Genesys Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into by and between [Genesys Legal Entity] and the Customer specified below, as of the date last executed by the parties. This Addendum adds to, and is governed by, the Master Agreement (as defined below).

Genesys	**Customer**
Pointillist, Inc.	[Customer]
321 Summer Street	[Customer Address]
Boston, MA 02210	
DataPrivacy@genesys.com	[Customer email]
[Genesys Signature]	[Customer Signature]

[Genesys Signatory] Authorized Representative's Name	[Customer Signatory] Authorized Representative's Name
[Genesys Signatory Title] Title	[Customer Signatory Title] Title
[Month Day, Year]	[Month Day, Year]

TERMS

1. **DEFINITIONS**

a. ***In General.*** Capitalized terms used in this DPA but not defined herein shall have the meaning given to them in the Master Agreement or the Privacy Legislation.

b. ***Affiliates*** means a business entity that: (a) Controls the party; (b) is Controlled by the party; or (c) is under common Control with the party, but only during the time that such Control exists. For the purposes of this definition, "Control(led)" is the ability to determine the management policies of an entity through ownership of a majority of shares or by control of the board of management.

c. ***Controller Instructions*** means instructions from the entity acting as the controller.

d. ***Customer*** means the customer receiving Genesys Services and any of its Affiliates.

e. ***Customer Data*** means the personal data (as defined in the Privacy Legislation) that is uploaded to the Service by Customer or an entity acting on behalf of Customer.

f. ***EEA*** means the European Economic Area.

g. ***Master Agreement*** means the agreement executed by Genesys and the Customer for the provision of Services.

h. ***Privacy Legislation*** means: (i) Regulation (EU) 2016/679 (the "***General Data Protection Regulation***" or "***GDPR***"); (ii) The amended version of the UK's DPA 2018 (UK GDPR); (iii) the California Consumer Privacy Act; (iv) and any further applicable national and international privacy and data protection legislations and regulations, as such legislations and regulations are amended, extended and re-enacted from time to time.

i. ***Service(s)*** means the software, cloud services, professional services, and customer care services provided by Genesys to the Customer, which process is further described in the Master Agreement.

j. ***Subsequent Subprocessor*** or ***Subprocessor*** means any subsequent sub-processor engaged by Genesys who agrees to process Customer Data on behalf of Genesys in accordance with: Controller Instructions, this DPA, or the Master Agreement.

k. ***Standard Contractual Clauses*** means Attachment 1 to this DPA, pursuant to the European Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries.

2. **DATA PROCESSING**

a. ***Scope.*** This DPA governs the processing of Customer Data by Genesys as a processor.

b. ***Term.*** This DPA shall remain in force from when it is duly executed by Genesys and the Customer until further notice, however at least as long as Genesys receives Controller Instructions for the provision of Services. This DPA shall be coterminous with the Master Agreement.

c. ***Compliance with Laws.*** Each party will comply with all laws, rules, and regulations applicable to it. Where Genesys has any reason to believe that the legislation applicable to it and any Subsequent Subprocessor, prevents them from fulfilling the Controller

Instructions and its respective obligations under this DPA and the sub-processing agreements, Genesys shall, upon becoming aware of such fact, promptly inform the Customer of such fact, as soon as it is aware about it. In such a case, the Customer is entitled to suspend the transfer of Customer Data or terminate this DPA.

d. ***Instructions for Data Processing.*** Genesys will process Customer Data in compliance with the Controller Instructions, this DPA, and the applicable Privacy Legislation. To ensure compliance with its own data protection obligations pursuant to applicable Privacy Legislation, the Customer will first use the functions of the platform provided by Genesys. If Customer cannot redress an action required by applicable Privacy Legislation with those tools or functions provided by Genesys, Customer is entitled to give detailed instructions to Genesys. The Customer will immediately confirm oral instructions regarding privacy either via a support care ticket or an email to DataPrivacy@Genesys.com. If Controller Instructions are given under this DPA, Genesys will document it for the duration of the DPA to ensure the accountability principle of the applicable Privacy Legislation.

e. ***Access or Use.*** Genesys will not access or use Customer Data except as necessary to provide the Service or in compliance with Controller Instruction.

f. ***Disclosure.*** Genesys will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Genesys a demand for Customer Data, Genesys will attempt to redirect the law enforcement agency to request that data directly from the applicable Customer. As part of this effort, Genesys may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Genesys will promptly notify the applicable Customer to allow it to seek a protective order or other appropriate remedy unless Genesys is legally prohibited from doing so. Genesys will also promptly notify the applicable Customer about any accidental or unauthorised access.

g. ***Genesys Personnel.*** Genesys personnel may not process Customer Data without proper internal authorization. All Genesys personnel receive data security and privacy training on an annual basis and have agreed to appropriate confidentiality obligations (for the term of their employment and thereafter), insofar as they are not already bound to do so in accordance with relevant legislations and regulations.

h. ***Data Controls.*** Insofar as a Data Subject contacts Genesys directly concerning a rectification, erasure, or restriction of processing, Genesys will promptly notify the Customer about the Data Subject's request. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by Genesys without unreasonable delay, or Genesys will provide tools for Customer to fulfil such requests via the Service including, without limitation: (a) to provide Customer with a copy of the Customer Data in tangible form; and (b) to access, correct, erase Customer Data or restrict processing of Customer Data as requested by the Data Subject.

i. ***Transfers of Customer Data.*** Customer authorizes Genesys to transfer Customer Data to countries outside of the EEA as set forth in Attachment 2. The Customer is responsible for ensuring it has authorization for such transfers. Genesys will provide notice to Customer of additional transfers.

   i. Where the Customer authorizes Genesys to, where necessary, transfer any Customer Data to a country or territory outside the EEA, the Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the applicable Privacy Legislation).

   ii. The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Genesys warrants that any Customer Data transferred to a country or territory outside the EEA shall meet the adequate level of data protection as required by the applicable Privacy Legislation.

j. ***Deletion and Return of Customer Data.***

   i. On termination of this DPA, Genesys and its Subprocessors shall, at the choice of the Customer: (a) return all the Customer Data processed by Genesys or any Subsequent Subprocessor and the copies thereof directly to the Customer or (b) delete all the Customer Data and provide notice to the Customer that it has done so.

3. **RESPONSIBILITIES OF GENESYS**

a. ***DPO.*** Genesys has appointed a Data Protection Officer in accordance with the applicable Privacy Legislation. Genesys has appointed Mr Shahzad Muhammad Naveed AHMAD, VP Cloud Competence Center & Data Privacy EMEA, office phone +44 (0)1753418818, mobile: +447717861224, email address: Shahzad.Ahmad@Genesys.com as Data Protection Officer. The Customer shall be informed as soon as possible of any change of Data Protection Officer.

b. ***Security.***

   i. *Security Procedures.* Genesys shall establish security procedures in accordance with applicable Privacy Legislation. The measures to be taken are appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. Genesys has taken into account the state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons. Please refer to Appendices for details.

ii. *Technical and Organizational Measures.* Genesys has implemented appropriate technical and organizational measures to maintain and protect the security of its facilities and networks as set forth in the Appendices and in accordance with the applicable Privacy Legislation. The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Genesys to implement alternative adequate measures, provided such changes do not reduce the security provided. Substantial changes will be documented. Genesys warrants that it and any Subsequent Subprocessors provide sufficient guarantees in respect of the technical and organisational security measures specified in this DPA and in accordance with the applicable Privacy Legislation.

iii. *Review of Genesys Security.* The Customer is solely responsible for reviewing the information made available by Genesys relating to data security and making an independent determination as to whether the Services meet Customer's requirements and for ensuring that the Customer personnel and consultants follow the guidelines that are provided regarding data security.

c. ***Other Responsibilities.***

i. Genesys shall deal promptly and properly with all inquiries from the Customer, relating to the processing of Customer Data, and to abide by the advice of the data protection supervisory authority competent according to the applicable Privacy Legislation.

ii. Genesys shall provide all information, documentation and assistance necessary for the Customer to meet all the requirements of applicable Privacy Legislation and to demonstrate compliance with such requirements.

iii. Genesys shall maintain and keep available up to date records on processing activities including the name, contact details, representative (including data protection officer, if applicable) and domicile of each legal entity acting as data sub-processor, the categories of processing carried out on behalf of Customer and, where applicable, the occurrence of International Data Transfers (including identification of the country/ies involved and documentation regarding applicable transfer mechanisms). Genesys shall, upon Customer's request and without undue delay, provide the documentation set out in this section in order for the Customer to comply with the applicable Privacy Legislation.

4. **AUDITS**

a. ***Audits.*** At least annually, Genesys uses external auditors to assess security measures for Multicloud and Genesys Cloud. These audits are performed by an independent third party who produces an audit report ("**Reports**"). The Reports are Genesys Confidential Information. Report summaries will be made available to Customer subject to a mutually agreed upon non-disclosure agreement ("**NDA**"). At Customer's written request, Genesys will provide Customer with a Report summary so that Customer can reasonably verify Genesys' compliance of the assessed platform(s) with the security obligations under this DPA.

b. Genesys will make available to the Customer all information necessary to demonstrate compliance with the obligations that are set out in applicable Privacy Laws. At the Customer's request, Genesys will also permit and contribute to audits of the processing activities covered by this DPA. The scope of such audits will be limited to Genesys and Genesys Affiliates and excludes personal information of any other Genesys customer. Audits shall be subject to reasonable advance notification, and agreement of Genesys. Such audits must not interrupt Genesys' business and may be carried out either by the staff of the entity making the audit request or by a professional third party contracted by the party making the audit request, provided that such contracted third party has entered into confidentiality obligations reasonably acceptable to Genesys. The party conducting the audit shall bear its own costs for audits. Such audits will incur time and material fees for party conducting the audit.

c. Genesys agrees that the Data protection supervisory authority competent for the has the right to conduct an audit of Genesys and of any Subsequent Subprocessor which has the same scope and is subject to the same conditions as would apply to an audit of the Customer under the applicable Privacy Legislation.

5. **SECURITY BREACH NOTIFICATION**

a. ***Notification.*** Where Genesys or any Subsequent Subprocessor engaged by it fails to fulfil their obligations, Genesys shall promptly inform the Customer of such fact, as soon as it is aware about it. In such case, the Customer is entitled to suspend the transfer of Customer Data or terminate this DPA. Where Genesys or any Subsequent Subprocessor fails to fulfil its data protection obligations under this DPA, any sub-processing agreement or any applicable Privacy Legislation, Genesys shall remain fully liable to the Customer for the performance of its and its Subprocessor's obligations under this DPA and such sub-processing agreement.

Genesys will assist the Customer in complying with the reporting requirements for data breaches. These include:

i. The obligation to report a personal data breach without undue delay to the Customer. The parties are aware that data protection requirements impose a duty to inform in any event of the loss or unlawful disclosure of personal data or access to it. Such incidents should therefore be communicated without undue delay to the Customer. Genesys will take appropriate measures to secure the data and limit any possible detrimental effect on the data subjects. Where Customer is obligated under applicable law to notify a government authority, Genesys is obliged to assist the Customer in preparing such notification.

ii. The duty to assist the Customer to provide information to the Data Subject concerned, if required by the applicable Privacy Legislation, and to provide the Customer with all relevant information in this regard as soon as reasonably possible.

6. **SUBPROCESSING**

a. ***Subprocessors.*** Genesys may transfer data to its Affiliates and hire other companies to provide limited services on its behalf, such as assisting customer support. Any such Affiliates and Subprocessors will be permitted to obtain Customer Data only to deliver the services Genesys has retained them to provide, and they are prohibited from using Customer Data for any other purpose. Genesys shall make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Customer Data, even in the case of outsourced ancillary services.

b. ***Third Party Services.*** The Genesys Services can function in coordination with various third-party services (for example, the Genesys Cloud AppFoundry). If Customer uses a third-party service that integrates with Genesys Services, Customer is responsible for ensuring proper data privacy terms, international transfer mechanisms, and service terms and conditions (for example, customer care & professional services) are in place with that third-party.

c. ***Current Subprocessors.*** Customer agrees that Genesys may use Subprocessors to provide the Services and meet other contractual obligations. An up-to-date list of Genesys Subprocessors is attached hereto as Attachment 2 ("Subprocessor List"). Customer consents to Genesys' such use of Subprocessors. At least 30 days prior to engaging a new Subprocessor, Genesys will update the Subprocessor List and notify the Customer. Customer acknowledges that it is the Customer's responsibility to provide any necessary notice to Customers regarding changes in Genesys Subprocessors. Customer may object to a new Subprocessor, on its own behalf or on behalf of the Customer, by contacting DataPrivacy@genesys.com. Note that such object may limit the availability of some features in the Genesys Services.

7. **FINANCIAL INSTITUTIONS**

a. ***Applicability.*** This Section 7 applies only where: (a) Customer is an institution as defined in Article 4(1)(3) of Regulation (EU) No 575/2013 or otherwise subject to the EBA.REC/2017/03, or (b) Customer uses the Genesys Services for purposes that are subject to regulatory oversight by EEA authorities (including BaFin) with authority to regulate Customers financial service activities.

b. ***Access and Audit.*** Genesys agrees to provide the Customer and the Customer's statutory auditor with: (a) full access to its business premises, and (b) rights of inspection and auditing related to the Genesys Services. The following conditions apply:

i. The Customer will exercise such rights in a risk-based and proportional manner considering the nature of the Genesys Services.

ii. The Customer may appoint a third party to perform such audits, provided that Customer can verify the third-party has the necessary skills and knowledge to perform the audit effectively.

iii. The Customer must provide written notice in a reasonable time period prior to an on-site visit.

iv. If Customer's audit rights could risk another Genesys customer's data or services, Genesys and the Customer will agree on an alternate means to provide necessary assurances.

v. When possible, the Customer will rely on certifications, reports, and attestations in place of an audit.

c. Genesys Outsourcing. Genesys will enter into written agreements with any Subprocessors that contain obligations and restrictions substantially similar to those found herein.

8. **NONDISCLOSURE**

Confidential Information. Both parties agree that, subject to applicable Privacy Legislation, the contents of this DPA are Confidential Information. Notwithstanding the above, this DPA may be disclosed to the Customer and a Subprocessor. Genesys shall keep Customer Data confidential and ensure that all persons authorised to process Customer Data are informed of the confidential nature thereof, have received appropriate training on their responsibilities and have committed themselves to confidentiality or are under an appropriate statutory obligations of confidentiality. It is expressly understood that such confidentiality obligations shall survive the termination of this DPA or the Master Agreement.

9. **GOVERNING LAW**

This DPA shall be governed by the law of the Member State in which the Customer is established.

10. **ENTIRE AGREEMENT; CONFLICT**

Entire Agreement; Conflict. Except as amended by this DPA, the Master Agreement will remain in full force and effect. If there is a conflict between the Master Agreement and this DPA, the terms of this DPA will control.

Attachments:

- **Attachment 1:** Standard Contractual Clauses (SCC)
- **Attachment 2:** Genesys Subprocessors
- **Attachment 3:** Data Processing Description
- **Attachment 4:** Genesys Security Measures

Attachment 1 –

INTRA-EU STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

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

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c)The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d)The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a)GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b)Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d)The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a)Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b)The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b)The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c)In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1)the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2)the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679/.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

A. LIST OF PARTIES

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

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date: …

   Role (controller/processor): …

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Genesys Cloud Services B.V., and on behalf of its Genesys Affiliates
   Address: Prins Bernhardplein 200, 1097 JB Amsterdam, The Netherlands

   Contact person's name, position and contact details: William Dummett, Chief Privacy Officer. Shahzad Ahmad, Data Privacy Officer. DataPrivacy@genesys.com…

   Activities relevant to the data transferred under these Clauses: Provision of services per the services agreement

   Signature and date: …

   Role (controller/processor): processor

2. …

B. DESCRIPTION OF TRANSFER

See Attachment 3

C. COMPETENT SUPERVISORY AUTHORITY

Netherlands

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Attachment 4

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

See Attachment 2

Attachment 2 - Genesys Subprocessors

Genesys Cloud services are hosted by third party data center providers. Premise services operate on systems controlled and operated by the Customer. Genesys may share personal data with any affiliated Genesys entities under common control with Genesys for troubleshooting and support. Genesys may utilize subprocessors, depending on what services, features, and functionality the customer utilizes. Additional subprocessors may be selected by Customer in a customized environment, and if so such subprocessor will be listed in a Statement of Work or Order Form. Customer acknowledges that signature of such Statement of Work or Order form constitutes written consent for use of such subprocessor named therein. Note that third party integrations, such as AppFoundry, require a direct relationship between the third party and the customer.

The subprocessors listed at the following website (along with its subsidiary companies) may be utilized, depending on what services and functionality is selected by the Customer. Customer acknowledges that changes to this website shall constitute notice of changes to subprocessors.

https://help.mypurecloud.com/articles/genesys-subprocessors/

Further, the Pointillist services use the following subprocessors:

Subprocessor	Region	Website	When Applicable	Services
Amazon Web Services, Inc.	In region (data center region selected by customer)	http://www.amazon.com	All Pointillist customers	Data Center and cloud computing services
Atlassian	Various regions available (US, Germany, Ireland)	www.atlassian.com	All Pointillist customers	Jira Cloud
AT&T Cybersecurity (formerly Alienvault)	Various regions available (US, Germany, Ireland)	https://cybersecurity.att.com/	All Pointillist customers	Cybersecurity services

Attachment 3 - Data Processing Description

Nature and Purpose of Processing

Genesys will process Customer Data pursuant to the Master Agreement, as further specified in the Documentation, and as further instructed by Controller Instructions.

Duration of Processing

Subject to the DPA, Genesys will process Customer Data for the duration of the Master Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

The Customer Data is processed to the extent determined and controlled by Controller Instructions, and may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

Type of Personal Data

The Customer Data is processed to the extent of which is determined and controlled by Controller Instructions, and may include but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data
- Other categories of data as customized by the Data Controller

Attachment 4 - Genesys Security Measures

Genesys Minimum Security Controls

This Appendix describes the minimum-security requirements generally applicable to Customer's use of Genesys Services. Additional controls for specific services or modules can be found in the applicable licensing agreement. Considering 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, Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Therefore, Processor will use necessary reasonable technical, organizational and security measures designed to protect personal Data of Customer in possession of Processor or otherwise processed by Processor against unauthorized access, alteration, disclosure or destruction, as further described in this Appendix:

1. **Security Program**

We have implemented and will maintain an information security program that follows generally accepted system security principles embodied in the SOC-2 standard designed to protect the Customer Data as appropriate to the nature and scope of the Services provided. The information security program includes at least the following elements:

a. **Security Awareness and Training**

We have implemented and maintain an information security and awareness program that is delivered to employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass. Additionally, development staff members are provided with secure code development training.

b. **Policies and Procedures**

We maintain policies and procedures to support the information security program. Policies and procedures are reviewed annually and updated as necessary.

c. **Malware Prevention**

We use industry standard practices to avoid the inclusion of any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) in applications running within Genesys services.

2. **Network Security**

Genesys will employ effective network security controls based on industry standards to ensure that Customer Data is protected.

3. **User Access Control**

Genesys will implement appropriate access controls to ensure only authorized users have access to Customer Data.

4. **Business Continuity and Disaster Recovery**

Genesys will maintain a corporate business continuity plan designed to ensure that ongoing monitoring and support services will continue in the event of a disruption event involving the corporate environment.

5. **Security Incident Response**

We maintain a Security Incident response program based on industry standards designed to identify and respond to suspected and actual Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

.

Pointillist by Genesys Cloud Services

These security terms for Pointillist by Genesys Cloud Services ("Cloud Security Terms") are incorporated by this reference into this Agreement with Genesys or its Affiliate, Pointillist, Inc. (hereinafter, "Genesys"), and describe the contractual requirements for information security provided by Genesys to Customer related to the provision of Cloud Services that Customer has licensed from Genesys pursuant to this Agreement. These terms are applicable to the extent that Genesys has access and control over Customer Data.

1. Security Program

1.1. Security Standards. Genesys has implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect Customer Data, as appropriate to the nature and scope of the Cloud Services provided.

1.2. Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass. Specifically, with regard to Customer Data access, this includes annual compliance, information security, privacy, HIPAA security & privacy, and PCI training. Access to Genesys' code repository requires additional annual training in secure development.

1.3. Policies and Procedures. Genesys will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated as necessary.

1.4. Change Management. Genesys will utilize a change management process based on Industry Standards to ensure that all changes to the Cloud Services environment are appropriately reviewed, tested, and approved.

1.5. Data Storage and Backup. Genesys will create backups of critical Customer Data. Customer Data will be stored and maintained using cloud provider-based Server-Side Encryption (SSE). Backup data will not be stored on portable media. Customer Data backups will be protected from unauthorized access.

1.6. Anti-virus and Anti-malware. Industry Standard anti-virus and anti-malware protection solutions are used on systems commonly affected by malware to protect the infrastructure that supports the Cloud Services against malicious software, such as Trojan horses, viruses, and worms. Genesys deploys File Integrity Management (FIM) solutions on all production systems, as well as robust monitoring of system access and command use. Cloud Services server instances are primarily Linux, which is a system not commonly affected by malware. Where Windows-based server instances are used, Industry Standard anti-malware software is deployed.

1.7. Vulnerability and Patch Management. Genesys will maintain a vulnerability management program that ensures compliance with Industry Standards. Genesys will assess all critical vulnerabilities to the Cloud Services production environment for access/vector complexity, authentication, impact, integrity, and availability. If the resulting risk is deemed to be "Critical" to Customer Data by Genesys, Genesys will endeavor to patch or mitigate affected systems within 7 working days. Certain stateful systems cannot be patched as quickly due to interdependencies and customer impact but will be remediated as expeditiously as practicable.

1.8. Data Deletion and Destruction. Genesys will, and will ensure that subprocessors will, follow Industry Standard processes to delete obsolete data and sanitize or destroy retired equipment that formerly held Customer Data. Recording retention policies are determined by Customer and can be used as part of a routine deletion process for recorded interactions. For instance, a recording retention policy can be created to delete conversations that occurred within a range of dates. All deletion within the Cloud Services is a simple deletion. Secure data deletion is not applicable in a virtual disk environment.

1.9. Penetration Testing. On at least an annual basis, Genesys will conduct a vulnerability assessment and penetration testing engagement with an independent qualified vendor. Issues identified during the engagement will be appropriately addressed within a reasonable time-frame commensurate with the identified risk level of the issue. Test results will be made available to Customer upon written request and will be subject to non-disclosure and confidentiality agreements.

2. Product Architecture Security

2.1. Logical Separation Controls. Genesys will employ effective logical separation controls based on Industry Standards to ensure that Customer Data is logically separated from other customer data within Cloud Services environment.

2.2. Firewall Services. Genesys uses firewall services to protect the Cloud Services infrastructure. Genesys maintains granular ingress and egress rules, and changes must be approved through Genesys' change management system. Rulesets are reviewed semi-annually.

2.3. Intrusion Detection System. Genesys has implemented intrusion detection across the Cloud Services environment that meets PCI DSS requirements.

2.4. No Wireless Networks. Genesys will not use wireless networks within the Cloud Services environments.

2.5. Data Connections between Customer and the Cloud Services Environment. All connections to browsers, mobile apps, and other components are secured via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS v1.2) over public Internet (note some Cloud Voice telephony cannot be due to carrier limitations).

2.6. Data Connections between the Cloud Services Environment and Third Parties. Transmission or exchange of Customer Data with Customer and any Genesys vendors will be conducted using secure methods (e.g. TLS 1.2, HTTPS, SFTP).

2.7. Encrypted Recordings. Genesys encrypts call recordings and chat sessions. Customer may elect to implement Local Key Encryption and maintain Customer's own keys for voice and screen recordings. To the extent required by applicable law or Customer's policies, Customer is responsible for the content of recordings and ensuring PCI Sensitive Authentication Data is not recorded, using applicable security features or other tools made available by Genesys.

2.8. Encryption Protection. Genesys uses Industry Standard methods to support encryption, with AES and TLS 1.2. Digital Recording encryption is addressed in Sections 2.7 and 7.6.

2.9. Logging and Monitoring. Genesys will log security events from the operating perspective for all infrastructure providing the Cloud Services to Customer. Genesys will monitor and investigate events that may indicate a Security Incident or problem. Event records will be retained at least one year. Limited audit data is accessible to customers via the User Interface (UI) and Application Programming Interface (API).

3. User Access Control

3.1. Access Control. Genesys will implement appropriate access controls to ensure only authorized Users have access to Customer Data within the Cloud Services environment.

3.2. Customer's User Access. Customer is responsible for managing User access controls within the application. The Cloud Services application password requirements are configurable by Customer for minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. Genesys has a lockout period after several invalid attempts. Most Users experience a lockout period after 5 bad attempts, but Customer can automatically try again in 5 minutes. These settings are not configurable. Customer defines user names and roles in a granular access permissions model. Customer is entirely responsible for any failure by itself, its agents, contractors or employees (including without limitation all its users) to maintain the security of all usernames, passwords and other account information under its control. Except in the event of a security lapse caused by Genesys' gross negligence or willful action or inaction, Customer is entirely responsible for all use of the Cloud Services through Customer's usernames and passwords, whether or not authorized by Customer, and all charges resulting from such use. Customer will immediately notify Genesys if Customer becomes aware of any unauthorized use of the Cloud Services.

3.3. Genesys' User Access. Genesys will create individual user accounts for each of Genesys' employees that have a business need to access Customer Data or Customer's systems within the Cloud Services environment. The following guidelines will be followed regarding Genesys' user account management:

3.3.1. User accounts are requested and authorized by Genesys management.

3.3.2. Strong password controls are systematically enforced.

3.3.3. Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days and multi-factor authentication.

3.3.4. Session time-outs are systematically enforced.

3.3.5. User accounts are promptly disabled upon employee termination or role transfer that eliminates a valid business need for access.

4. Business Continuity and Disaster recovery

4.1. Disruption Protection. The Cloud Services will be deployed and configured in a high-availability design and will be deployed across separate Data Centers to provide optimal availability of the Cloud Services. The Cloud Services environment is physically separated from Genesys' corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the Cloud Services.

4.2. Business Continuity. Genesys will maintain a corporate business continuity plan designed to ensure that ongoing monitoring and support services will continue in the event of a disruption event involving the corporate environment.

4.3. Disaster Recovery. The Cloud Services platforms take advantage of the distributed nature of the infrastructure to enable full multi-site disaster recovery by operating in multiple availability zones ("AZ's"); distinct locations that are engineered to be

insulated from each other. Independent application stacks are run in multiple AZ's. In the event of the loss of a single AZ or data center, the remaining Cloud Services remain operational and are designed to auto-scale to replace the lost system capacity.

5. Security Incident Response

5.1. Security Incident Response Program. Genesys will maintain a Security Incident response program based on Industry Standards designed to identify and respond to Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

5.2. Notification. In the event of a Security Incident or other security event requiring notification under applicable law, Genesys will notify Customer within twenty-four (24) hours and will reasonably cooperate so that Customer can make any required notifications relating to such event, unless Genesys specifically requested by law enforcement or a court order not to do so.

5.3. Notification Details. Genesys will provide the following details regarding any Security Incidents to Customer: (i) date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions Genesys has already taken; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.

5.4. Ongoing Communications. Genesys will continue providing appropriate status reports to Customer regarding the resolution of the Security Incident and continually work in good faith to correct the Security Incident and prevent future such Security Incidents. Genesys will cooperate, as reasonably requested by Customer, to further investigate and resolve the Security Incident.

6. Data Center Protections. Genesys contracts with Data Centers for Platform as a Service (PaaS). Security and compliance certifications and/or attestation reports for Data Centers must be obtained directly from the Data Center. Data Center may require Customer to execute additional non-disclosure agreements.

7. Use of the Cloud Services

7.1. Use Restrictions. Customer will not, and will not permit or authorize others to, use the Cloud Services for any of the following: (i) to violate applicable law; (ii) to transmit malicious code; (iii) to transmit 911 or any emergency services (or reconfigure to support or provide such use); (iv) to interfere with, unreasonably burden, or disrupt the integrity or performance of the Cloud Services or third-party data contained therein; (v) to attempt to gain unauthorized access to systems or networks; or (vi) to provide the Cloud Services to non-User third parties, including, by resale, license, lend or lease.

7.2. Customer Testing Restrictions. Customer will not perform any type of penetration testing, Vulnerability Assessment, or Denial of Service attack on the Cloud Services production, test, or development environments.

7.3. Prohibited Use. Customer will use commercially reasonable efforts to prevent and/or block any prohibited use by Users.

7.4. Customer Safeguards. Customer will maintain a reasonable and appropriate administrative, physical, and technical level of security regarding its account ID, password, antivirus and firewall protections, and connectivity with the Cloud Services.

7.5. VoIP Services Lines. Customer shall maintain strict security over all VoIP Services lines. Customer acknowledges that Genesys does not provide Customer the ability to reach 911 or other emergency services, and Customer agrees to inform any individuals who may be present where the Cloud Services are used, or who use the Cloud Services, of the non-availability of 911 or other emergency dialing.

7.6. Security Features. If the Cloud Services will be used to transmit or process Personal Data, Customer will ensure that all Personal Data is captured and used solely via the use of security features made available by Genesys.

7.7. Recordings. Customer acknowledges that use of recordings is solely within Customer's discretion and control. Without limiting the foregoing: (i) Customer accepts sole responsibility for determining the method and manner of performing recording such that it is compliant with all applicable laws and for configuring and using the Cloud Services accordingly; and (ii) Customer shall ensure that recordings shall be made only for purposes required by and/or in compliance with, all applicable laws. Customer will ensure that: (a) recordings will not knowingly include any bank account number, credit card number, authentication code, Social Security number or Personal Data, except as permitted by all applicable laws; or (v) recordings are encrypted at all times. Customer shall not modify, disable, or circumvent the recording encryption feature within the Cloud Services.

8. Industry-Specific Certifications. Genesys security and operational controls are based on Industry Standard practices and are certified to meet the guidelines of SOC 2 Type 2 and HIPAA. Nevertheless, Customer is solely responsible for achieving and maintaining any industry-specific certifications required for Customer's business.

9. Audit. Subject to Genesys' reasonable confidentiality and information security policies, Customer or a qualified third party chosen by Customer, shall have the right, not more than once a year and upon thirty (30) days' written notice, to perform a security assessment of Genesys' compliance with the terms of these Cloud Security Terms, provided that Customer has demonstrated that it has a reasonable belief that Genesys is not in compliance. During normal business hours, Customer or its authorized representatives may inspect

Genesys policies and practices implemented to comply with these Cloud Security Terms, which may include a site visit and a review of reasonable supporting documentation, provided that Customer agrees that such right shall not include the right to on-site inspections or audits of any of Genesys' subcontractors, including Genesys' third-party hosting facilities and equipment. No such assessment shall violate Genesys' obligations of confidentiality to other customers or partners, or reveal Genesys' intellectual property. Any assessment performed pursuant to this Section shall not interfere with the normal conduct of Genesys' business. Genesys shall cooperate with any reasonable requests made by Customer during the course of such assessments. Genesys reserves the right to charge Customer a reasonable fee for Genesys' costs incurred (including internal time spent) in connection with any Customer assessments, whether the assessment was performed remotely or on-site.

10. **Privacy**. Genesys has developed and will maintain a privacy program designed to respect and protect Customer Data under Genesys control.