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**
[Genesys Legal Entity]	[Customer]
[Genesys Legal Entity Address]	[Customer Address]
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

STANDARD CONTRACTUAL CLAUSES – INTERNATIONAL TRANSFER

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union [3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the

breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

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

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes

prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to 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 sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with

the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country

to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of the Netherlands.

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: Gooimeer 6 – 02 1411 DD Naarden 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/

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 provides a number of solutions and configurations of its platforms. The following TOMs apply to the offer specified below. Anything not listed below are covered by the Genesys Minimum Security Controls. Note that any third-party product that is resold by Genesys or integrates with Genesys will have security controls specific to that third party.

Offer	Applicable TOMs
MultiCloud CX (fka Engage Cloud)	Cloud Services
MultiCloud Private Edition (fka Engage Premise)	Premise Support
PureConnect Cloud	PureConnect Cloud
PureConnect Premise	Premise Support
Genesys Cloud CX	Cloud Services
Predictive Engagement	Cloud Services
PureConnect Premise WhatsApp Hybrid PureConnect Premise with Cobrowsing	Premise Support for the PureConnect services, and Cloud Services for the Cobrowsing/WhatsApp integration
Genesys Hub	Genesys Minimum Security Controls
WEM 2.0	Cloud Services
Genesys DX (fka Bold360)	Genesys DX

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.

.

Cloud Services

These security terms for Cloud Services ("Cloud Security Terms") are incorporated by this reference into this Agreement with 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 endeavour 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 usernames 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 wilful 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 dialling.

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 PCI, SOC 2 Type 2, ISO 27001, 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.

PureConnect Cloud

This security policy describes the minimum requirements for information security and data protection provided by Genesys to Customer related to the provision of Genesys PureConnect Cloud Services under the Master Agreement. This security policy is applicable to the extent that Genesys has access and control over Customer Data. For the purposes of this Exhibit B, "Data Center" means a data center where Genesys houses servers and other components used to deliver the Genesys PureConnect Cloud Service.

1. SECURITY PROGRAM

1.1 Security Certifications. 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 the Customer Data as appropriate to the nature and scope of the Genesys PureConnect Cloud Services provided. Genesys has developed and will maintain an information security and awareness program that is delivered to all its 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.

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.

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 Customer's environment are appropriately reviewed, tested, and approved.

1.5 Data Storage and Backup. Genesys will create backups of critical Customer Data according to documented backup procedures. Customer Data will be stored and maintained solely on designated backup storage media within the Data Center(s). Backup data will not be stored on portable media. Customer Data stored on backup media will be protected from unauthorized access. Backup data for critical non-database production servers will be retained for approximately thirty (30) days. Backup data for critical production database servers and transactional data will be retained for a minimum of seven (7) days.

1.6 Anti-Virus and Anti-Malware Protection. Genesys will utilize industry standard anti-virus and anti-malware protection solutions to ensure that all servers in Customer's Genesys PureConnect Cloud Service environment are appropriately protected against malicious software such as trojan horses, viruses, and worms. The solution will be centrally managed and configured to ensure updates are applied in a timely manner. Genesys will use standard industry practice to ensure that the Genesys PureConnect Cloud Services as delivered to Customer does not include any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) that are designed to disrupt the proper operation of the Genesys PureConnect Cloud Services, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the Genesys PureConnect Cloud Services to be destroyed, damaged, or rendered inoperable. Customer acknowledge that the use of license keys will not be a breach of this section.

1.7 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. A cleansed version of the executive summary of the test results will be made available to Customer upon written request and will be subject to non-disclosure and confidentiality Master Agreements.

1.8 Vulnerability and Patch Management. Genesys will maintain a vulnerability management program based on industry standard practices that routinely assesses the Data Center environment. Routine network and server scans will be scheduled and completed on a regular basis. The scan results will be analyzed to confirm identified vulnerabilities, and remediation will be scheduled within a timeframe commensurate with the relative risk. Genesys will monitor a variety of vulnerability advisory services to ensure that newly identified vulnerabilities are appropriately evaluated for possible impact to the Genesys PureConnect Cloud Service. Critical and high-risk vulnerabilities will be promptly addressed following the patch management and change management processes.

1.9 Data Destruction. Genesys will follow industry standard processes for the secure destruction of Customer Data that becomes obsolete or is no longer required under the Master Agreement. Retired or decommissioned

equipment that formerly held Customer Data and is scheduled for destruction will be securely destroyed using a qualified vendor who will provide a certificate of secure destruction.

2 NETWORK SECURITY

2.1 Network Controls. Genesys will employ effective network security controls based on industry standards to ensure that Customer Data is segmented and isolated from other customer environments within the Data Center. Controls include, but are not limited to:

A) Segregated Firewall Services. Customer environments are segmented using physical and contextual firewall instances.

(B) Network-Based Intrusion Detection System (NIDS). Genesys has implemented industry standard network intrusion detection systems at Internet egress points across the Genesys PureConnect Cloud Service environment.

(C) No Wireless Networks. Wireless networks are not utilized within the Data Center environments.

(D) Data Connections between Customer and the Genesys PureConnect Cloud Service Environment. Genesys uses SSL/TLS or MPLS circuits to secure connections between browsers, client apps, and mobile apps to the Genesys PureConnect Cloud Service. Connections traversing a non-dedicated network (i.e., the Internet) will use SSL/TLS.

(E) Data Connections between Genesys PureConnect Cloud Service Environment and Third Parties. Transmission or exchange of Customer Data with Customer and any third parties authorized by Customer to receive the Customer Data will be conducted using secure methods (e.g., SSL/TLS, HTTPS, SFTP).

(F) Encrypted Recordings. Genesys encrypts call recordings and chat sessions. Customer may elect to implement a unique password, known only to Customer, to protect the encryption keys used to secure the call recordings and chat sessions.

(G) Encryption Protection. Genesys uses industry standard methods to support encryption. For asymmetric key encryption, Genesys uses RSA 2048-bit keys. For symmetric key encryption, Genesys uses AES-128-bit keys. For hashing, Genesys uses SHA1 and SHA2.

(H) Logging and Monitoring. Genesys will log security events from the operating perspective for all servers providing the Genesys PureConnect Cloud Service to Customer. Genesys will monitor and investigate events that may indicate a security incident or problem. Event records will be retained for ninety (90) days.

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 Genesys PureConnect Cloud Service environment.

3.2 Customer's User Access. Customer is responsible for managing user access controls within the application. Customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for its users. 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 Genesys PureConnect Cloud Service through its 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 Genesys PureConnect Cloud Service.

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

(A) User accounts are requested and authorized by Genesys management.

(B) Strong password controls are systematically enforced.

(C) Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days.

(D) Dormant or unused accounts are disabled after ninety (90) days of non-use.

(E) Session time-outs are systematically enforced.

(F) User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

4. BUSINESS CONTINUITY AND DISASTER RECOVERY

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

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 Genesys PureConnect Cloud Service will be deployed in a high-availability, geographically redundant design such that a disruption event at a single Data Center will trigger a system fail-over to the back-up Data Center to minimize disruption to the Genesys PureConnect Cloud Service. Customer is responsible for defining specific parameters regarding fail-over.

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 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.

5.2 Notification. In the event of a confirmed breach involving the unauthorized release or disclosure of Customer Data or other security event requiring notification under applicable law, Genesys will notify Customer within 36 hours and will reasonably cooperate so that Customer can make any required notifications in connection with such event, unless Genesys is specifically requested by law enforcement or a court order not to do so.

5.3 Notification Details. Genesys will provide the following details regarding the confirmed Security Incident to Customer: (i) date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions already taken by Genesys; (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, continually work in good faith to correct the Security Incident and to 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

6.1 Data Center Co-Location. Genesys contracts with third-party providers for Data Center colocation space. Data Center providers and related services are reviewed on an annual basis to ensure that they continue to meet the needs of Genesys and its customers. Each Data Center provider maintains certification based on their independent business models. Security and compliance certifications or attestation reports for the Data Center(s) relevant to Customer's Genesys PureConnect Cloud Service will be provided upon written request and may require additional non-disclosure Master Agreements to be executed.

6.2 Physical Security. Each Data Center is housed within a secure and hardened facility with the following minimum physical security requirements: (a) secured and monitored points of entry; (b) surveillance cameras in facility; (c) on-site access validation with identity check; (d) access only to persons on an access list approved by Genesys; (e) on-site network operations center staffed 24x7x365.

6.3 Environmental Controls. Each Data Center is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power, and redundant temperature and humidity controls.

7. RIGHT TO AUDIT

7.1 Customer or its designated representative will have the right to audit Genesys records and systems related to the performance of the Genesys PureConnect Cloud Service under this Master Agreement, upon thirty (30) business days' prior written notice. Genesys agrees to cooperate in good faith with Customer to determine and implement a mutually agreeable resolution to any significant concerns identified during any such audit. Any audits performed by Customer or its designated representatives under this Master Agreement will be conducted a maximum of one (1) time during any twelve (12) month period during which this Master Agreement remains in force. Audits will be conducted during normal business operating hours and will be conducted in a manner that minimizes any disruption to Genesys normal daily operations.

8, PRIVACY

8.1 Genesys has developed and will maintain a privacy program designed to respect and protect Customer Data under our control. Genesys will not rent, sell or otherwise share any Customer Data with outside parties. Customer Data will only be used or accessed for providing the Genesys PureConnect Cloud Service.

9. INDUSTRY SPECIFIC CERTIFICATIONS

9.1 Genesys security and operational controls are based on industry standard practices. Genesys will configure the solution and the Genesys PureConnect Cloud Service based on Customer's specifications as defined in a mutually agreed upon Statement of Work (SOW); however, Customer is solely responsible for achieving and maintaining any industry specific certifications required for its business (e.g., PCI DSS, HIPAA, GLBA, NIST 800-53, FedRAMP, etc.).

10. PREMIUM SERVICES

10.1 Additional Services. The standard security controls listed prior to this Section 10 meet industry standards and are sufficient for most customers. Customers requiring a higher level of assurance may need to contract for additional "Premium Services" as described in this Section 10. If an industry specific certification is required for Customer's business relative to the Genesys PureConnect Cloud Service, Customer agrees to contract for the additional "Premium Services" required to meet the industry specific certification. For an additional fee, Genesys will implement the following controls and procedures during the implementation period. The controls and procedures are designed to meet the certification requirements of certain industry standards (PCI DSS, HIPAA, etc.) where appropriate for Customer Genesys PureConnect Cloud Service environment within the Data Center. Additional controls may include, but may not be limited to:

(A) Remote Access. Genesys authorized employees and contractors will require two-factor authentication to access Customer's Genesys PureConnect Cloud Service environment within the Data Center.

(B) Vulnerability and Patch Management. Genesys will conduct quarterly vulnerability scans of Customer's Genesys PureConnect Cloud Service environment within the Data Center. Critical and high-risk vulnerabilities will be addressed, following the documented change management and patch management procedures. Medium and lower risk vulnerabilities will be remediated.

(C) Logging and Monitoring. Genesys will conduct reviews of infrastructure event logs daily. Identified issues and concerns will be risk ranked and addressed according to documented vulnerability management procedures. Certification Audits. Genesys will contract with qualified third-party assessors to conduct industry specific certification audits of the Genesys PureConnect Cloud Service within the Data Center. Certification audits will be conducted on an annual basis. The resulting certification or executive summary of the audit report will be provided to Customer upon written request. Genesys currently maintains PCI DSS 3.0 certification for a specific deployment model within the U.S. Data Centers located in Carmel, Indiana and Englewood, Colorado. PCI certification does not extend to any other Data Center.

GENESYS

Premise Support Security

This security policy describes the minimum requirements for information security and data protection provided by Genesys to Customer related to the provision of support for Genesys premises-based services under the Master Agreement. This security policy is applicable to the extent that Genesys has access and control over Customer Data.

1. SECURITY PROGRAM

1.1 Security controls. 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 the Customer Data as appropriate to the nature and scope of the services provided. Genesys has developed and will maintain an information security and awareness program that is delivered to all its 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.

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.

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 Customer's environment are appropriately reviewed, tested, and approved.

1.5 Anti-Virus and Anti-Malware Protection. Genesys will utilize industry standard anti-virus and anti-malware protection solutions to ensure that all servers in Genesys' environment are appropriately protected against malicious software such as trojan horses, viruses, and worms. The solution will be centrally managed and configured to ensure updates are applied in a timely manner. Genesys will use standard industry practice to ensure that the Genesys PureConnect Cloud.

1.6 Data Destruction. Genesys will follow industry standard processes for the secure destruction of Customer Data that becomes obsolete or is no longer required under the Master Agreement. Retired or decommissioned equipment that formerly held Customer Data and is scheduled for destruction will be securely destroyed using a qualified vendor who will provide a certificate of secure destruction.

2. USER ACCESS CONTROL

2.1 Access Control. Genesys will implement appropriate access controls to ensure only authorized users have access to Customer Data within Genesys' environment.

2.2 Genesys User Access. Genesys will create individual user accounts for each of its employees or contractors that have a business need to access Customer Data. The following guidelines will be followed regarding Genesys user account management:

(A) User accounts are requested and authorized by Genesys management.

(B) Strong password controls are systematically enforced.

(C) Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days.

(D) Dormant or unused accounts are disabled after ninety (90) days of non-use.

(E) Session time-outs are systematically enforced.

(F) User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

3. BUSINESS CONTINUITY AND DISASTER RECOVERY

3.1 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. SECURITY INCIDENT RESPONSE

4.1 Security Incident Response Program. Genesys will 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.

4.2 Notification. In the event of a confirmed breach involving the unauthorized release or disclosure of Customer Data or other security event requiring notification under applicable law, Genesys will notify Customer within 36 hours and will reasonably cooperate so that Customer can make any required notifications in connection with such event, unless Genesys is specifically requested by law enforcement or a court order not to do so.

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

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

GENESYS

Genesys DX Security

1. Products and Services

This document covers the security and privacy controls for Genesys DX. These products are live chat, omni-channel and conversational ai engagement services that help customer service staff directly engage with and assist visitors to their organization's website. Key features include conversation bots, real-time visitor monitoring, co-browsing, detailed reporting on chat activity and its overall effectiveness, the ability to define rules that automatically trigger the initiation of a live chat or bot engagements, the ability to route and distribute chats to improve efficiency, and the ability to monitor and manage customer conversations on various social channels, email and via SMS messages, knowledge management, and intent insights. Genesys DX offer multiple service tiers based on the number of engagements, users and features desired. Further, Genesys DX provides valuable built-in integrations and open APIs to allow customers to streamline operations with all of their systems working together.

2. Product Architecture

Genesys DX is a SaaS-based application delivered via a chat client and internet-based application server that writes to a database. The chat client functions inside the visitor's browser making https calls and maintaining a web socket connection to the application server. Agents connect using a .NET or web client over authenticated https to the same servers. Genesys Customer Content (as the term is defined in the Terms of Service) is processed on database servers and stored in an encrypted form.

2.1 Storage and Service

End-user interfaces traffic (incl. live chat with an agent) is handled by co-located servers with Equinix as well as on Amazon Web Services. Customers can choose to store their service in Europe, USA or India. Access to infrastructure is limited to authorized individuals of the Development Operations team.

According to customers geo-location, the Genesys DX ai Chatbot data center is handled by co-located servers with Equinix as well as on Amazon EC2 cloud within Europe, USA or India, and accessed by the Network Operations Team for support purposes with no access to customer content.

All touch points and APIs are processed by our application servers, that mediate access to storage servers which can only be accessed from within our secured network.

Our back-office management interface, hosted on co-location facilities with Equinix and Switch, is a secured and encrypted web console (using TLS and SSL encryption). Credentials are encrypted and use a strict password complexity policy to ensure only your authorized personnel can access your knowledge.

3. Genesys DX Technical Security Controls

Genesys employs industry standard technical controls appropriate to the nature and scope of the Services designed to safeguard the Service infrastructure and data residing therein.

3.1 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or “least privilege”) access to specified Genesys systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

Administrative controls set or restrict agent/user access to certain actions, setup areas, departments and folders.

The Genesys operational system is only accessible with an authorized username (or email) and password combination. Usernames (and emails) must be unique throughout the entire Genesys system, and minimum password length and complexity requirements are enforced. Enhanced password controls, including initial login reset, rotation, aging, non-reuse and incorrect password lockout, are available to administrators in the user configuration settings. Single Sign On (SSO) integration is available to Enterprise subscribers using SAML 2.0-compliant user management systems.

User logins to Genesys are logged and reported within the application. Access to these reports can be restricted using permission settings.

3.2 Perimeter Defense and Intrusion Detection

The Genesys on-premises and Genesys components and services running on third-party cloud providers' network architecture is segmented into public, private, and Integrated Lights Out (iLO) management network zones. The public zone contains internet- facing servers. All traffic that enters this network must transit a firewall. Only required network traffic is allowed; all other network traffic is denied, and no network access is permitted from the public zone to either the private or iLO management network zones.

The private network zone hosts application level administrative and monitoring systems, and the iLO management network zone is for hardware and network administration and monitoring. Access to these networks is restricted to authorized employees via two-factor authentication.

Moreover, Genesys employs perimeter protection measures, including a third party, cloud-based distributed denial of service (DDoS) prevention service, designed to prevent unauthorized network traffic from entering our product infrastructure.

3.3 Data Segregation

Genesys leverages a multi-tenant architecture logically separated at the database level, based on a user's or organization's Genesys account. Only authenticated parties are granted access to relevant accounts.

New Genesys customers can use the Data Residency Option to choose whether their Content will be stored in Genesys' on-premises United States or European data centers and third-party cloud providers' United States, European and Indian regions hosted and replicated in separate regions to meet cross-border data privacy and residency requirements.

3.4 Physical Security

Data center Physical Security

Genesys contracts with Data centers and third-party cloud providers to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation, and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant Data center
- Scheduled maintenance and validation of all critical security and environmental controls

Genesys and third-party providers limit physical access to production data centers to authorized individuals only. Access to an on-premises server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. Genesys management reviews physical access logs to on-premises data centers and server rooms on at least a quarterly basis. Additionally, physical access to data centers is removed upon termination of previously authorized personnel.

3.5 Data Backup, Disaster Recovery, Availability

Genesys has near instantaneous fail-over capabilities for most failure scenarios. The production Data centers utilize redundant high-speed network connections. There are pools of redundant servers across geographically distant data centers. Load balancers distribute network traffic among these servers and maintain the availability of these servers in the event of server or Data center failures.

The Genesys database is synchronized every five minutes to another data center. In addition, a differential back-up is completed nightly, and full backups are conducted every weekend. The backup database is stored with the same encryption as the original. Backups are retained on-premises for one week. In the event of a complete failure of the data center hosting the primary database, Genesys is designed to be restored within fifteen minutes.

3.6 Malware Protection

Malware protection software with audit logging is deployed on all Genesys servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.7 Encryption

Genesys maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant standards groups. This standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption

All network traffic flowing in and out of Genesys data centers, including all Customer Content, is encrypted in transit with 256-bit AES encryption.

At-Rest Encryption

Genesys encrypts all Customer Content at rest with 256-bit AES encryption.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

3.9 Logging and Alerting

Genesys collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4. Organizational Controls

Genesys operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of Genesys.

4.1 Security Policies and Procedures

Genesys maintains and implements a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

Genesys complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certifications and external audit reports:

- International Organization for Standardization – ISO/IEC 27001:2013 Information Security Management System (ISMS) Certification
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) Compliance for Genesys' eCommerce and Payment Environments

4.3 Security Operations and Incident Management

Genesys' Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with Genesys' critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including Genesys. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the Genesys intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

Genesys' application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modelling, static code analysis, dynamic analysis, and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

Genesys employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding kits, and awareness campaigns for securing data, devices, and facilities.

5. Privacy Practices

Genesys takes the privacy expectations of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Data Protection and Privacy Policy

Genesys is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs Genesys' processing of Personal Data as may be located within Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of Genesys' technical and organizational measures. Additionally, to account for CCPA coming into force, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that Genesys will not sell our users' 'personal information.'

For visitors to our webpages, Genesys discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.2 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. The Service is compliant with the applicable provisions of the GDPR.

5.3 CCPA

Genesys hereby represents and warrants that it will follow the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA.

5.4 Transfer Frameworks

Genesys is aware of the European Court of Justice's decision with respect to the EU-U.S. Privacy Shield Framework and is actively monitoring the situation.

Genesys' privacy program and contracts have been designed to account for shifts in the regulatory landscape to avoid impacts to our ability to provide our services to you. The EU-U.S. Privacy Shield Framework was just one (of several) mechanism that Genesys relied on to lawfully transfer personal data. Therefore, Genesys offer in the following Transfer Frameworks.

5.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law. Genesys has invested in a world-class data privacy program designed to meet

the exacting requirements of the SCCs for the transfer of personal data. Genesys offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope Genesys services as part of its global DPA. Execution of the SCCs helps ensure that Genesys customers can freely move data from the EEA to the rest of the world.

5.5 Return and Deletion of Customer Content

At any time, Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available or Genesys is otherwise unable to complete the request, Genesys will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request. Customer's Genesys Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Upon written request, Genesys will certify to such Content deletion.

5.6 Sensitive Data

While Genesys aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of Genesys for certain kind of information. Unless Customer has written permission from Genesys, the following data must not be uploaded or generated to Genesys:

- Government issued identification numbers and image of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. One exception extends to explicitly identified payment forms and pages that are used by Genesys to collect payment for Genesys. Another exception is that Genesys allows customers to maintain PCI-DSS compliance, while using Genesys to process payments, through a third-party gateway, contingent on Customer's appropriate configuration of their Genesys environment.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political believes, organizational memberships, etc.

5.7 Tracking and Analytics

Genesys is continuously improving its websites and products using various third-party web analytics tools, which help Genesys understand how visitors use its websites, desktop tools, and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy.

6. Third Parties

6.1 Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes.

Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by Genesys are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, Genesys reviews relevant third party's terms and conditions and either utilizes Genesys-approved procurement templates or negotiates such third-party terms, where deemed necessary.