# PLUM VOICE DATA PROCESSING ADDENDUM

## 1. **Overview**

This Data Processing Addendum ("**DPA**") forms part of the **Plum Voice Hosted Order Form**, and/or any other principal written or electronic agreement ("**Principal Agreement**") between Plum Voice "Plum" and Customer, acting on its own behalf, for the purchase and use of Plum's services, to reflect the parties' agreement regarding Plum's Processing of Personal Data on behalf of Customer.

The terms used in this DPA have the meanings set forth in this DPA. Except as outlined below, the terms of the Principal Agreement remain in full force and effect.

## 2**. Enforcement of this Addendum**

2.1 To enforce this DPA, Customer must complete the information on pages 5,13, and 15.
2.2 This Addendum will be effective only if it is executed and submitted to Plum in accordance with Section 2.1 of this Agreement, and all information is accurate and complete.

## 3. **Definitions**

**"Breach"** is an unlawful access to Personal Data, or an unlawful access to Plum's equipment or facilities through which Personal Data is Processed.

**"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

**"Data Protection Laws and Regulations"** refers to applicable laws and regulations, including, but not limited to, US federal and state laws and the General Data Protection Regulations of the EU.

**"Data Subject"** is the person to whom the Personal Data relates.

**"GDPR"** stands for the General Data Protection Regulations of the European Union, and relates to the Processing of Personal Data and the free movement of such data.

**"Personal Data"** means any information relating to an identified or identifiable natural person (Data Subject). Under the GDPR, an identifiable natural person is one who could be particularly identified, directly or indirectly, by reference to identifiers that include, but are not limited to:

- a name;
- an identification number;
- location data;
- an online identifier; or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person.

References to "Customer's Personal Data" include both Personal Data the belongs to the Customer, and Personal Data that belongs to Customer's end-users.

**"Processing"** as defined in Article 4 of the GDPR, means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as: collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use or disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**"Processor"** is the entity that completes the Processing of Personal Data on behalf of the Controller.

**"Sub-Processor"** means any Processor engaged by Plum.

**"Supervisory Authority"** means an independent public authority which is established by an EU member state pursuant to Article 51 of the GDPR, who is responsible for monitoring adherence to the GDPR by those subject to the regulations. The goal of Supervisory Authorities is to protect the fundamental rights and freedoms of Data Subjects in relation to Processing, and to facilitate the free flow of Personal Data within the European Union.

## 4. Processing of the Personal Data

4.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, and Plum is the Processor, and its affiliates are Sub-Processors.

4.2 **Plum's Processing of Personal Data.** Plum will only process Customer's data according to the Customer's instructions.

4.3 **Description of the Processing**. The details of the Processing performed by Plum, which includes the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1.

## 5. Rights of the Data Subjects

**Data Subject Request.** As mandated under the GDPR, if a Data Subject requests to change or delete incorrect data, or otherwise access the Data Subject's Personal Data that was Processed by Plum, Plum must review that request and respond as required by GDPR and other applicable Data Protection Laws and Regulations as outlined above. This includes a prompt notification to Customer of the request. This process must be completed to allow the Data subject to exercise its rights granted by the GDPR.

## 6. Plum Security Standards

6.1 **Plum Personnel**. Plum must ensure that its personnel that is responsible for the Processing of Personal Data, is well-informed of the confidential nature of the Personal Data, and has received appropriate training on their responsibilities.

6.2 **Limitation of Access**. Plum shall ensure that access to Personal Data is limited to personnel that is required to Process this data or otherwise access this data per designated job duties.

6.3 **Disclosure**. Plum will not disclose Customer's Personal Data to any government, except as necessary to comply with the law. If a law enforcement agency sends Plum a request or demand for Customer Data, Plum will, as permitted by law, redirect the request to Customer.

6.4 **Periodic Evaluation.** On a periodic basis, Plum will review the adequacy of its security program and standards through methods that include, but are not limited to, the following: internal audits of Plum's systems to evaluate personnel compliance to company procedures; periodic review of Plum's security policies; and periodic review of relevant laws, standards, and regulations, in an effort to keep up with all applicable changes and updates. The results of these evaluations will allow Plum to determine if there is a need to update or change its current security measures.

## 7. Plum's Security Responsibilities

7.1 **Overall Security Responsibilities.**

7.1.1 Plum understands and acknowledges that it is responsible for the security of Personal Data, including cardholder data, that it Processes. To carry out this responsibility, Plum understands and acknowledges that it must maintain appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of any Personal Data Plum Processes on behalf of the Customer.

7.1.2 Plum monitors its compliance with these measures periodically. Customer is solely responsible for reviewing the information made available by Plum relating to Plum's data security measures, and for making an independent determination as to whether these measures are sufficient.

7.2 **Network Security.** Plum will maintain access controls and policies that aim to manage who has access into Plum's Network, which includes daily monitoring of network access. Plum also has an incident response plan in place which outlines response mechanisms for potential security threats, which is tested on an annual basis.

7.3 **Physical Security.** The physical components of Plum's infrastructure are housed in a secure data center facility. Measures in place that prevent unauthorized access into the data center include ID badges and a fingerprint scan, which is required at various points of entry throughout the data center. Human security personnel is also on-site to prevent unauthorized access. Additionally, all visitors are required to sign-in with designated personnel, and must show proper identification to obtain a visitor's pass, which must be worn at all times that the visitor is in the facility.

## 8. Transfers of Personal Data

**Application of Standard Contractual Clauses.** The Standard Contractual Clauses[1] outlined in Appendix A will apply if Customer's Personal Data is transferred outside of the EEA, either directly, or via onward transfer, to a country that is not recognized to have the adequate safeguards outlined in Article 45 of the GDPR in place for such transfers. However, if Plum adopts Binding Corporate Rules, or an alternative recognized compliance standard for the lawful transfer described above, the Standard Contractual Clauses will no longer apply.

## 9. Audit of Technical and Organizational Measures

Plum engages with external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which Plum provides its Services. These audits are performed on an annual basis, and are performed according to applicable Data Protection Laws and Regulations that Plum is subject to.

[1] Note that the Standard Contractual Clauses still refer to Directive 95/46/EC, which was repealed by the GDPR on May 25, 2018. Despite the standing references, this DPA does incorporate the requirements listed under Article 28 of the GDPR that are not fully covered by the Standard Contractual Clauses in its current form.

**10. Security Breach Notification**

10.1 If Plum becomes aware of a Breach, involving Customer's Personal Data that is Processed by Plum, Plum will promptly notify Customer of the Breach, and will take reasonable steps to mitigate the effects of, and any damage resulting from the Breach, as required by Data Protection Laws and Regulations.

10.2 Customer agrees that an unsuccessful security incident will not be subject to this section. An unsuccessful security incident is one that results in no unauthorized access to Customer's Personal Data, or to any of Plum's equipment or facilities where Processing of Data occurs.

10.3 Customer agrees that Plum's obligation to report or respond to a Breach under this section is not, and will not, be construed as an acknowledgment by Plum of Plum's fault or liability with respect to the security incident.

10.4 Unless otherwise required by law, if a security notice is required, Plum will first notify Customer via email. Notice will be given promptly, consistent with the legitimate needs of law enforcement. Plum may delay notification if Plum, a law enforcement agency, or Supervisory Authority, determines that the notification will impede a criminal investigation, unless Plum, or the relevant agency determines that notification will not compromise the investigation.

**11. Confidentiality and Nondisclosure**

11.1 Customer agrees that the details of this Addendum are not publicly known and is considered confidential information under the confidentiality provisions of the other contracts between Plum and Customer, such as an NDA between the parties. If an NDA does not exist between the parties, and other contracts do not contain a confidentiality provision protecting Plum's confidential information, then by signing this DPA, Customer agrees that it will not disclose the contents of this DPA to any third party, except as required by law.

11.2 A provision regarding Plum's commitment to the confidentiality of the Customer's Personal Data is also included in Appendix 1 to the Standard Contractual Clauses.

**12. Consent to Plum's Use of Sub-Processors**

12.1 Customer agrees to Plum's use of Sub-Processors to fulfil the obligations described in this DPA. Plum informs its customers of the Sub-Processors it currently utilizes via a public list and description of Sub-Processors found on Plum's Privacy Policy which is available on Plum's website. In the event that Plum ceases to work with one or more of the Sub-Processes listed, or engages with a new Sub-Processor, this list will be updated promptly. If Customer has any issues or questions about any of the Sub-Processors used by Plum, Customer should notify Plum immediately.

12.2 In signing this DPA, Customer consents to Plum's use of Sub-Processors as described in Section 12.1. In the event that Customer objects to any changes regarding the Sub-Processors that Plum chooses to work with, Customer has the right to object to the changes.

**13. Entire Agreement; Conflict**

Except as amended by this Addendum, the Principal Agreement will remain in full force and effect. If there is a conflict between the Principal Agreement and this addendum, the terms of this Addendum will control.

The parties' authorized signatories have duly executed this DPA:

**PLUM VOICE**

Signature: _____

Print Name: _____

Title: _____

Date: _____

**CUSTOMER**

Signature: _____

Print Name: _____

Title: _____

Date: _____

## Appendix A

### Standard Contractual Clauses (Processors)

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

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

and

Plum Voice

Address: HQ– 131 Varick St #934, New York, NY 10013

(the data **importer)**

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

Have both agreed on the following Contractual Clauses in order to ensure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the Personal Data specified Appendix 1 to the Standard Contractual Clauses.

Background

The data exporter has entered into a Data Processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of Personal Data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the Processing of Personal Data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

*Clause 1*

***Definitions***

For the purposes of the Clauses:

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

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

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

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

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

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

*Clause 2*

***Details of the transfer***

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

*Clause 3*

***Third-party beneficiary clause***

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

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

rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

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

*Clause 4*

***Obligations of the data exporter***

The data exporter agrees and warrants:

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

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

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

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

*Clause 5*

***Obligations of the data importer[2]***

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before Processing the Personal Data transferred;

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

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

  (ii) any accidental or unauthorised access, and

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

(e) to deal promptly and properly with all inquiries from the data exporter relating to its Processing of the Personal Data subject to the transfer and to abide by the advice of the Supervisory Authority with regard to the Processing of the data transferred;

(f) at the request of the data exporter to submit its data Processing facilities for audit of the Processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professionals, as important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Supervisory Authority;

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

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

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

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

*Clause 6*

***Liability***

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

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

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

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

*Clause 7*

***Mediation and jurisdiction***

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

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

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

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

*Clause 8*

***Cooperation with supervisory authorities***

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

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

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

*Clause 9*

***Governing Law***

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

*Clause 10*

***Variation of the contract***

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

*Clause 11*

***SubProcessing***

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

the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

*Clause 12*

***Obligation after the termination of Personal Data Processing services***

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

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

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Roles of the Parties**:

**Data exporter**

The data exporter is the entity identified as "Customer" in the DPA.

**Data importer**

The data importer is Plum Voice.

**Data subjects**

Data subjects include the data exporter's customers and end-users.

**Types of Data Processed**:

**Subject Matter/Categories of data**

Examples of the subject matter/categories of data that may be processed are listed below.

Data exporter may submit Personal Data to Plum, the extent of which is determined and controlled by the data exporter, as the Controller of the information, in its sole discretion.

The Personal Data transferred may include, but is not limited to the following:

- First and Last Name;
- Location Data;
- Employer/Company Name;
- Cardholder Data;
- Email Address;
- Business Address; and
- Phone Number

**Special categories of data**

Plum does not knowingly Process Personal Data that falls within the "Special Categories" of Personal Data as defined in Art. 9 of the GDPR.

**Purpose/Nature of the Processing**:

The purpose of the Processing is to carry out Plum's responsibilities to Customer as outlined in the Principal Agreement.

The nature of the Processing is outline below:

**Processing operations**

The Personal Data Processed will be subject to the following basic Processing activities:

- Transmission of Personal Data for use by Customer

**Duration of Processing**
The Duration of Processing will not exceed the "Term" outlined in the Principal Agreement.

**<u>Confidentiality and Rights of the Data Subject</u>**:

**Confidentiality**
Plum ensures that its personnel that is authorized to Process Personal Data is committed to the confidentiality of that Personal Data, and is adequately informed of that responsibility.

**Responding to Data Subject Requests**
In the event that Plum receives a Data Subject request as outlined in Clause 5(d)(iii) of the Standard Contractual Clauses, and taking into account the specific nature of the Processing that Plum is carrying out on behalf of the Customer, and the information available to Plum regarding the request, Plum agrees to assist the Customer with responding to the request, and with ensuring compliance with related GPDR provisions via appropriate technical and organizational measures, as reasonably possible.

**Responding to Data Breaches**
In the event that Plum is involved in a Breach of Customer's Personal Data, Plum will promptly notify Customer of the Breach as required by the timing requirements in Article 33 of the GDPR, and will take reasonable steps to cooperate with the Customer in its investigations into and response to the Breach, as required under Article 28 of the GDPR.

**Cooperation with Customer Assessments**
In the event that Customer is required to carry out an assessment, audit, or inspection, such as a Data Protection Impact Assessment (DPIA), as described in Article 35 of the GDPR, Plum agrees to cooperate and participate as needed and required under the GDPR with carrying out the required activity, as reasonably possible.

**Cross-Border Transfers**
As required under Article 28 of the GDPR, Plum will not transfer Customer's Personal Data outside of the EEA without permission of the Customer. The signing of this DPA will indicate that permission is granted to Plum for this purpose, when necessary to carry out its Processing responsibilities.

**DATA EXPORTER**

Name:……

Authorised Signature ……

**DATA IMPORTER**

Name:……

Authorised Signature ……

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses, and must be completed and signed by the parties. By signing the signature page on page 14 attached to Appendix 1, the parties will be deemed to have signed Appendix 2 of this DPA.

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

Data Importer will maintain the administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data processed by Plum, as described throughout the DPA.