCCs.

1.15. “**UK SCCs**” means the EU SCCs, as amended by the UK Addendum.

1.16. “**EU SCCs**” means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this DPA.

2. Relationship of the Parties; Processing of Data

2.1. The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

2.2. Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.4. Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

2.5. CCPA. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not sell any such personal information. Company shall not retain, use or disclose any personal information provided by Customer pursuant to the Agreement except as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms “personal information,” “service provider,” “sale,” and “sell” are as defined in Section 1798.140 of the CCPA. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality

3.1. Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

4.1. Customer acknowledges and agrees that Company may (1) engage its Affiliates as well as the Authorized Sub-Processors on the List (defined below) to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal

Data. By way of this DPA, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2. A list of Company's current Authorized Sub-Processors (the “List”) is available to Customer at https://resend.com/legal/subprocessors. Such List may be updated by Company from time to time. Company shall specifically inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

4.3. If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

4.4. If Customer does not object to the engagement of a third party in accordance with Section 4.2 within fourteen (14) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

4.5. Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.6. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Customer.

4.7. The Company shall only disclose the personal data to a third party on documented instructions from the data exporter or in alignment with this DPA. In addition, the data may only be disclosed to Authorized Sub-Processors.

5. Security of Personal Data.

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Company's technical and organizational security measures.

6. Transfers of Personal Data

6.1. The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2. Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

6.2.1. Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.

6.2.2. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA. 6.2.3. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

6.3. For each module, where applicable the following applies:

6.3.1. The optional docking clause in Clause 7 does not apply.

6.3.2. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this DPA;

6.3.3. In Clause 11, the optional language does not apply;

6.3.4. All square brackets in Clause 13 are hereby removed;

6.3.5. In Clause 17 (Option 1), the EU SCCs will be governed by Ireland law.

6.3.6. In Clause 18(b), disputes will be resolved before the courts of Ireland;

6.3.7. Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

6.3.8. Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and

6.3.9. By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4. Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein by reference.

6.5. Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

6.5.1. The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the “FADP,” and as revised as of 25 September 2020, the “Revised FADP”) with respect to data transfers subject to the FADP.

6.5.2. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (“FDPIC”) of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4. The term “EU Member State” as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6. Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1. As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

6.6.2. Our organization may disclose personal information in response to lawful requests by public authorities, including to comply with national security or law enforcement requirements. In the event the Data Importer receives such a request after the date of this DPA, the Company will, where permitted by law, make reasonable efforts to redirect the requesting authority to seek the data directly from the Data Exporter (Customer). To facilitate this, the Company may provide the requesting authority with the Customer's basic contact information. If the Company is compelled to disclose Personal Data to a public authority, it will, unless prohibited by law, provide the Customer with prompt notice of the request and reasonably cooperate with the Customer to enable it to seek a protective order or other appropriate remedies. The Company will not voluntarily disclose Personal Data to any public authority in the absence of a valid and binding legal requirement. Furthermore, the Data Exporter and Data Importer agree to consult and determine, as soon as practicable, whether any transfers of Personal Data under this DPA should be suspended to safeguard the rights and interests of the Data Subjects, taking into account the scope and implications of such requests.

6.6.3. The Data Exporter and Data Importer will meet as needed to consider whether:

6.6.3.1. the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

6.6.3.2. additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

6.6.3.3. it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4. If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required

by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

6.7. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, the Company commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

7. Rights of Data Subjects

7.1. Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively “Data Subject Request(s)”). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

7.2. Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

7.3. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, the Company commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, should first contact the Company at privacy@resend.com.

8. Actions and Access Requests; Audits

8.1. Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.2. Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3. Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. Customer shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

8.4. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for

the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

8.5. Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6. In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

8.7. In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8. The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Company's Role as a Controller

9.1. The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by the Company as a controller

shall be in accordance with the Company's privacy policy set forth at https://resend.com/legal/privacy-policy.

10. Conflict

10.1. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) the Company's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11. Data Privacy Framework

11.1. The Company complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. The Company has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program and Principles and to view our certification, please visit https://www.dataprivacyframework.gov/.

11.2. The Company is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). This ensures that our practices comply with applicable privacy and data protection laws as required under the EU-U.S. and UK Extension Data Privacy Framework.

11.3. Under certain conditions, Customers have the right to invoke binding arbitration to address residual complaints that have not been resolved through other recourse mechanisms. This arbitration is conducted in accordance with the terms set forth in Annex I of the DPF Principles. To initiate binding arbitration, a Customer must deliver notice to our organization and follow the procedures outlined in Annex I of the DPF Principle, including exhausting all other available remedies under the DPF. The arbitration panel has authority to impose specific, non-monetary equitable relief necessary to remedy violations of the DPF Principles. This mechanism ensures a fair resolution process at no cost to the Customer.

11.4 In the context of onward transfers to third parties, the Company remains responsible for the processing of personal data it receives under the DPF and subsequently transfers to an agent on its behalf. The Company may be liable under the DPF if its agent processes such personal

data in a manner inconsistent with the DPF Principles, unless the Company can prove that it is not responsible for the event giving rise to the damage. The Company ensures that any third-party agent processes personal data in accordance with the DPF Principles and requires such agents to safeguard personal data consistent with our commitments under this policy.

12. Signatures

The signature blocks set forth below are provided for reference purposes only. This DPA becomes legally binding upon Customer's acceptance of the Agreement or execution of this DPA, as set forth in the preamble above. The executed version of this DPA may be accessed by Customer through the Resend dashboard at any time following execution.

Customer

By: _____

Name: _____

Title: _____

Date: _____

PLUS FIVE FIVE, INC.

By: DocuSigned by: Zeno Rocha Bueno Netto
6E371008C43F42B...

Name: Zeno Rocha Bueno Netto

Title: CEO

Date: 1/14/2026

Exhibit A

Details of Processing

Categories of data subjects whose personal data is transferred

> *Data subjects are the recipients of emails the Customer sends using our Services – typically their customers. Where the Customer is a processor, data subjects are their customers and end users. > Resend also transfers the personal data of the (representatives of the) Customer, those who enter into this agreement and anyone they allow to access their account (users, for example employees, contractors, collaborators). For this processing and transfer of personal data, Resend is the Controller and our Privacy Policy applies.*

Categories of personal data transferred

> *The categories of personal data transferred relates to the sending and receiving of email messages (and which constitutes personal data). At a minimum, this includes metadata, email address and message content. Message content may also include name and other information decided and added by the sender, like attachments. The Customer also has the option to enable open/link tracking and other analytics/tracking of recipient actions, which could include IP address, location, operating system, browser, device, email client and spam complaints.*

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 specialized 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).

> *The frequency of transferring the personal data is continuous, until the agreement comes to an end.*

Nature of the processing

> *Application emails sent through Resend are categorized as _transactional or marketing electronic messages. Transactional emails are primarily functional, high-priority messages sent to a single recipient, like password resets or receipts/invoices. Marketing emails are sent to multiple recipients at once, like announcements of product updates or revised terms of service. The nature of the processing relates to facilitate sending and receiving such email messages, including hosting/storage of contact lists and message content, and analytics services._*

Purpose(s) of the data transfer and further processing

> *The purpose of transferring the personal data is to allow the Customer to reliably deliver application emails to their users/customers.*

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

> *We process personal data on behalf of the Customer for as long as the Agreement is active. When the Customer terminates their use of the Services, we delete their user/ customer data within 90 days of the account termination.*

Exhibit B

List of Parties

Data Exporter:

- Name: Customer, as specific in the Agreement.
- Contact: As specified in the Agreement.

- Signature and date: The parties agree that execution of the Agreement by the Data Importer and the Data Exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.
- Role: Controller/Processor

Data Importer:

- Name: Plus Five Five, Inc.
- Address: 2261 Market Street #5039 San Francisco, CA 94114
- Contact: Resend Security - privacy@resend.com
- Signature and date: The parties agree that execution of the Agreement by the Data Importer and the Data Exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.
- Role: Processor

Exhibit C

Technical and Organisational Security Measures

Resend will maintain administrative, physical, and technical safeguards designed for protection of the security, confidentiality, and integrity of Personal Information uploaded to the Service, as described in this annex.

1. **SECURITY GOVERNANCE**

1.1. Resend maintains an information security program (including the adoption and enforcement of internal policies and procedures) designed to: (a) help our customers secure their data processed using Resend's online product against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Resend online product, and (c) minimize security risks, including through risk assessment and regular testing. Resend's head of security coordinates and is primarily responsible for the company's information security program.

1.2. The team covers the following core functions:

1.2.1. Application security (secure development, security feature design, the Security Champions program, and secure development training)

1.2.2. Infrastructure security (data centers, cloud security, and strong authentication)

1.2.3. Monitoring and incident response (cloud native and custom)

1.2.4. Vulnerability management (vulnerability scanning and resolution)

1.2.5. Compliance and technical privacy

1.2.6. Security awareness (onboarding training and awareness campaigns)

1. **ACCESS CONTROL**

2.1. Preventing Unauthorized Product Access

2.1.1. Third party data hosting and processing: We host our Service with third party cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with the DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

2.1.2. Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls of such providers are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

2.1.3. Authentication: Customers who interact with the products via the user interface are required to authenticate before they are able to access their non-public data. We support two-factor authentication via social login as well as Single-Sign On.

2.1.4. Authorization: Customer Content (data originated by customers that a customer transmits through Resend) is stored in multi-tenant storage systems which are only accessible to Customers via application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

2.1.5. Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through OAuth authorization. Authorization credentials are stored encrypted.

2.2. Preventing Unauthorized Product Use. We implement industry-standard access controls and detection capabilities for the internal networks that support our products.

2.2.1. Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

2.2.2. Static code analysis: Automated security reviews of code stored in our source code repositories, performed through static code analysis, checking for coding best practices and identifiable software vulnerabilities.

2.2.3. Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

2.3. Limitations of Privilege & Authorization Requirements

2.3.1. Product access: A subset of our personnel have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of personnel is to provide effective customer support, troubleshoot potential problems, detect, and respond to security incidents, and implement data security.

2.3.2. Personnel Security: Resend personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Resend conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local law and regulations.

2.3.3. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Resend's confidentiality and security policies. Personnel are provided with security training.

1. **ENCRYPTION TECHNOLOGIES**

3.1. In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on all our interfaces. Our HTTPS implementation uses industry-standard algorithms and certificates.

3.2. At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

1. **INPUT CONTROLS**

4.1. Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal

systems aggregate log data and alert appropriate personnel of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

4.2. Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, and/or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and customer damage or unauthorized disclosure. Notifications will be in accordance with the terms of the Agreement.

1. **DATA DELETION AND PORTABILITY**. Resend enables customers to request deletion or export of their account and data in a manner consistent with the functionality of the Resend product.

2. **AVAILABILITY CONTROLS**. Resend products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

6.1. Redundancy: The infrastructure providers use designs to eliminate single points of failure and minimize the impact of anticipated environmental risks. Resend's product is designed to allow the company to perform certain types of preventative and corrective maintenance without interruption.

6.2. Business Continuity: Resend has designed and regularly plans and tests its business continuity planning/disaster recovery programs.