Genesys Partner Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into by and between Genesys and the Partner specified in the Master Agreement (as defined below), as of the date last executed by the parties ("**Effective Date**"). This DPA adds to and is governed by the Master Agreement. This DPA is intended to cover data privacy and protection obligations of the parties in order to comply with various data privacy laws and regulations around the world.

Partner enters into this DPA on behalf of itself and in the name and on behalf of its Affiliates, to the extent Genesys processes Partner Data on behalf of such Affiliates as part of the Services. This DPA is presented online and incorporated by the terms and conditions specifically referencing this DPA.

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. Other terms not defined herein and related to the protection of personal data, including but not limited to those such as "**controller**"/"**business**," "**data subject**," "**personal data**," "**personal data breach**," "**processing**," "**processor**"/"**service provider**," and "**sensitive personal data**" shall have the meaning assigned to these and materially similar terms (e.g., personal information, (data) breach, etc.) in 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. ***Authorities*** means any law enforcement agency, government body, regulatory or supervisory authority, court, tribunal, or other public authority with jurisdiction or authority to enforce applicable laws and regulations.

d. ***Controller Instructions*** means instructions from the entity acting as the controller. For Personal Customer Data, Controller Instructions may come from the Customer or from the Partner. For Partner Data, Controller Instructions may come from the Partner. The End User License Agreement or End User Agreement, Master Agreement as well as the Customer DPA and the instructions provided by Customer through its use of the Services features shall constitute Controller instructions.

e. ***Customer*** means the customer and any of its Affiliates indirectly receiving Services, as a Partner's end user customer that has licensed or been granted access to use the Services pursuant to an End User License Agreement or End User Agreement.

f. ***Personal Customer Data*** means the personal data that is uploaded to the Service or otherwise disclosed to Genesys by Customer or an entity/person acting on behalf of Customer.

g. ***Customer DPA*** means the agreement concluded between the Customer as data controller and the Partner as processor regarding the processing of Personal Customer Data.

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

i. ***Master Agreement*** means (i) the Genesys Master Partner Network Agreement executed by Genesys and the Partner for the reselling of Services to a Customer, and (ii) any Services Order, Order, Order Form, Statement of Work (SOW), Supplemental Agreement, or other contract that forms part of (i).

j. ***Partner*** means the partner and any of its Affiliates reselling Services to Customers subject to a Master Agreement with Genesys.

k. ***Partner Data*** means the personal data that is uploaded to the Service or otherwise disclosed to Genesys by Partner or an entity/person acting on behalf of Partner. This excludes the Personal Customer Data that the Partner or an entity/person acting on behalf of Partner uploads to the Service or otherwise discloses to Genesys on behalf of the Customer.

l. ***Privacy Legislation*** means any legally binding federal, national, state, provincial, regional or local regulation, law, statute, rule or administrative order regulating any processing activities of

personal data insofar it is directly applicable to each party in its processing of Personal Customer Data or Partner Data under the Agreement, as well as any other applicable provisions replacing, supplementing, amending, extending, reconstituting, or consolidating them, which may include without limitation (any reference to a specific country's Privacy Legislation shall be interpreted as a reference to the respective Privacy Legislation):

i. Antigua and Barbuda's Data Protection Act, 2013;

ii. Argentina's Data Protection Act, 2000;

iii. Australia's Privacy Act 1988;

iv. Bahamas' Data Protection Act, 2003;

v. Barbados' Data Protection Act, 2019;

vi. Belize's Data Protection Act, 2021;

vii. Brazilian Data Protection Law (**LGPD**), 2018;

viii. Canadian Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5);

ix. Chile's Data Protection Act, 1999 and Law No. 21.719;

x. Colombia's Data Protection Act, 2012;

xi. Costa Rica's Law on the Protection of Persons Regarding the Processing of their Personal Data, 2011;

xii. Cuba's Law on Personal Data Protection, 2022;

xiii. Dominican Republic's On Protection of Data, 2013;

xiv. Ecuador's Organic Law on the Protection of Personal Data, 2021;

xv. El Salvador's Personal Data Protection Law, 2024;

xvi. Grenada's Data Protection Act, 2023;

xvii. Guyana, Data Protection Act, 2023;

xviii. India's Digital Personal Data Protection Act, 2023, as of date of entry into force, and Information Technology Act, 2011, as applicable;

xix. Israel's Protection of Privacy Law, 5741-1981;

xx. Jamaica, Data Protection Act, 2020;

xxi. EU General Data Protection Regulation 2016/679 (the "**GDPR**") and the EU Directive on privacy and electronic communications 2002/58/EC;

xxii. Malaysia's Personal Data Protection Act 2010;

xxiii. Mexico's Data Protection Act, 2010;

xxiv. New Zealand Privacy Act, 2020;

xxv. Nicaragua's Law on Personal Data Protection, 2012;

xxvi. Panama's Law's on Personal Data Protection, 2019;

xxvii. Paraguay's Law on the Protection of Personal Credit Data, 2020;

xxviii. Peru's Law on the Protection of Personal Data, 2011;

xxix. Philippines' Data Privacy Act of 2012;

xxx. Saint Kitts and Nevis, Data Protection Act, 2018;

xxxi. Saint Lucia's Data Protection Act, 2011 and Data Protection Amendment Act, 2015;

xxxii. Saudi Arabia's Personal Data Protection Law, 2021;

xxxiii. Suriname;

xxxiv. Singapore's Data Protection Act, 2012;

xxxv. South Africa's Protection of Personal Information Act (POPIA), 2013;

xxxvi. Swiss Federal Act on Data Protection 235.1 of 25 September 2020, and the Ordinance on the Federal Act on Data Protection 235.11 of 31 August 2022 ("**FADP**");

xxxvii. Thailand's Data Protection Act, 2019;

xxxviii. Trinidad and Tobago's Data Protection Act, 2011;

xxxix. Turkey Data Protection Act, 2016;

xl. UK's Data Protection Act 2018, and the GDPR, as incorporated into UK law as the UK GDPR ("**UK GDPR**");

xli. United Arab Emirates' Federal Decree-Law No. 45 of 2021;

xlii. Uruguay 's Data Protection Act, 2008;

xliii. United States federal, state, and local data protection laws and regulations, such as the California Consumer Privacy Act of 2018, and Gramm-Leach-Bliley Act (together "**US Privacy Legislation**").

m. ***Service(s)*** means the software, cloud services, professional services, and customer care services provided by Genesys indirectly to a Customer via Customer request to the Partner, as further described in the Master Agreement.

n. ***Subprocessor*** means any subsequent processor engaged by Genesys, which may include a Genesys Affiliate, who agrees to process Customer Data or Partner Data on behalf of Genesys.

o. ***Transfer Clauses*** means any contractual clauses required under Privacy Legislation to transfer personal data from one country to another and that are provided or referenced in Annex 4 to this DPA.

2. APPLICABILITY

a. ***Interplay with existing agreements.***

If the Partner signing this DPA is a party to the Master Agreement, this DPA is an addendum to and forms part of the Master Agreement. In such case, the Genesys entity that is party to the Master Agreement is party to this DPA.

If the Partner entity signing this DPA has executed an Order Form with Genesys or its Affiliate pursuant to the Master Agreement but is not itself a party to the Master Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Genesys entity that is party to such Order Form is party to this DPA.

If the Partner entity signing this DPA is neither a party to an Order Form nor the Master Agreement, this DPA is invalid and not legally binding. Such entity should request that the Partner entity who is a party to the Master Agreement execute this DPA on its behalf.

This DPA is not applicable to Customers. Such entity should contact the authorized reseller and refer to its Customer DPA.

This DPA shall not replace any comparable or additional rights relating to processing of Partner Data contained in Master Agreement.

b. ***Data Protection Roles.***

This DPA governs the processing of Partner and Personal Customer Data by Genesys, as set out in Annex 1 to this DPA, which acts respectively as a processor or a subprocessor. In the latter case, the Partner will seek the Customer's prior written authorization to allow the Partner to authorize Genesys to carry out the data processing services in conformity with the Customer DPA and the applicable Privacy Legislation.

The obligations under the Privacy Legislation shall apply to the parties to this DPA, in their respective roles as follows:

i. The Customer signing the Customer DPA acts as a controller, to the extent that the Customer determines the purposes of the processing of personal data in the context of its use of the Services and the essential means thereof and/or fulfils other mandatory conditions for acting as a controller under the applicable Privacy Legislation.

ii. The Partner signing this DPA acts as processor, to the extent it processes, on behalf of the Customer and under its Customer DPA and Controller Instructions, personal data necessary for the provision of the Services to the Customer. In such cases, Genesys acts as subprocessor when it processes, on behalf of the Partner and under the Controller Instructions provided by the Partner, the personal data necessary for provision of Services to Customer. Genesys Affiliates act as subsequent Subprocessors in the context of the provision of the Services to the Customer.

iii. Where the Partner processes personal data for purposes of the Partner Program, the Partner acts as a controller. In such cases, Genesys acts as a processor for such Partner Data.

3. **RIGHTS AND OBLIGATIONS**

a. ***Compliance* with laws.** Each party will comply with all Privacy Legislation applicable to it. Partner shall ensure that Partner Data disclosed to Genesys have been collected and can be processed through the Services in accordance with the Privacy Legislation, including by providing and collecting any required notices and consents. Where Genesys has any reason to believe that (i) the applicable Privacy Legislation prevents Genesys from fulfilling the Controller Instructions and its obligations under this DPA, or (ii) Controller Instructions fully or partially infringe the applicable Privacy Legislation, Genesys shall, upon becoming aware of it, promptly inform the Partner of such fact, as applicable.

b. ***Instructions for Data Processing.*** Genesys will process Personal Customer Data and Partner 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 Partner shall and shall be cause Customer to independently use the tools and functions provided by Genesys as part of the Services. Only if Customer or Partner cannot address a requirement under applicable Privacy Legislation with such tools or functions, Customer or Partner may request in writing reasonable assistance from Genesys. Such request must be sent to Genesys either via a support care ticket or an email to DataPrivacy@Genesys.com. If Controller Instructions are given under this DPA, Genesys will document them for the duration of the DPA in accordance with the accountability principle of the applicable Privacy Legislation.

c. ***Sensitive* Data.** Partner is solely responsible for alerting Genesys in writing as to (i) use of the Service by the Partner or the Customer involving sensitive personal data and/or personal data subject to particular heightened legal requirements, such as under sectoral legislation, and (ii) additional privacy and security measures that may be applicable to such personal data, which are not already included in the Services.

d. ***Genesys Personnel.*** Genesys personnel may not process Personal Customer or Partner 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.

e. ***Security.***

i. ***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 Annex 3 to this DPA. 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 materially reduce the security provided. Material changes will be documented.

ii. ***Review of Genesys Security***. The Partner 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 Partner and Customer requirements as well as applicable Privacy Legislation regarding Partner Data and Personal Customer Data. The Partner is solely responsible for ensuring that Partner and Customer personnel and consultants follow any end user security guidelines provided by Genesys.

f. ***Data Controls.*** Insofar as a data subject contacts Genesys directly concerning their Partner Data or Personal Customer Data rights under Privacy Legislation ("**Request**"), Genesys will promptly notify the Partner about such Request. Partner is solely responsible for communicating any such Requests to the Customer, as appropriate. As part of its Services, Genesys provides tools to Partner to help fulfil such Requests via the Services including, without limitation: (a) to provide a copy of the Partner Data or Personal Customer Data in a commonly used format; and (b) to access, correct, erase Partner Data or Personal Customer Data or restrict processing of Partner Data or Personal Customer Data as requested by the data subject. If the Partner cannot fulfil such requests using the tools provided on the Services, and insofar as it is included in the scope of Services, Genesys can assist Partner without unreasonable delay with the erasure, rectification, data portability and access Requests. Additional Genesys assistance with Requests fulfilment will be subject to additional fees at standard rates.

g. ***Assistance.*** To the extent these are not directly available to Partner, Genesys shall, upon request, provide the information, documentation and assistance reasonably necessary for the Partner to demonstrate compliance with the Privacy Legislation requirements. Assistance requested by the Partner beyond what is reasonably required under this DPA shall be subject to additional fees at standard rates.

h. ***Audits.*** Genesys will request independent external auditors to assess Cloud Security Terms (as defined below) and produce an audit report ("**Report**") annually, or as otherwise applicable subject to standard certification periods. The Report is Genesys Confidential Information. Genesys will make Report summaries available to the Partner or Customer upon written request and subject to a mutually agreed upon non-disclosure agreement. To the extent Partner discloses such Report summaries to the Customer, it shall ensure that the Customer executes an equivalent non-disclosure agreement. Upon Partner's written request (on its own, or on behalf of the Customer), Genesys will reasonably permit and cooperate with audits of the Partner Data or Personal Customer Data processing activities subject to this DPA. Such audits shall be subject to the conditions agreed upon by the parties with regards to auditing of Genesys security compliance under Section 16 of Cloud Security Terms set out in the Annex 3 to this DPA. Customer may participate in such audits to the extent it agrees to be bound by the same conditions as the Partner.

i. ***Deletion and Return of Partner and Personal Customer Data.***

i. ***Choice***. On termination of this DPA, and in any case no later than as reasonably necessary to accommodate standard Genesys and Subprocessor data and backup deletion cycles, Genesys shall at the choice of the Customer, regarding Personal Customer Data (that may be expressed on its behalf by the Partner) or Partner regarding Partner Data, as appropriate, delete or return directly to the Customer or Partner all the Personal Customer Data or Partner Data processed by Genesys and copies thereof, as appropriate. Notwithstanding the foregoing, Genesys may retain Personal Customer Data or Partner Data if necessary for compliance with applicable laws, provided that the retained Personal Customer Data or Partner Data will be securely processed in accordance with Annex 3 to this DPA until deleted or returned in accordance with this Section 3.i.i.

ii. ***Notice***. Upon Partner's request (on its own or on behalf of the Customer), Genesys shall confirm the deletion or return of Personal Customer Data or Partner Data.

j. ***Personal Data Breaches.***

i. ***Notification and Assistance***. Genesys will notify the Partner, as applicable, without undue delay after becoming aware of a personal data breach of Personal Customer Data or Partner Data. Genesys shall provide details regarding such

personal data breach and continue to provide ongoing communications in line with Section 14 of Cloud Security Terms set out in the Annex 3 to this DPA to the extent this is required for the Partner to fulfil its obligations under applicable Privacy Legislation and Partner cannot reasonably obtain such information on its own. If required by the applicable Privacy Legislation, Genesys will assist Customer or Partner in providing information to the data subject concerned. Partner acknowledges that it is the Partner's responsibility to provide any necessary notice and assistance to an Customer regarding personal data breach of Personal Customer Data, which Genesys notified to the Partner pursuant to this DPA.

ii. ***Mitigation***. Genesys will at its sole discretion take appropriate measures to address the personal data breach and secure any data it processes, as well as its systems and other assets, and limit any potential detrimental effects on the data subjects.

k. ***Subprocessing.***

i. ***Current Subprocessors.*** Partner authorizes Genesys to disclose Personal Customer Data or Partner Data to Subprocessors, as detailed in Annex 2 (Subprocessors) to this DPA, subject to contractual requirements providing personal data protections materially equivalent to those that Genesys has under this DPA, to provide or support Services and meet other contractual and legal obligations.

ii. ***Updates to the list of Subprocessor.*** At least 30 days prior to engaging a new Subprocessor, Genesys will update the list of Subprocessors and notify the Partner. Partner acknowledges that it is the Partner's responsibility to provide any necessary notice to Customer regarding changes in the list of Subprocessors. Within this period, the Partner may object to the new Subprocessor (on its behalf or on behalf of the Customer), by contacting DataPrivacy@genesys.com. The parties to this DPA agree to work in good faith to resolve any such reasonable objections raised by the Partner (on its behalf or on behalf of the Customer). Note that such objections, until resolved, may limit the availability of some features in the Services provided or supported by the Subprocessor(s) in question.

iii. ***Liability for Subprocessor***. Where a Subprocessor fails to fulfil its data protection obligations under this DPA, Genesys shall remain fully liable to the Partner for their performance.

iv. ***Third Party Services.*** The Services may function in coordination with various third-party services (e.g., the Genesys Cloud AppFoundry). If Partner uses a third-party service that integrates with the Services, Partner is solely responsible for ensuring compliance of such third-party services and that proper data privacy and service terms and conditions, international transfer mechanisms (e.g., customer care, professional services, etc.) are in place with that third party.

l. ***Disclosure to Authorities.*** Genesys will not disclose Personal Customer Data or Partner Data to Authorities, except as necessary to comply with the law or a valid and binding order (such as a subpoena or a court order). If Authorities request Personal Customer Data or Partner Data from Genesys, Genesys will attempt to redirect the Authorities' request to the Partner or Customer. As part of this effort, Genesys may provide Authorities with Partner or Customer contact information. Genesys will promptly notify the Partner if compelled to disclose Personal Customer Data or Partner Data to Authorities, unless legally prohibited from doing so.

4. INTERNATIONAL DATA TRANSFERS

Partner authorizes Genesys to transfer Personal Customer Data or Partner Data to countries outside of the jurisdiction they originated in, or outside a jurisdiction that has been found to provide adequate protections under applicable Privacy Legislation, subject to adopting the appropriate safeguards, including Transfer Clauses, as applicable. The appropriate Transfer Clauses shall be attached or incorporated in this DPA by reference and apply to any transfers between the parties of Personal Customer Data or Partner Data to countries outside of the jurisdiction they originated in, or outside a jurisdiction that has been found to provide adequate protections under applicable Privacy Legislation, as applicable. The Partner is responsible for ensuring it has the Customer's prior written authorization for such transfers in accordance with the Customer DPA.

5. **LOCAL REQUIREMENTS**

To the extent any Privacy Legislation contains local requirements for a lawful processing of Personal Customer Data and Partner Data subject to this DPA, the parties agree to apply such requirements for relevant jurisdictions as appropriate, as set out in Annex 5 as part of this DPA.

6. **NON-DISCLOSURE**

Subject to obligations under Privacy Legislation or other applicable laws the parties are subject to, the contents of this DPA are Confidential Information. This non-disclosure obligation does not apply to any disclosures of the DPA to the Partner, Customer or a Subprocessor.

7. **ENTIRE AGREEMENT AND CONFLICTS**

a. ***Entire Agreement.*** This DPA and the Master Agreement constitute the entire agreement between the parties concerning the subject matter thereof as of the Effective Date and supersedes any prior agreements, understandings, or communications of the parties.

b. ***Conflicts***. 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. If there is a conflict between the Master Agreement, this DPA, and Transfer Clauses, the Transfer Clauses shall control.

8. **LIABILITY AND INDEMNIFICATION, NOTICES, GOVERNING LAW AND JURISDICTION**

The parties agree that any limitations of liability, liability disclaimers, indemnifications, notice requirements, governing law and jurisdiction clauses contained in the Master Agreement shall equally apply under this DPA.

9. **TERM AND SURVIVAL**

a. ***Term.*** This DPA shall be in force from the Effective Date, for as long as Genesys receives Controller Instructions for the provision of Service. The DPA shall be coterminous with the Master Agreement.

b. ***Survival.*** Genesys shall continue to provide appropriate protections to Personal Customer Data or Partner Data under this DPA after the termination of the DPA until it deletes Personal Customer Data or Partner Data in line with Section 3.i. of this DPA.

10. **SEVERABILITY**

If any term of this DPA is not valid, legal, or enforceable, it will be considered stricken from this DPA, and the validity, legality, and enforceability of the remaining terms will not in any way be affected or impaired thereby.

ANNEXES

Annex 1 – Data Processing Description

Annex 2 – Subprocessors

Annex 2a – Partner Data Subprocessors

Annex 2b – Personal Customer Data Subprocessors

Annex 3 – Security Measures

Annex 4 –Transfer Clauses

Annex 4a – EEA Transfer Clauses

Annex 4b – UK Transfer Clauses

Annex 4c – Swiss Transfer Clauses

Annex 4d – Brazil Transfer Clauses

Annex 4e – Mexico Transfer Clauses

Annex 4f– South Africa Transfer Clauses

Annex 1 – Data Processing Description

The table below sets forth the characteristics of the Personal Customer Data or Partner Data processed (including, as applicable, transferred), by Genesys, in its capacity as subprocessor and processor respectively.

Nature and purpose of the processing	Genesys will process Personal Customer Data for the purposes of the provision of Services to the Customer and Partner Data for the purposes of the provision of Partner Program to the Partner pursuant to the Master Agreement, as further specified in the Documentation, and as further instructed by Controller Instructions.
Categories of data subjects	The Personal Customer Data or Partner 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 the Customer or Partner (who are natural persons) • Employees or contact persons of the Customer or Partner's prospects, customers, business partners and vendors • Employees, agents, advisors, freelancers of the Customer or Partner (who are natural persons) • Customer's or Partner's users authorized by Customer or Partner to use the Services
Categories of Personal Data	The Personal Customer Data or Partner Data is processed in accordance with 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 (only included in Personal Customer Data) • Professional life data • Personal life data • Connection data • Localization data • Other categories of data as customized by the controller Sensitive data may be processed depending on the Customer or Partner use of the Service. Technical and organizational measures appropriate to the nature of the data and risks involved shall be applied in accordance with Section 3.c of this DPA.
Duration of the processing / data retention periods / frequency of transfers	Subject to the DPA, Genesys will process Personal Customer Data or Partner Data in a continuous manner for the duration of the Master Agreement, unless otherwise agreed upon in writing.

Subprocessors	Subprocessors, as described in Annex 2.
Genesys Data Protection Officer ("DPO")	Contact: DataPrivacy@genesys.com.
Partner DPO or privacy contact	Contact:

Annex 2 –Subprocessors

To give effect to the requirements in Section 3.k of this DPA, the parties attach the following Annexes:

Annex 2a – Partner Data Subprocessors

Annex 2b – Personal Customer Data Subprocessors

The terms outlined in these Annexes shall apply respectively to the relevant set of Partner Data / Personal Customer Data, as appropriate according to Partner's role as set out in Section 2.b. of this DPA.

Annex 2a – Partner Data Subprocessors

Genesys may disclose Partner Data to Subprocessors (along with their subsidiary companies) listed in this Annex, depending on what Services, features and functionality Customer or Partner decides to use.

Genesys may use its Affiliates as Subprocessors to provide, for example, support and troubleshooting, depending on the region Partner is based in. Please note that although Genesys Cloud Services are hosted on third-party data center providers, on-premise Services are hosted on systems controlled and operated by the Partner (or its third-party providers), for which the Partner is solely responsible.

Additional Subprocessors may be selected by the Partner in a customized environment. Such additional Subprocessor will be listed in a Statement of Work, Order Form, or other relevant documentation executed by the parties. Partner agrees that signature of such Statement of Work, Order Form, or other relevant documentation authorizes Genesys to use such Subprocessors in line with Section 3.k. of this DPA.

Sub-processor	**Location**	**Website**	**Processing**
Salesforce	USA	www.salesforce.com	Account information for Partner and prospects. (contact information, job title)
Seismic Software, Inc.	USA	www.seismic.com	Genie, Genesys' knowledge management. (Name, email account of Partner employees for log-in)
Zift Solutions	USA	www.ziftsolutions.com	Partner marketing central. (Account information for customers and prospects of Partner including contact information for sending marketing communication)
Okta	USA	www.okta.com	Identity authentication for log-in.
Docebo	USA	www.docebo.com	Partner academy and education. (Name, email account of Partner employees for log-in)

Genesys Affiliates (entities) that may access Personal Information in order to administer the Partner Program:

Name	**Country**
Genesys Cloud Service France (fka. Genesys Telecommunications Laboratories)	France
Genesys Cloud Services Czech s.r.o. (fka. Genesys Telecommunications Laboratories s.r.o.)	Czech Republic
Genesys Cloud Services Hungary Kft	Hungary
Genesys Cloud Services Ireland Limited (fka. Genesys Telecommunications Laboratories Limited)	Ireland
Genesys Europe B.V.	Netherlands
Genesys International B.V.	Netherlands
Genesys Cloud Services B.V.	Netherlands

Name	Country
Genesys Telecommunications Laboratories AB	Sweden
Genesys Cloud Services Germany GmbH	Germany
Genesys Telecommunications Laboratories S.L.	Spain
Genesys Cloud Services S.r.l.	Italy
Genesys Telecommunications Laboratories Sp. z o.o.	Poland
Genesys Cloud Services Corp. fka Genesys Laboratories Canada Inc.	Canada
Genesys Cloud Services K.K. (fka Genesys Japan Co. Ltd.)	Japan
Genesys Cloud Services New Zealand Limited (fka. Genesys Telecommunications Laboratories Limited)	New Zealand
Genesys Korea LLC (fka. Genesys Telecommunications Laboratories LLC)	South Korea
Genesys Labs Ltd.	Israel
Genesys Telecommunications Laboratories – Europe Limited	United Kingdom
Genesys Telecommunications Laboratories S.R.L.	Argentina
Genesys Chile SpA	Chile
Genesys Cloud Services Cayman Ltd. - Philippine Branch (fka. Genesys Telecommunications Laboratories Ltd. – Philippine Branch)	Philippines
Genesys Cloud Services Malaysia Sdn. Bhd. (fka. Genesys Laboratories Sdn. Bhd.)	Malaysia
Genesys Cloud Services Pty. Ltd. (fka Genesys Laboratories Australasia Pty. Ltd.)	Australia
Genesys Cloud Services Singapore Pte. Ltd. (fka. Genesys Telecommunications Laboratories Asia Pte Ltd)	Singapore
Genesys Cloud Services, Inc. (fka Genesys Telecommunications Laboratories, Inc.)	United States
Genesys International B.V. – Dubai Branch	United Arab Emirates
Genesys Serviços Cloud Ltda. (fka Genesys Laboratórios de Telecomunicações Ltda.)	Brazil
Genesys Telecom Labs India Private Limited	India
Genesys Cloud Services (PTY) Limited (fka Genesys Telecommunications Laboratories (PTY) Limited)	South Africa
Genesys Telecommunications Laboratories Colombia Ltda	Colombia
Genesys Telecommunications Laboratories S. de R.L. de C.V.	Mexico
Genesys Turkey Cloud Software Services LLC	Turkey

Name	Country
Branch of Genesys Cloud Services Inc. Middle East for Business Services	Saudi Arabia

Annex 2b – Personal Customer Data Subprocessors

Genesys may disclose Personal Customer Data to Subprocessors listed on the following website (along with their subsidiary companies), depending on what Services, features and functionality Customer decides to use.

Genesys may use its Affiliates as Subprocessors to provide, for example, support and troubleshooting, depending on the region Customer is based in. Please note that although Genesys Cloud Services are hosted on third-party data center providers, on-premise Services are hosted on systems controlled and operated by the Customer (or its third-party providers), for which the Customer is solely responsible.

Partner acknowledges that changes to this website shall constitute notice of changes to Subprocessors and that it will make sure notice available to Customer as required. The authorized Subprocessors can be found on the following link:

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

Additional Subprocessors may be selected by the Customer in a customized environment. Such additional Subprocessor will be listed in a Statement of Work, Order Form, or other relevant documentation executed by the parties. Partner agrees that signature of such Statement of Work, Order Form, or other relevant documentation authorizes Genesys to use such Subprocessors in line with Section 3.k. of this DPA.

Annex 3 – Security Measures

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Genesys provides several solutions and configurations for its platforms. The Genesys Minimum Security Controls apply to all Genesys Services. Any specific TOMs listed below apply in addition for the respective offer specified below. 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**
All Genesys Services (e.g. Genesys Cloud CX, Genesys Hub, Genesys Beyond)	Genesys Minimum Security Controls
Partner Program	Genesys Minimum Security Controls
Genesys Cloud CX	Cloud Services
A3S and R2S Apps	A3S and R2S Security Terms

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 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 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**") form part of agreement between Customer and Genesys for the supply of the Cloud Services ("**Master Agreement**"). These Cloud Security Terms set out the security and compliance posture related to the provision by Genesys of the Cloud Services that Customer has purchased from Genesys pursuant to the Master Agreement. These Cloud Security Terms are applicable to the extent that Genesys has access and control over Customer Data, as defined below. For avoidance of doubt, these Cloud Security Terms do not apply to applications purchased via the AppFoundry Marketplace (even if such application is created by Genesys) or to Genesys Professional Services.

1 Definitions

The following definitions shall only apply regarding these Cloud Security Terms. For the avoidance of doubt, the following definitions do not apply to the Master Agreement.

1.1 **Cloud Services** means Genesys-operated cloud offerings that are based on Genesys proprietary software deployed in a Genesys-managed Cloud Services Environment, and the support for such offerings.

1.2 Cloud Services Environment means the Genesys-controlled infrastructure, including equipment, servers and software, within Data Centers used to provide Cloud Services.

1.3 **Customer Data** means Customer's data that is inputted, or generated from Customer-inputted data, and stored in the Cloud Services. Customer Data does not include any anonymized data incorporated into Service Improvements pursuant to the Master Agreement.

1.4 **Data Center** means a data center where Genesys houses the Cloud Services Environment.

1.5 **Industry Standard** means generally accepted cloud information security practices as reflected in Genesys' policies and procedures.

1.6 **Malicious Code** means viruses, worms, time bombs, corrupted files, Trojan horses and other harmful or malicious code, files, scripts, agents, programs, or any other similar code that may interrupt, limit, damage the operation of Genesys' or another's computer or property.

1.7 **Organisation/Org** means a dedicated Cloud Services instance. Each Org is assigned to a single AWS Cloud Services region and has a unique Org Name and Org ID.

1.8 Security Incident means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

1.9 **User** means an individual who: (i) is authorized by Customer and has been supplied a user identification and password(s) by Customer to access the Cloud Services on Customer's behalf, or (ii) a person licensed to use the Cloud Services for one or more roles (e.g. agent, supervisor, administrator).

2 General

2.1 Shared Responsibility. Security of Customer Data is a shared responsibility between Genesys and Customer, as set out in these Cloud Security Terms and at https://www.genesys.com/company/trust/resources.

2.2 **Security of the AWS Cloud Services.** Amazon Web Services is responsible for protecting the infrastructure that runs AWS services, including the Cloud Services, in the AWS Cloud. Oversight of AWS' security posture is managed in accordance with the agreement between AWS and Genesys. AWS-specific certifications are available at https://aws.amazon.com/compliance/programs. Security and compliance certifications and/or attestation reports for Data Centers must be obtained directly from AWS. AWS may require Customers to execute additional non-disclosure agreements. Third-party auditors also regularly test and verify the effectiveness of AWS security as part of AWS' internal compliance programs. Details on AWS data center specific security controls can be found here: https://aws.amazon.com/compliance/data-center/controls/.

2.3 **Security of the Cloud Services Platform**. Genesys is responsible for the security of the Cloud Services that run on the AWS cloud infrastructure. This includes the cloud-hosted application and related Cloud Services applications, including but not limited to Genesys Cloud User Client, Genesys Cloud Collaborate, Genesys Cloud Communicate.

2.4 Security of Customer's Cloud Services Org. The Customer is responsible for the security of its Cloud Services Org. This security is dependent on Org-specific configurations, and user access restrictions, both of which fall under the Customer's control.

3 Genesys Security Program

3.1 Security Standards. Genesys has implemented and will maintain an information security program designed to protect Customer Data processed in the Cloud Services that follows generally accepted system security principles embodied in the ISO 27001 standard, as appropriate to the nature and scope of the Cloud Services provided. For GC CX Commercial AWS regions, the Cloud Services will maintain, as a minimum, industry standard certifications such as SOC2 Type 2, ISO 27001, C5 and PCI DSS. The then-current list of certifications and attestations applicable to the Cloud Services can be found at https://www.genesys.com/company/trust/compliance.

3.2 Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all Genesys 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, this includes annual compliance training on information security, privacy, HIPAA security & privacy, and PCI. Access to Genesys' code repository requires additional annual training in secure development.

4 **Policies and Procedures.** Genesys will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed at least annually and updated as necessary with the aim of increasing the level of security protection for the Cloud Services. Customers can subscribe to updates to the Cloud Services Security Policy at this page - https://help.mypurecloud.com/subscribe-to-policies/.

5 **Change Management.** The Cloud Services utilize a change management process based on ISO 27001 standards to ensure that all changes to the Cloud Services Environment are appropriately reviewed, tested, and approved.

6 **Data Storage and Backup.** Genesys will create backups of Customer Data. Customer Data will be stored in the same AWS Region as the Customer's Cloud Services Org and maintained using Server-Side Encryption (SSE). Backup data will not be stored on portable media. Customer Data backups are protected from unauthorized access and are encrypted.

7 **Anti-virus and Anti-malware.** Industry Standard anti-malware protection solutions are used to protect the infrastructure that supports the Cloud Services against threats such as Malicious Code. Genesys deploys File Integrity Management (FIM) solutions on all production systems, as well as robust monitoring of system access and command use.

8 **Vulnerability and Patch Management.** Genesys will maintain a vulnerability management program as per Genesys risk management process, that ensures compliance with Industry Standards. Genesys will assess all critical vulnerabilities to the Cloud Services Environment using industry standard CVSS and CVE scores or other similar approach for access/vector complexity, authentication, impact, integrity, and availability. If Genesys deems the resulting risk to be critical to Customer Data, Genesys will endeavour to patch or mitigate affected systems within three (3) working days. Certain stateful systems cannot be patched as quickly due to interdependencies and customer impact, but will be remediated as expeditiously as practicable. In normal operation OS patch management operations will be performed in 30 (thirty) days or less.

9 **Data Deletion and Destruction, Exit Plan.** Genesys will follow, and will ensure that its sub-processors will follow, Industry Standard processes to delete obsolete data and sanitize or destroy retired equipment that formerly held Customer Data. Customer Org related recording and call detail record retention policies are

customer configurable. All other retention policies are managed by Genesys at platform level. Termination of the Cloud Services for Customer will be subject to the Exit Plan in Exhibit A.

10 Penetration Testing.

10.1 **Independent 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.

10.2 Customer Testing. Customers have the option to run a penetration test in conjunction with Genesys Security teams within agreed parameters. This service is chargeable at Genesys' then-current rates. Customer will be required to enter into a Services Order for two Test Orgs and a Statement of Work for related professional services support. This service is available once per year. 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 save as set out above.

11 Product Architecture Security

11.1 **Logical Separation Controls**. The Cloud Services are a multi-tenanted Software as a Service (SaaS) platform. As such, customers on the platform share resources such as server instances, services, data storage locations and databases. Genesys will employ effective logical separation controls based on Industry Standards to ensure that Customer Data is logically separated from other customer data within the Cloud Services Environment. More detail can be found here: https://help.mypurecloud.com/articles/multitenant-security/.

11.2 Firewall Services. Genesys uses Security Groups and appropriate firewall services to protect the Cloud Services Environment. Genesys maintains granular ingress and egress rules, and changes must be approved through Genesys' change management system.

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

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

11.5 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 or higher) over public Internet.

11.6 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 or higher).

11.7 **Encryption Protection**.

11.7.1 **Encryption Methods.** The Cloud Services use Industry Standard encryption methods to uphold confidentiality, integrity and availability of data being stored, processed and transmitted. The Cloud Services provide

a. at rest and in transit encryption of all processed Customer Data;

b. at rest encryption, which is AES 256-based meeting FIPS 197 standard, using encryption keys to which neither AWS and its subcontractors nor Genesys' subcontractors have access; and

c. in transit encryption, which is TLS 1.2 or higher using encryption keys to which neither AWS and its subcontractors nor Genesys' subcontractors have access.

11.7.2 Recording Encryption. The Cloud Services encrypt, as standard, call recordings for voice and digital communications with customer specific keys generated by Genesys but rotation can be managed by Customer. Customer may elect to implement customer-owned encryption keys for recordings, allowing Customer to store and manage its keys outside the Cloud Services. To the extent required by applicable law or Customer's policies, the Customer is responsible for the content of recordings and ensuring that PCI Data is not recorded, using Secure Pause or other tools made available by Genesys.

11.8 **Logging and Monitoring**. Genesys will log security events for the Cloud Services. Genesys will continuously monitor and investigate events that may indicate a Security Incident for the Cloud Services. Platform-related event records will be retained for at least one year. Audit log data related to Customer's Org is available to customers via the Cloud Services UI (https://help.mypurecloud.com/articles/about-the-audit-log-viewer/) or the Cloud Services REST based API's or real-time stream (https://help.mypurecloud.com/articles/about-the-amazon-eventbridge-integration/). Genesys Platform security logs are not available to customers.

12 Access Control

12.1 Access Control. Genesys will implement appropriate tools for access controls to ensure that only authorized Users have access to Customer Data within the Cloud Services Environment.

12.2 **Customer's User Access**.

12.2.1 Usernames and Passwords. Customer is solely responsible for managing User access controls within Customer's Org. The application password requirements are configurable by Customer. Native Multi-Factor Authentication (MFA) is available as part of the Cloud Services and is configurable by Customer. Password Parameters that can be set include minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. 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 Org, whether or not authorized by Customer, and all charges resulting from such use.

12.2.2 **Single Sign On**. Customers can elect to integrate with a customer supplied Single Sign On (SSO) provider for authentication and can use Cross-domain Identity Management (SCIM) for user management. More detail on SCIM is available here: https://help.mypurecloud.com/articles/about-genesys-cloud-scim-identity-management/ and on SSO here: https://help.mypurecloud.com/articles/about-single-sign-on-sso/.

12.3 **Genesys' User Access.** Genesys will follow strict protocol and authorisation flows to 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 protocol will be followed regarding Genesys' user account management:

12.3.1 Accounts. Genesys user accounts are requested by the relevant employee and authorized by Genesys management;

12.3.2 VPN. Genesys employees, who are approved to access the Cloud Services Environment use a client-to-site Virtual Private Network (VPN) for entry into the Cloud Services AWS Virtual Private Cloud (VPC) and they require multi-factor authentication;

12.3.3 Password. Genesys user passwords expire every ninety (90) days;

12.3.4 Time-outs. Session time-outs are systematically enforced;

12.3.5 Termination. Genesys user accounts are promptly disabled (within one working day) upon employee termination or role transfer that eliminates a valid business need for access;

12.3.6 Endpoints. Genesys users can only access the Cloud Services Environment from Genesys-managed endpoints. Genesys-managed endpoints have hard drive encryption enabled;

12.3.7 Review. Genesys employee accounts to the Cloud Services Environment are reviewed at least every 60 days.

13 Business Continuity and Disaster Recovery

13.1 Business Continuity.

13.1.1 Availability Zones. The Cloud Services are deployed and configured in a load balanced active/active/active design and are deployed across at least three AWS Availability Zones ("AZs") within a single region to provide high availability and performance of the Cloud Services. The Cloud Services are 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.

13.1.2 Replication. Using synchronous replication, Cloud Services data is automatically updated in multiple AZs. The Cloud Services use load balancers to route internal and external traffic to available application components. Load balancers are clusters of servers that load balance HTTP requests across multiple AZs. When the load balancer detects that a Cloud Services component is either at capacity or has failed, it routes traffic to other instances automatically to compensate. Both the Cloud Services public APIs and application components are fronted by load balancers.

13.1.3 **Regions.** List of Cloud Services regions can be found on https://www.genesys.com/cloud-platform/global-availability. Highly available architecture is explained under this link https://help.mypurecloud.com/articles/about-architecture-and-technology/.

13.2 **Disaster Recovery**. For the Cloud Services, disaster recovery (DR) tests are performed at least annually. Backup data is not stored off-site or on portable media. Genesys creates backups of Customer Data according to documented backup procedures. Customer Data is stored and maintained solely in Amazon AWS S3 with SSE in the same AWS region where Customer Data resides.

13.3 Business Continuity and Disaster Recovery Plans.

13.3.1 **Corporate Business Continuity Plan.** 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.

13.3.2 **Cloud Services Business Continuity Plan.** Genesys will maintain a Cloud Services business continuity plan designed to assure high availability with a target Recovery Time Objective (RTO) of zero and Recovery Point Objective (RPO) of zero.

13.3.3 Testing. The Cloud Services Business Continuity and Disaster Recovery Plans, annual testing of restores and BC/DR are audited annually as part of compliance audits (SOC 2 Type II, ISO 27001/27017/27018, PCI-DSS, HIPAA & HITRUST, etc.).

13.4 **Customer's Responsibility.** Customer is responsible for building and maintaining business continuity and disaster recovery plans for its operations, connectivity to the Cloud Services and other third-party services.

14 Security Incident Response

14.1 **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.

14.2 **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.

14.3 **Notification Details**. Genesys will provide the following details regarding any Security Incidents to Customer: (i) date on which 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 planned to be taken; and (v) evaluation of alternative measures and next steps.

14.4 **Ongoing Communication**. Genesys will continue providing status updates 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.

15 Use of the Cloud Services

15.1 **VoIP Services Lines**. Customer shall maintain strict security over all VoIP Services lines.

15.2 **Recordings**. Customer acknowledges that use of recordings is within Customer's sole 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 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.

16 Audit of Genesys Security Compliance

16.1 Customer Audit. Provided that Customer has demonstrated that it has a reasonable belief that Genesys is not in compliance with the security standards in Section 3.1 above and subject to Genesys' reasonable confidentiality and information security policies, Customer or a qualified third party chosen by Customer shall have the right, upon at least thirty (30) days' written notice, to perform a remote audit of Genesys' compliance with the terms of these Cloud Security Terms, limited to review of Genesys certifications and attestations, policies, interviews of key personnel, and the completion of a security assessment questionnaire provided by Customer.

16.2 Audit Requirements. Customer may undertake an audit without reasonable belief described in 16.1, provided that:

a. The audit is performed during normal business hours,

b. Genesys will invoice Customer a fee for Genesys' costs incurred (including internal time spent) in connection with any Customer audit, whether the audit was performed remotely or on-site,

c. The scope and price of the audit will be agreed upon by the parties in a Statement of Work,

d. Customer agrees that such audit will not include the right to on-site inspections or audits of any of Genesys' subcontractors, including Genesys' third-party hosting facilities and equipment,

e. The audit will not violate Genesys' obligations of confidentiality to other customers or partners, or reveal Genesys' intellectual property, and

f. Any assessment performed pursuant to this section shall not interfere with the normal conduct of Genesys' business.

16.3 **Cooperation**. Genesys shall cooperate with Customer on any reasonable requests made by Customer during such assessments.

A3S and R2S Security Terms

These security terms for A3S and R2S Services ("A3S and R2S 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 A3S and R2S 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.

a. **General**. Except as otherwise provided in the relevant Service Order or Statement of Work incorporated in the Service Agreement, Genesys Recording as a Service ("**R2S**") and Genesys Cloud Analytics Add-on Services ("**A3S**") will be subject to the Genesys Cloud Service Terms and Conditions for Security ("Standard Security Terms") incorporated into the Agreement. However, Customer acknowledges that R2S and A3S are hosted in an environment separate from the Cloud Services Environment, and thus are subject to a separate security program managed by Genesys' Professional Services team. As such, Customer acknowledges the following with respect to R2S and A3S: (i) the point(s) of contact for any security-related issues will be Genesys' Professional Services team, and not the Cloud Services security team; (ii) obligations of Genesys in the Standard Security Terms will be performed by Genesys' Professional Services team, including audit and Security Incident response obligations; and (iii) R2S and A3S are not in scope of the certifications and attestations applicable to the Cloud Services as described in the Standard Security Terms, and instead will be subject to a separate set of certifications and attestations.

b. **Security Attestations**. Security for R2S and A3S is based on the principles embodied by SOC 2 Type I audit standards, ISO 27001 certification, and HIPAA compliance.

c. **Data Storage and Backup**. Customer Data will be stored in a region of customer's R2S and A3S deployment. It is not required to be backed up in the same region as the Cloud Services instance.

d. **Customer Data (Reporting Metrix) Handover**. Customer data may be exported directly from R2S and A3S using native file export functionality.

e. **Vulnerability and Patch Management**. If Genesys deems the resulting risk to be critical to Customer Data, Genesys will endeavor to patch or mitigate the affected R2S and A3S area within fourteen calendar days.

f. **Intrusion Detection System**. Genesys has implemented intrusion detection across R2S and A3S, however that system has not been assessed for compatibility with PCI DSS standards.

g. **Genesys' User Access**. Genesys employees approved to access R2S or A3S are required to use multi-factor authentication, but VPN is not required. Genesys employee accounts to R2S are reviewed at least every 90 days.

h. **Customer's User Access**. Customer is solely responsible for managing User access controls within Customer's A3S instance and R2S instance. The application password requirements are configurable. MFA is available. Password parameters that can be set include minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. 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 willful action or inaction, Customer is entirely responsible for all use of A3S through Customer's Org, whether or not authorized by Customer, and all charges resulting from such use. Customers can elect to integrate with a customer supplied Single Sign On (SSO) provider for authentication and can use Cross-domain Identity Management (SCIM) for user management.

i. **Business Continuity**. R2S and A3S are deployed and configured in a load balanced active/active design across at least two, and sometimes three AWS Availability Zones ("AZs") within a single region to provide high availability and performance.

j. **Incident Notification**. In the event of a Security Incident through R2S or A3S or other security event requiring notification under applicable law, Genesys will notify Customer within 5 days of becoming aware 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.

Annex 4 –Transfer Clauses

To give effect to the requirements in Section 4 of this DPA, the parties attach and where possible incorporate by reference the following Transfer Clauses, which have been divided by jurisdiction in Annexes 4a *et seq*., as applicable.

Annex 4a – EEA Transfer Clauses

1. **APPLICABILITY.**

a. ***Transfers among Parties***. When the parties transfer among themselves Personal Customer Data or Partner Data, which is subject to the GDPR or EEA Transfer Clauses, to a non-EEA country, which has not been found to provide adequate protections to personal data by relevant Authorities ("**Third Country**"), the parties agree to, and incorporate by reference to this DPA, an appropriate module of the standard contractual clauses set out in the Annex to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time ("**EEA Transfer Clauses**"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. ***Genesys Transfers to Subprocessors***. When Genesys shares Personal Customer Data or Partner Data, which is subject to the GDPR or EEA Transfer Clauses by virtue of an onward transfer with a Subprocessor in a Third Country, they shall conclude Module three of the EEA Transfer Clauses.

c. ***Data Importer and Data Exporter***. For the purposes of the EEA Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the GDPR is the "**data exporter**" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "**data importer**".

2. **EEA TRANSFER CLAUSES MODULES.**

a. ***Controller-to-Processor***. The module two: Transfers Controller to Processor of the EEA Transfer Clauses shall be deemed completed as follows:

i. Optional **Clause 7** (**"Docking clause"**) shall be deemed incorporated.

ii. In **Clause 9(a)** (**"Use of sub-processors"**), the parties choose Option 2, 'General Written Authorisation', with a time period subject to Section 3.k.ii. of the DPA.

iii. In **Clause 11(a)** (**"Redress"**), optional wording shall not be deemed incorporated.

iv. In **Clause 17** (**"Governing law"**), the parties choose Option 1 and agree that EEA Transfer Clauses shall be governed by the law of the EEA Member State where the data exporter is established.

v. In **Clause 18** (**"Choice of forum and jurisdiction"**), the parties agree that any disputes arising from EEA Transfer Clauses shall be resolved by the courts of the EEA Member State where the data exporter is established.

vi. **Annex I.A** (**"List of parties"**) **and I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Section 1.c. of this Annex 4a and in the Annex 1 to this DPA.

vii. **Annex I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Annex 1 to this DPA.

viii. For the purpose of **Annex I.C** (**"Competent supervisory authority"**), the competent supervisory authority shall be that of the EEA Member State where the data exporter is established.

ix. If the data exporter is not established in the EEA and personal data sharing under this DPA is subject to the EEA Transfer Clauses by virtue of the extraterritorial application of the GDPR, or an onward transfer, the 1) applicable governing law under Section 2.a.iv.; 2) courts under Section 2.a.v.; and 3) competent authority under Section 2.a.viii of this Annex 4a to the DPA shall be those of the EEA Member State identified in the original EEA Transfer Clauses which the data exporter is subject to. Data exporter shall notify data importer of such EEA Member State upon request.

x. **Annex II** (**"Technical and organizational measures"**) shall be deemed completed with the information set out in Annex 3 to this DPA.

xi. **Annex III** ("**List of sub-processors**") shall be deemed completed with the information set out in Annex 2 to this DPA.

b. ***Processor-to-Processor***. The module three: Transfers Processor to Processor of the EEA Transfer Clauses shall be deemed completed as follows:

i. Optional **Clause 7** (**"Docking clause"**) shall be deemed incorporated.

ii. In **Clause 9(a)** (**"Use of sub-processors"**), the parties choose Option 2, 'General Written Authorisation', with a time period subject to Section 3.k.ii. of the DPA.

iii. In **Clause 11(a)** (**"Redress"**), optional wording shall not be deemed incorporated.

iv. In **Clause 17** (**"Governing law"**), the parties choose Option 1 and agree that EEA Transfer Clauses shall be governed by the law of the EEA Member State where the data exporter is established.

v. In **Clause 18** (**"Choice of forum and jurisdiction"**), the parties agree that any disputes arising from EEA Transfer Clauses shall be resolved by the courts of the EEA Member State where the data exporter is established.

vi. **Annex I.A** (**"List of parties"**) **and I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Section 1.c. of this Annex 4a and in the Annex 1 to this DPA.

vii. **Annex I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Annex 1 to this DPA.

viii. For the purpose of **Annex I.C** (**"Competent supervisory authority"**), the competent supervisory authority shall be that of the EEA Member State where the data exporter is established.

ix. If the data exporter is not established in the EEA and personal data sharing under this DPA is subject to the EEA Transfer Clauses by virtue of the extraterritorial application of the GDPR, or an onward transfer, the 1) applicable governing law under Section 2.a.iv.; 2) courts under Section 2.a.v.; and 3) competent authority under Section 2.a.viii of this Annex 4a to the DPA shall be those of the EEA Member State identified in the original EEA Transfer Clauses which the data exporter is subject to. Data exporter shall notify data importer of such EEA Member State upon request.

x. **Annex II** (**"Technical and organizational measures"**) shall be deemed completed with the information set out in Annex 3 to this DPA.

xi. **Annex III** ("**List of sub-processors**") shall be deemed completed with the information set out in Annex 2 to this DPA.

c. ***Processor-to-Controller***. The module four: Transfers Processor to Controller of the EEA Transfer Clauses shall be deemed completed as follows:

i. Optional **Clause 7** (**"Docking clause"**) shall be deemed incorporated.

ii. In **Clause 11(a)** (**"Redress"**), optional wording shall not be deemed incorporated.

iii. In **Clause 17** (**"Governing law"**), the parties choose Option 1 and agree that EEA Transfer Clauses shall be governed by the law of the EEA Member State where the data exporter is established.

iv. In **Clause 18** (**"Choice of forum and jurisdiction"**), the parties agree that any disputes arising from EEA Transfer Clauses shall be resolved by the courts of the EEA Member State where the data exporter is established.

v. **Annex I.A** (**"List of parties"**) **and I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Section 1.c. of this Annex 4a and in the Annex 1 to this DPA.

vi. **Annex I.B** (**"Description of transfer"**) shall be deemed completed with the information set out in Annex 1 to this DPA.

vii. If the data exporter is not established in the EEA and personal data sharing under this DPA is subject to the EEA Transfer Clauses by virtue of the extraterritorial application of the GDPR, or an onward transfer, the 1) applicable governing law under Section 2.b.iii.; and 2) courts under Section 2.b.iv of this Annex 4a to the DPA shall be those of the EEA Member State identified in the original EEA Transfer Clauses which the data exporter is subject to. Data exporter shall notify data importer of such EEA Member State upon request.

viii. For the avoidance of any doubt, parties agree that **Section III** ("**Local laws and obligations in case of access by public authorities**") does not apply unless data exporter based in the EEA

combines the personal data received from the data importer based in a third country with personal data collected by the data exporter in the EEA.

Annex 4b – UK Transfer Clauses

1. **APPLICABILITY.**

a. ***Transfers among parties***. When the parties transfer among themselves Personal Customer Data or Partner Data, which is subject to the UK GDPR or UK Transfer Clauses, to a Third Country, parties agree to and incorporate by reference to this DPA the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, and as may be amended or replaced by the UK Information Commissioner's Office and approved by UK Parliament, or/and the Secretary of State from time to time ("**UK Transfer Clauses**"), incorporating the appropriate EEA Transfer Clauses modules, depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. ***Genesys Transfers to Subprocessors***. When Genesys shares Personal Customer Data or Partner Data, which is subject to the UK GDPR or UK Transfer Clauses by virtue of an onward transfer with a Subprocessor in a Third Country, they shall conclude UK Transfer Clauses incorporating module three of the EEA Transfer Clauses.

c. ***Data Importer and Data Exporter***. For the purposes of the UK Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the UK GDPR is the "**data exporter**" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "**data importer**".

2. **UK TRANSFER CLAUSES.**

a. ***Completion***. UK Transfer Clauses shall be deemed completed as follows:

i. **Table 1** shall be deemed completed with the relevant information set out in Section 1.c. of Annex 4a and in the Annex 1 to this DPA;

ii. In **Table 2**, the parties select the checkbox that reads: "*The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information*", and for this purpose, the parties hereby agree to apply the content of the appropriate module(s) of EEA Transfer Clauses, as set out in Annex 4a to this DPA;

iii. **Table 3** shall be deemed completed with the relevant information applicable to the appropriate module(s) of EEA Transfer Clauses incorporated into the UK Transfer Clauses, as set out in Annex 4a to this DPA (including any cross-references to other Annexes it may contain);

iv. The parties agree that both parties may end the UK Transfer Clauses as set out in Section 19 of the UK Transfer Clauses.

Annex 4c – Swiss Transfer Clauses

1. **APPLICABILITY.**

a. ***Transfers among parties***. When the parties transfer among themselves Personal Customer Data or Partner Data, which is subject to the FADP, to a Third Country, the parties agree to and incorporate by reference to this DPA the appropriate modules of the EEA Transfer Clauses adapted for the use under the FADP, as outlined in Section 2 of this Annex 4c to the DPA ("**Swiss Transfer Clauses**"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. ***Genesys Transfers to Subprocessors***. When Genesys shares Personal Customer Data or Partner Data, which is subject to the FADP with a Subprocessor in a Third Country, they shall conclude module three of the Swiss Transfer Clauses.

c. ***Data Importer and Data Exporter***. For the purposes of the Swiss Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the FADP is the "**data exporter**" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "**data importer**".

2. **SWISS TRANSFER CLAUSES.**

a. ***Completion***. Swiss Transfer Clauses shall be deemed completed as follows:

i. Swiss Transfer Clauses shall be completed as outlined in Section 2. of the Annex 4a, as applicable, subject to the below changes.

ii. The term 'member state', as used in the EEA Transfer Clauses, must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility bring proceedings regarding their rights against the data importer and/or data exporter in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EEA Transfer Clauses.

iii. With regards to Annex I.C to the EEA Transfer Clauses, Swiss Federal Data Protection and Information Commissioner (the "**FDPIC**") shall (also) be the competent Supervisory Authority, as follows. When transfer is subject to both the FADP and the GDPR, parallel supervision should apply (i.e., FDPIC shall be competent insofar as the Personal Customer Data or Partner Data transfer is governed by the FADP; competent EEA Authority shall be competent insofar as the Personal Customer Data or Partner Data transfer is governed by the GDPR). Where transfer is subject exclusively to the FADP, the competent supervisory authority is the FDPIC.

iv. With regards to Clause 17 of the EEA Transfer Clauses, the governing law for contractual claims shall be the law of Switzerland or the EEA Member State where the data exporter is established.

v. With regards to Clause 18b of the EEA Transfer Clauses, the place of jurisdiction for actions between the parties shall be the Swiss courts or the courts of the EEA Member State where the data exporter is established.

vi. References to the GDPR should be understood as references to the FADP, as applicable.

Annex 4d – Brazil Transfer Clauses

1. **APPLICABILITY.**

a. ***Transfers among Parties***. When the parties transfer among themselves Personal Customer Data or Partner Data, which is subject to Transfer Clauses under Brazil Privacy Legislation by virtue of a transfer to a country outside Brazil, which has not been found to provide adequate protections to personal data by relevant Authorities ("**Third Country**"), the parties agree to, and incorporate by reference to this DPA, the Standard Contractual Clauses as adopted under Brazil Data Protection Law by the Resolution CD/ANPD No. 19 of 23 August 2024 and approved by the Brazilian Data Protection Authority (ANPD) ("**Brazil Transfer Clauses**"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. ***Genesys Transfers to Subprocessors***. When Genesys shares Personal Customer Data or Partner Data, which is subject to the Transfer Clauses by Brazil Privacy Legislation by virtue of an onward transfer with a Subprocessor in a Third Country, it shall apply these as appropriate.

2. **BRAZIL TRANSFER CLAUSES MODULES.**

a. The Brazil Transfer Clauses shall be deemed completed as follows:

i. **Clause 1.1 ("Identification of the Parties")** shall be completed as follows:

a. Name: See Master Agreement b. Qualification: For the purposes of these Clauses, the party transferring Customer Data subject to the Brazil Privacy Legislation is the "exporter" and the party receiving Customer Data in the Third Country is the "importer". c. Main Address: See Master Agreement. d. Mail Address: See Annex 1 to the DPA. e. Contact for the Data Subject: See Annex 1 to the DPA. f. Other Information: N/A g. As applicable per Section 2.a. of the DPA: (X) Exporter/Controller (X) Exporter/Processor

a. Name: See Master Agreement b. Qualification: For the purposes of these Clauses, the party transferring Customer Data subject to the Brazil Privacy Legislation is the "exporter" and the party receiving Customer Data in the Third Country is the "importer". c. Main Address: See Master Agreement. d. Mail Address: See Annex 1 to the DPA. e. Contact for the Data Subject: See Annex 1 to the DPA. f. Other Information: N/A g. As applicable per Section 2.a. of the DPA: (X) Importer/Controller (X) Importer/processor

ii. **Clause 2 ("Object")** shall be completed as follows:

a. Main purposes of the transfer: See Annex 1 to the DPA.

b. Categories of personal data transferred: See Annex 1 to the DPA.

c. Period of data storage: See Annex 1 to the DPA.

d. Other information: See Annex 1 to the DPA.

iii. In **Clause 3 ("Object")**, parties select Option B, which shall be completed as follows:

a. Main purposes of the transfer: See Annex 1 to the DPA.

b. Categories of personal data transferred: See Annex 1 to the DPA.

c. Period of data storage: See Annex 1 to the DPA.

d. Other information: See Annex 1 to the DPA.

iv. In **Clause 4 ("Responsibilities of the Parties")**, parties select:

a. Option A, in instances where Personal Customer Data is transferred between the parties. In this instance, Clause 4.1 shall be completed as follows:

1. Responsible for publishing the document provided in CLAUSE 14;

(X) Exporter ( ) Importer

2. Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15:

(X) Exporter ( ) Importer

3. Responsible for notifying the security incident provided in CLAUSE 16:

(X) Exporter ( ) Importer

b. Option B, in instances where Partner Data is transferred between the parties. In this instance, Clause 4.1 shall be completed as follows:

1. Responsible for publishing the document provided in CLAUSE 14;

(X) Exporter ( ) Importer

2. Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15:

(X) Exporter ( ) Importer

3. Responsible for notifying the security incident provided in CLAUSE 16:

(X) Exporter ( ) Importer

v. **Section III ("Security Measures")** shall be completed as follows:

a. Governance and supervision of internal processes: see Annex 3 to this DPA.

b. Technical and administrative security measures, including measures to guarantee the security of the operations carried out, such as the collection, transmission and storage of data: see Annex 3 to this DPA.

vi. Parties do not wish to include any **"Additional Clauses and Annexes"** in **Section IV.**

Parties make a reference to the place and date and signatures of the Master Agreement for the purposes of these Brazil Transfer Clauses.

Annex 4e – Mexico Transfer Clauses

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under the Mexico Privacy Legislation. The parties are entering into this agreement for the purpose of satisfying the provisions of Mexico Privacy Legislation.

1. For the purposes of these Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the Mexico Privacy Legislation is the "exporter" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "data importer".

2. The data exporter under the Mexico Privacy Legislation warrants and undertakes that the personal data to be transferred to the data importer concern(s) personal data of its data subjects and is being transferred to the importer in accordance with the Mexico Privacy Legislation.

3. The transfer is made exclusively for the purposes established in Annex 1 to the DPA, that has been acknowledged by the data subjects.

4. The data exporter warrants and undertakes to have a lawful legal ground, in accordance with the Mexico Privacy Legislation to transfer the data subjects' personal data to the data importer for the purposes described in Annex 1 to the DPA.

5. The data exporter will act as described in Section 2.b, which refer to the roles and responsibilities of the parties, in regards with the personal data of the data subjects that will be transferred.

6. The relevant technical and organizational security measures are set forth in Annex 3 to the DPA.

Annex 4f– South Africa Transfer Clauses

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under the South Africa Privacy Legislation. The parties are entering into this agreement for the purpose of satisfying the provisions of South Africa Privacy Legislation.

This Annex constitutes an Addendum to Annex 4a – EEA Transfer Clauses which applies to cross border transfers of personal data from any data exporter under South Africa Privacy Legislation.

1. For the purposes of these Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the South Africa Privacy Legislation is the "exporter" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "data importer".

2. The parties acknowledge that the clauses in the Annex 4a – EEA Transfer Clauses of this DPA, based on the EEA Clauses published by the European Commission, with the additions specified below, shall govern the personal data transfers from South Africa.

3. For the purposes of implementing the EEA Clauses also for data transfers concerning South Africa, the parties to the EEA Clauses hereby agree, considering the EEA Clauses, to the following:

   3.1. **Interpretation**. Where the context requires respectively that the data transfer is subject to South Africa Privacy Legislation, any references to the EU GDPR in the EEA Clauses shall be understood as including a reference to the relevant provision of the South Africa Privacy Legislation. Where the context requires respectively that the data transfer is subject to South Africa Privacy Legislation, any references to the Member States or a Member State shall be understood as including South Africa too.

   3.2. **Competent supervisory authority.** Under this Annex, the competent supervisory authority in accordance with the EEA Clauses shall also be the South African Data Protection Authority (the "Information Regulator").

   3.3. **Jurisdiction**. For the purposes of the EEA Clauses, it is understood that any data subject located in South Africa may also bring legal proceedings against the data exporter and/or data importer before the courts in South Africa, being the courts they have their habitual residence.

4. In the event of the adoption of South African Standard Contractual Clauses by the Information Regulator, during the term of this DPA, the parties agree that those South African Standard Contractual Clauses shall be incorporated by reference to this DPA, with all the relevant amendments and additions potentially required by the Information Regulator.

5. The relevant technical and organizational security measures are set forth in Annex 3 to the DPA.

Annex 4g – Singapore Transfer Clauses

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under the Singapore Privacy Legislation. The parties are entering into this agreement for the purpose of satisfying the provisions of Singapore Privacy Legislation.

This Annex, based on Association of Southeast Asian Nations ("**ASEAN**") Model Contractual Clauses, applies to cross border transfers of Personal Data from any Transferring Party under Singaporean Data Protection Laws.

1. For the purposes of these Transfer Clauses, the party transferring Personal Customer Data or Partner Data subject to the Singapore Privacy Legislation is the "exporter" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "data importer".

2. The data exporter warrants, represents and undertakes that the personal data has been collected, used, disclosed and transferred to the data importer under this DPA in accordance with Singapore Privacy Legislation, or where reasonable and practicable, the data subject has been notified of and given consent to the collection, use, disclosure and/or transfer of his/her personal data.

3. The data importer shall process the personal data only for the purposes described under Annex 1 to the DPA covering the categories of data subjects listed within such Annex.

4. The data exporter warrants, represents, and undertakes that any personal data that have been collected, processed, and transferred is accurate and complete to the extent necessary for the purposes of transfer as described under Annex 1.

5. The parties have taken appropriate steps to determine the level of potential risk of data breaches involved in transferring the relevant personal data and to consider suitable security measures that the parties must undertake.

6. The parties shall agree on and implement appropriate controls and adequate security standards that shall apply to the storage and processing of personal data.

7. The data importer warrants, represents and undertakes to:

   7.1. have in place reasonable and appropriate technical, administrative, operational and physical measures, consistent with the Personal Data Protection Act 2012, to protect the personal data against risks of data breaches.

   7.2. assume, upon receipt of the personal data, responsibility for the protection, processing, and maintenance of the personal data in its possession, in accordance with the Personal Data Protection Act 2012 and this DPA.

   7.3. provide to the data exporter and data subjects a contact point who is authorized on behalf of the data importer to respond to enquiries concerning personal data.

8. The data importer shall cease to retain all personal data in its possession or under its control, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes.

9. The data exporter and data importer shall, in accordance with Part 5 of the Personal Data Protection Act 2012, each respond to enquiries from relevant data subjects or enforcement authorities regarding processing of personal data in their respective jurisdictions, including requests to access or correct personal data.

10. The data importer shall:

    i. develop and implement policies and practices that are necessary to meet the obligations of the organization under this DPA;

ii. develop a process to receive and respond to complaints that may arise with respect to its obligations under this DPA;

iii. communicate to its staff information about the data importer's policies and practices mentioned in paragraph (i); and

iv. make information available on request about the policies and practices mentioned in paragraph (i); and the complaint process mentioned in paragraph (ii);

a) If the data importer becomes aware that a data breach has occurred or is likely to occur affecting personal data in its possession or under its control, or by the importer of an onward transfer, it shall notify the data exporter without undue delay and in any event within twenty-four (24) hours. If the data breach results in or is likely to result in significant harm to the data subject or is likely to be of a significant scale, the data exporter has the obligation to notify the Singaporean competent supervisory authority (the "PDPC") as soon as practicable but no later than 3 calendar days.

Upon the occurrence of a data breach and if required by the data exporter in writing, the data importer shall as soon as practicable, at its own costs, and in a manner that is reasonable in the circumstances, notify each affected individual affected by such notifiable data breach. If not practicable by the data importer, this obligation may be allocated to the data exporter instead.

11. The parties acknowledge that the Singapore Privacy Legislation confers a right on data subjects to enforce the data protection warranties and undertakings of this DPA as third-party beneficiaries. The parties agree that this DPA shall uphold such rights of data subjects under the Singaporean Data Protection Laws.

12. The relevant technical and organizational security measures are set forth in Annex 3 to the DPA.

Annex 4h – RIPD Transfer Clauses (Argentina, Colombia, Costa Rica, Panama, Peru, Uruguay)

Model Agreement for the International Transfer of Personal Data From Controller to Processor

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under Privacy Legislation in Argentina, Colombia, Costa Rica, Panama, Peru, and/or Uruguay, as applicable. The parties are entering into this agreement for the purpose of satisfying the provisions of Privacy Legislation in such jurisdictions.

The Parties to the Contract have agreed to this Agreement based on model contract clauses (hereinafter, model contract clauses" the "Agreement").

The contact details information of the Parties (i.e., full name, address and contact details) shall be deemed completed with the information set out in the Master Agreement.

The Agreement shall be governed by the country of the Data Exporter. The Competent Supervisory Authority shall be the Personal Data Protection authority of the of the Data Exporter's country.

The Parties agree that by signing this DPA, this Agreement shall be deemed signed and completed with the contact details information set out in the Master Agreement.

FIRST PART: GENERAL PROVISIONS

Clause 1. Purpose, parties, scope of application and definitions

1.1. Purpose

a The purpose of these model contractual clauses is to ensure and facilitate compliance with the requirements for the international transfer of Personal Data set by the Governing Law, in order to comply with the principles and obligations on the protection of Personal Data

b Any interpretation of this Agreement shall take these purposes into account.

1.2. Contracting parties

a The Contracting Parties are the Data Exporter and the Data Importer

b This Agreement allows the incorporation of additional importers or exporters as Contracting Parties, using the form in Annex A following the procedure established in Clause 5.

1.3. Scope of application

This Agreement shall apply to international transfers of Personal Data between Data Exporters and Data Importers, in accordance with the specifications of Annex B. The annexes form an integral part of this Agreement.

The defined terms are identified in this Agreement by capital letters. For the purposes of this Agreement, the following terms shall be defined:

Agreement: this contract for the international transfer of Personal Data based on model contractual clauses together with its title page and its annexes.

Anonymization: the application of measures of any kind aimed at pre-venting the identification or re-identification of an individual without disproportionate efforts.

Competent Supervisory Authority: personal data protection authority in the country of the Data Exporter or Data Importer.

Cloud Computing: model for enabling access to a set of IT services (such as networks, servers, storage, applications, and ser-vices) in a convenient manner and on demand, which can be rapidly provided and released with administrative efforts and based on the interaction with the service provider.

Consent: expression of the free, specific, unequivocal and in-formed will of the Data Subject through which he/she accepts and authorizes the Processing of his/her Per-sonal Data.

Personal Data: any information regarding an identified or identifiable individual, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, oracoustic way, or in any other form. It is considered that a per-son is identifiable when his/her identity can be determined directly or indirectly, provided that this does not require disproportionate time or efforts.

Sensitive Personal Data: Personal Data that refer to the intimate sphere of the Data Subject, the undue use of which may result in discrimination or create a serious risk thereof. In an illustrative way, Personal Data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; trade union membership; political opinions; information regarding health, sexual life, preference or orientation; genetic data; or biometric data aimed at identifying a natural person in an unequivocal manner will be considered as sensitive.

Automated Individual Decisions: decisions that produce legal effects concerning the Data Subject, or that affect him/her in a significant way, based solely on automated processing intended to assess, without human intervention, specific personal aspects, or to analyze or predict, specifically, his/her professional performance, economic situation, health status, sexual preferences, reliability or behavior.

Processor: service provider who, as a natural or legal person or public authority, outside the organization of the Controller, processes Personal Data in the name and on behalf of the Controller.

Standards: Standards for Personal Data Protection for the Ibero-American States approved by the RIPD in 2017.

Data Exporter: natural person or private legal entity, public authority, service, body or service provider, located in the territory of a State that performs international transfers of Personal Data, according to the provisions of the Standards.

Data Importer: natural person or private legal entity, public authority, service, body or service provider located in a third country that receives Personal Data from a Data Exporter through an international transfer of Personal Data.

Governing Law: the Personal Data protection law of the Data Exporter's jurisdiction.

Administrative, Physical and Technical Measures: measures aimed at preventing any damage, loss, alteration, destruction, access, and, in general, any illicit or unauthorized use of Personal Data, even if accidental, sufficient to ensure the confidentiality, integrity and availability of the Personal Data.

Controller: natural person or private legal entity, public authority, service or body that, alone or together with others, determines the purposes, means, scope and other matters related to the Processing of Personal Data.

Sub-processor: another Processor relied on by the Processor to carry out certain processing activities on behalf of the Controller.

Third-Party Beneficiaries: Data Subject whose Personal Data is subject to an international transfer under this Agreement. The Data Subject is a Third-Party Beneficiary of the rights provided in his/her favor in the MCCs and can therefore exercise the rights granted to it by the MCCs, even if s/he has not joined the model contract between the Parties.

Data Subject: natural person to whom the Personal Data relates.

Onward Transfer: transfer of data by the Data Importer to a third party located outside of the jurisdiction of the Data Exporter that complies with the safeguards set out in the MCCs.

Processing: any operation or set of operations performed on Per-sonal Data through physical or automated procedures, related, but not limited, to the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, conservation, elaboration, transfer, dissemination, possession, exploitation, and in general any use or disposal of Personal Data.

Personal Data Breach: any damage, loss, alteration, destruction, access, and in general any illicit or unauthorized use of Personal Data, even if accidental.

Clause 2. **Effects and invariability of the clauses**

2.1. Modification of the model contractual clauses. Limitations

This Agreement based on model contractual clauses establishes adequate safeguards for Data Subjects pertaining to the transfer of their data, from Controller(s) to Processor(s), provided that the clauses are not modified in their essence compared to the original model, except to complete the title page and the annexes. This does not prevent the Parties from including model contractual clauses in a broader contract, nor does it prevent them from adding further clauses or safeguards, provided they do not directly or indirectly contradict these model contractual clauses or affect the rights of Data Subjects.

2.2. Hierarchy with the governing law. Interpretation

a This Agreement shall be read and interpreted in accordance with the provisions of the Governing Law.

b The Parties may add new definitions and further safeguards to these model contractual clauses when necessary to comply with the Governing Law and provided this does not negatively affect the protections granted by the model contractual clauses.

c This Agreement shall not be interpreted in a manner that conflicts with the rights and obligations set out in the Governing Law.

d This Agreement is understood to be without prejudice to the obligations to which the Data Exporter is subject by virtue of its legislation or the Governing Law.

2.3. Hierarchy with other agreements

In case of a contradiction between this Agreement and the provisions of related agreements between the Parties, the clauses of this Agreement shall prevail.

Clause 3. **Third-party beneficiaries**

Data Subjects may invoke, as Third-Party Beneficiaries, the clauses of this Agreement against the Data Exporter and/or the Data Importer and require them to ensure compliance.

Clause 4. **Description of the transfer(s) and the purpose(s) thereof**

The details and characteristics of the transfer or transfers and, particularly, the categories of the Personal Data transferred and the purposes for which they are transferred are specified in Annex B of this Agreement.

Clause 5. **Docking clause**

a The Parties accept that any entity that is not a Party to this Agreement may, with the prior consent of all Parties involved, adhere to this Agreement at any time, either as a Data Exporter or as a Data Importer, by signing the form in Annex A, and completing the other Annexes, if applicable.

b Once it has signed Annex A and completed the other annexes, if applicable, the joining entity shall be considered a Party to this Agreement and shall have the rights and obligations of a Data Exporter or a Data Importer, depending on the role under which it has adhered to the Agreement, as indicated in Annex A.

c The entity joining the Agreement shall not acquire rights and obligations under this Agreement for the period prior to its adhesion.

SECTION II: OBLIGATIONS OF THE PARTIES

Clause 6. **Data protection safeguards**

6.1. Instructions

The Data Importer shall carry out Personal Data processing activities without any decision-making power over the scope and content thereof, and instead limit its actions to the terms and instructions established by the Data Exporter.

6.2. Principle of accountability

a The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able to perform its obligations under this Agreement by applying appropriate Administrative, Physical and Technical Measures.

b The Data Importer shall implement the necessary mechanisms to demonstrate compliance with the principles and obligations established in this Agreement, thereby ensuring accountability to the Data Subject and the Competent Supervisory Authority for the Processing of the Personal Data in its possession.

c The Data Importer shall review and permanently assess the mechanisms that it voluntarily adopts to comply with the principle of accountability, in order to measure their level of effectiveness in complying with this Agreement.

6.3. Principle of purpose limitation

The Data Importer shall not process the Personal Data subject to this Agreement for purposes other than those set out in Annex B, unless instructed otherwise by the Data Exporter.

6.4. Transparency

a Upon request, the Parties shall make a copy of this Agreement available to the Data Subject free of charge. In any case, the Data Importer shall proactively assume the responsibility to inform about its existence. The sections or annexes of the Agreement containing trade secrets or other types of confidential information such as Personal Data of third parties or confidential information related to the contractual obligations between the Parties may be redacted.

b This clause is without prejudice to the obligations imposed upon the Data Exporter by the Governing Law.

6.5. Data accuracy and minimization

a 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.

b In this case, the Data Importer shall cooperate with the Data Exporter to erase or rectify the data.

6.6. Principle of data security

a The Data Importer and, during the transfer, also the Data Exporter, shall implement and maintain appropriate Administrative, Physical and Technical Measures to ensure the confidentiality, integrity and availability of the Personal Data subject to this Agreement, including protection against Personal Data Breaches. In assessing the appropriate level of security, the parties shall duly consider the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the risks for the Data Subjects linked to the Processing. To comply with the obligations set out in this paragraph, the Data Importer shall implement, at least, the Administrative, Physical and Technical Measures listed in Annex C to this Agreement. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b In the event of a breach of the Personal Data processed by the Data Importer under this Agreement, the Data Importer shall take appropriate measures to address this breach, including measures to mitigate its adverse effects.

c The Data Importer shall also notify the Data Exporter within seventy-two (72) hours of becoming aware of the Personal Data Breach. Such notification shall include a description of the Personal Data Breach (including, where possible, the categories of Personal Data and approximate number of Data Subjects affected), its likely consequences, and the measures taken or proposed to address the breach and especially, where appropriate, measures to mitigate its potential adverse effects.

d 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.

e The Data Importer shall cooperate with and assist the Data Exporter in enabling it to comply with its obligations under the Governing Law, in particular to notify the Competent Supervisory Authority and the affected Data Subjects, taking into account the nature of the Processing and the information available to the Data Importer.

6.7. Processing under the authority of the data importer and principle of confidentiality

a The Data Importer shall ensure that the persons acting under its authority only process data in accordance with its instructions and 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 this Agreement.

b The Data Importer shall ensure that the persons authorized to process the Personal Data maintain and respect the confidentiality thereof, which is an obligation that shall continue to apply even after the end of its contractual relationship with the Data Exporter.

6.8. Processing of sensitive personal data

a Where the transfer involves Sensitive Personal Data, the Data Importer shall apply the specific restrictions and/or additional safeguards described in Annex C to this Agreement.

b Where the transfer involves Personal Data concerning children or adolescents, the Data Importer shall privilege the protection of their superior interests, in accordance with the Convention on the Rights of the Child and other international instruments.

6.9. Onward transfers

a The Data Importer shall only disclose Personal Data to a third party on documented instructions from the Data Exporter.

b In addition, the Data Importer may only disclose the Personal Data to third parties located outside the Data Exporter's jurisdiction if the third party is bound by or agrees to be bound by this Agreement. Otherwise, the Data Importer may only carry out an Onward Transfer in the following cases:

i. in case this is provided for in the Governing Law, the Onward Transfer is to a country that has been the subject of an adequacy decision regarding its level of protection of Personal Data in accordance with the provisions of the Governing Law, provided that such decision covers the Onward Transfer;

ii. the third party recipient of the Onward Transfer otherwise provides adequate safeguards, in accordance with the Governing law, with regard to Personal Data subject to the Onward Transfer;

iii. the Onward Transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;

iv. if it is necessary to protect the vital interests of the Data Subject or of another natural person.

c All Onward Transfers shall be subject to compliance by the Data Importer with the other safeguards provided in this Agreement and, in particular, compliance with the principle of purpose limitation.

6.10. Documentation and compliance

a The Parties shall be able to demonstrate compliance with their obligations under this Agreement. In particular, the Data Importer shall keep appropriate documentation of the processing activities carried out under the instructions of the Data Exporter, which shall be made available to the Data Exporter and the Competent Supervisory Authority upon request.

b The Data Importer shall promptly and in an appropriate manner deal with the Data Exporter's enquiries that relate to the Processing under this Agreement.

c The Data Importer shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations set out in this Agreement and, at the Data Exporter's request, allow for and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance. The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor to do so. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice.

d The Parties shall make the information referred to in the previous paragraphs, including the results of any audits, available to the Competent Supervisory Authority upon request.

6.11. Duration of the data processing and deletion or return of the data

a Processing by the Data Importer shall only take place for the duration specified in Annex B to this Agreement.

b After the end of the provision of the processing services, the Data Importer shall, at the request of the Data Exporter, securely 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 and securely delete existing copies, should the Data Exporter choose the latter option.

c Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with this Agreement. 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 this Agreement and will only process the data to the extent and for as long as required under that local law.

Clause 7. **Reliance on sub-processors**

7.1. Sub-processor authorization form

a The Data Importer has the Data Exporter's general authorization to contract the Sub-processors included in the 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 15 business 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) in question. The Data Importer shall provide the Data Exporter with the information necessary to enable the Data Exporter to exercise its right to object.

7.2. Data sub-processor agreement

a 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 this Agreement, including in terms of Third-Party Beneficiary rights for Data Subjects. The Parties agree that, by complying with this provision, the Data Importer fulfils its obligations under the clause on Onward Transfers. The Data Importer shall ensure that the Sub-processor complies with the obligations to which it is subject pursuant to this Agreement.

b The Data Importer shall remain fully responsible to the Data Exporter for the performance of the Sub-processor's obligations under its agreement 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 agreement.

Clause 8. **Rights of data subjects**

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 such a request itself unless it has been authorized 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 in the exercise of their rights under the Governing Law. In this regard, the Parties shall set out in Annex C the appropriate Administrative, Physical and Technical Measures, taking into account the nature of the Processing, by which they ensure the assistance to the Data Exporter, as well as the scope and the extent of the assistance required.

c In fulfilling its obligations under the previous paragraphs, the Data Importer shall comply with the instructions from the Data Exporter.

Clause 9. **Redress**

a The Data Importer shall inform the Data Subjects, in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints, who shall handle the complaints received from Data Subjects as quickly as possible.

b In case of a dispute between a Data Subject and one of the Parties as regards compliance with this Agreement, 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, collaborate in good faith to resolve them.

c Whenever a Data Subject invokes a Third-Party Beneficiary Right under this Agreement, the Data Importer undertakes to accept and not dispute the Data Subject's decision to: (i) lodge a complaint with the Supervisory Authority in his/her country of habitual residence or place of work, or with the Competent Supervisory Authority; (ii) file an action in court as regards his/her Personal Data.

d The Data Importer agrees to abide by decisions binding under the Governing Law or other applicable law.

Clause 10. **Civil liability**

a Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of this Agreement.

b Each Party shall be liable to the Data Subject. The Data Subject shall be entitled to receive compensation for any material or non-material damages caused by the Data Importer or its Sub-processor for violating the Third-Party Beneficiary Rights under this Agreement. This is without prejudice to the liability of the Data Exporter under the Governing Law.

c The Parties agree that if the Data Exporter is held liable under the previous paragraph 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.

d Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of this Agreement, all responsible Parties shall be jointly and severally liable.

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

f The Data Importer may not invoke the conduct of a Sub-processor to avoid its own liability.

Clause 11. **Supervision by the competent supervisory authority**

a 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 this Agreement.

b In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the Supervisory Authority, especially corrective and compensatory measures. It shall provide the Supervisory Authority with a written confirmation that the necessary measures have been taken.

Clause 12. **Local laws and practices affecting compliance with the clauses**

a The Parties confirm that, at the time of entering into this Agreement, they have used reasonable efforts to identify whether the transferred data is covered by any local law or practice in the Data Importer's jurisdiction that goes beyond what is necessary and proportionate in a democratic society to safeguard important public interest objectives, and that may reasonably be expected to affect the safeguards, rights, and guarantees afforded to the Data Subject under this Agreement. Based on the foregoing, the Parties confirm that they are not aware of the existence of any such practice or rule that adversely affects the specific safeguards under this Agreement.

b The Data Importer agrees to notify immediately the Data Exporter if any such laws become applicable to it in the future. In the event of such notification, or if the Data Exporter has reasons to believe that the Data Importer is no longer able to perform its obligations under this Agreement, the Data Exporter shall identify appropriate measures to address the situation (for example, Administrative, Physical and Technical Measures to ensure the security of the data). Likewise, it may suspend transfers under this Agreement if it considers that adequate safeguards cannot be ensured. In this case, the Data Exporter shall have the right to terminate this Agreement in accordance with the conditions set out in Clause 13.

c If a court or government agency requires the Data Importer to disclose or use the transferred data in a manner not otherwise permitted by this Agreement, the Data Importer shall assess the legality of such request and challenge it if, after a careful legal assessment, it concludes that there are reasonable grounds to consider that the request is illegal under local law and that the request affects the rights guaranteed by this Agreement. To the extent permitted by local law, it shall also promptly notify the Data Exporter that it has received such a request. If the Data Importer is prohibited by local law from notifying the Data Exporter, the Data Importer shall use reasonable efforts to obtain a waiver of this prohibition.

***SECTION III*: FINAL PROVISIONS**

Clause 13. **Non-compliance with the clauses and termination**

a The Data Importer shall immediately notify the Data Exporter if it is unable to comply with any provision of this Agreement, for whatever reason.

b In the event that the Data Importer fails to comply with its obligations under this Agreement, the Data Exporter shall suspend the transfer of Personal Data to the Data Importer until compliance is again ensured or the contract is terminated.

c The Data Exporter shall be entitled to terminate this Agreement when:

i. the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to the previous paragraph and compliance with this Agreement is not restored within a reasonable period of time and in any event within a period of thirty (30) business days following suspension;

ii. the Data Importer is in substantial or persistent breach of this Agreement; or

iii. the Data Importer fails to comply with a binding decision of a court or Competent Supervisory Authority regarding its obligations under this Agreement. In this case, it shall inform the Competent Supervisory Authority of its non-compliance

d Personal Data that has been transferred prior to the termination of the contract pursuant to the previous paragraph 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. 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 this Agreement. 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 this

Agreement and will only process the data to the extent and for as long as required under that local law.

Clause 14. **Governing law**

This Agreement shall be governed by the Governing Law.

Clause 15. **Choice of forum and jurisdiction**

a Any dispute arising from this Agreement shall be resolved by the courts of the Data Exporter's jurisdiction.

b Data Subjects may also bring legal action in court against the Data Exporter and/or the Data Importer, which may be initiated, at the Data Subject's choice, in the country of the Data Exporter, or in which the Data Subject has his/her habitual residence. With respect to the Data Importer, s/he may also bring legal action in the country of the Data Importer.

c The Parties agree to submit to the competent court(s) provided for in this clause.

***ANNEX A*: ACCESSION FORM FOR NEW PARTIES**

The Annex A "**Accession form for new parties**" of this Agreement shall be deemed completed as follows:

i. The paragraph relating to contact details information of the Data Exporter and the Data Importer who would access this Agreement (i.e., full name, address, contact details and jurisdiction – data exporter's domicile) shall be deemed completed with the information regarding the Affiliates in the sense of this DPA, as applicable.

ii. The paragraph "**Activities related to the data transfer**" shall be deemed completed with the information set out in the Annex 1 of this DPA.

iii. The "**Governing Law**" shall be the governing law of the of the Data Exporter's country.

iv. The "**Competent Supervisory Authority**" shall be the Personal Data Protection authority of the of the Data Exporter's country.

v. The "**Signature date**" shall be the same as the signature date of the Master Agreement.

***ANNEX B*: DESCRIPTION OF THE TRANSFER**

The Annex B "**Description of transfer**" of this Agreement shall be deemed completed as follows:

i. The paragraph "**Categories of Data Subjects whore Personal Data is transferred**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of data subjects").

ii. The paragraph "**Categories of Personal Data transferred**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of Personal Data").

iii. The paragraph "**Sensitive Personal Data transferred (if applicable) and restrictions or safeguards applied**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of Personal Data").

iv. The paragraph "**Transfer Frequency**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Duration of the processing / data retention periods / frequency of transfers").

v. The paragraph "**Term**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Duration of the processing / data retention periods / frequency of transfers").

vi. The paragraph "**Sub-processors**" shall be deemed completed with the information set out in the Annex 2 of this DPA.

***ANNEX C*: ADMINISTRATIVE, PHYSICAL AND TECHNICAL MEASURES TO ENSURE DATA SECURITY**

The Annex C "**Administrative, physical and technical measures to ensure data security**" of this Agreement shall be deemed completed with the information set out in Annex 3 to this DPA.

***ANNEX D*: LIST OF DATA SUBPROCESSORS**

The Annex D "**List of data subprocessors**" of this Agreement shall be deemed completed with the information set out in Annex 2 to this DPA.

***ANNEX E*: ADDITIONAL LEGAL DOCUMENTATION**

N/A

Annex 4i – Saudi Arabia Transfer Clauses

1. **APPLICABILITY.**

a. ***Transfers among Parties***. When the parties transfer among themselves Personal Customer Data and Partner Data, which is subject to Transfer Clauses under Saudi Arabia Privacy Legislation by virtue of a transfer to a country outside Saudi Arabia, which has not been found to provide adequate protections to personal data by relevant Authorities ("**Third Country**"), the parties agree to, and incorporate by reference to this DPA, the Standard Contractual Clauses for Personal Data Transfer as adopted under Saudi Arabia Data Protection Law and published by the Saudi Data and AI Authority on September 2024, as amended ("**Saudi Arabia Transfer Clauses**"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. ***Genesys Transfers to Subprocessors***. When Genesys shares Personal Customer Data or Partner Data, which is subject to the Transfer Clauses by Saudi Arabia Privacy Legislation by virtue of an onward transfer with a Subprocessor in a Third Country, it shall apply these as appropriate.

c. ***Data Importer and Data Exporter***. For the purposes of the Saudi Arabia Transfer Clauses, the party transferring Personal Customer Data subject to the GDPR is the "**data exporter**" and the party receiving Personal Customer Data or Partner Data in the Third Country is the "**data importer**".

2. **SAUDI ARABIA TRANSFER CLAUSES MODULES.**

a. The parties wish to incorporate the following modules of Saudi Arabia transfer clauses, as appropriate:

   i. Second Template: Controller to Processor

   ii. Third Template: Processor to Processor

      1. In **Clause 9.A ("Sub-Processor Appointment")** of the Third Template: Processor to Processor, parties specify the time period subject to Section 3.k.ii. of the DPA.

   iii. Fourth Template: Processor to Controller

b. **Appendix 1 ("Parties of List")** shall be deemed completed with the information set out in Section 3.c. of this Annex 4a and in the Annex 1 to this DPA.

c. **Appendix 2 ("Description of the Transferred Personal Data")** shall be deemed completed with the information set out in Annex 1 to this DPA.

d. **Appendix 3 ("Security Measures")** shall be deemed completed with the information set out in Annex 3 to this DPA.

Annex 4j – ASEAN Transfer Clauses (Thailand)

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under Privacy Legislation in Thailand. The parties are entering into this agreement for the purpose of satisfying the provisions of Privacy Legislation in Thailand. The parties agree that by signing this DPA, these ASEAN Transfer Clauses shall be deemed signed and completed with the contact details information set out in the Master Agreement.

Module 1: Contractual Provisions for Controller-to-Processor Transfers

1. Definitions

1.1 **"AMS Law":** Any and all written laws of an ASEAN Member State relating to data protection (or are, minimally, relevant to the transfer of Personal Data) which the Data Exporter or the Data Importer (or both) are subject to.

1.2 **"Data Breach":** Any loss or unauthorised use, copying, modification, disclosure, or destruction of, or access to, Personal Data transferred under this contract.

1.3 **"Data Exporter":** The Party which transfers Personal Data to the Data Importer under this contract.

1.4 **"Data Importer":** The Party which receives Personal Data from the Data Importer for Processing under this contract.

1.5 **"Data Sub-Processor":** Any person or legal entity which may be engaged by the Data Importer to assist in the Data Exporter's Processing of Personal Data on behalf of the Data Exporter.

1.6 **"Enforcement Authority":** Any public authority empowered by applicable AMS Law to implement and enforce the applicable AMS Law.

1.7 **"Personal Data":** Any information relating to an identified or identifiable natural person ("Data Subject") transferred under this contract.

1.8 **"Processing":** any operation or set of operations that are performed on Personal Data or on sets of Personal Data, whether or not by automated means, including, for example, collection, use and disclosure of Personal Data.

2. Obligations of Data Exporter

The Data Exporter warrants, represents and undertakes that:

2.1 The Personal Data has been collected, used, disclosed and transferred to the Data Importer under this contract in accordance with applicable AMS Law. In the absence of such law, where reasonable and practicable, the Data Subject has been notified of and given consent to the purpose(s) of the collection, use, disclosure and/or transfer of his/her Personal Data.

2.2 The Data Exporter shall implement adequate technical and operational measures to ensure the security of the Personal Data during transmission to the Data Importer.

2.3 The Data Exporter shall respond to enquiries from Data Subjects or Enforcement Authorities regarding the Processing of Personal Data by the Data Importer as required by applicable AMS Law, including requests to access or correct Personal Data, unless the Parties have agreed in writing that the Data Importer shall so respond, and such delegation is permitted by applicable AMS Law. Responses to such enquiries and requests shall be made within a reasonable time frame or within the time frame and in the manner, if any, required under the applicable AMS Law.

3. Obligations of Data Importer

The Data Importer warrants, represents and undertakes that:

3.1 The Data Importer shall Process the Personal Data only in compliance with the Data Exporter's instructions and for the purposes described in Appendix A.

3.2 The Data Importer shall not further disclose or transfer the Personal Data it receives from the Data Exporter to another person, Enforcement Authority or legal entity, including to Data Sub-Processors, unless it has notified the Data Exporter of such further disclosure or transfer in writing, and provided reasonable opportunity for the Data Exporter to object.

3.3 The Data Importer agrees that prior to any disclosure or transfer of Personal Data to third parties, including to Data SubProcessors, the Data Importer shall ensure that the third party shall be subject to and bound by the obligations of the Data Importer to the Data Exporter.

3.4 The Data Importer shall promptly communicate and refer to the Data Exporter any enquiries and requests from Data Subjects relating to the Personal Data transferred by the Data Exporter, including requests to access or correct the Personal Data.

3.5 Upon the termination of this contract or completion of Processing required under this contract, the Data Importer shall, at the election of the Data Exporter, either return to the Data Exporter the Personal Data held in its possession pursuant to this contract, or cease to retain such Personal Data in manner approved of by the Data Exporter. The Data Importer agrees to confirm this with the Data Exporter in writing once action has been taken to cease to retain such Personal Data.

3.6 The Data Importer shall have in place reasonable and appropriate technical, administrative, operational and physical measures, consistent with applicable AMS Laws to protect the confidentiality, integrity and availability of Personal Data, in particular against risks of Data Breaches.

3.7 If the Data Importer becomes aware that a Data Breach has occurred affecting Personal Data in its possession or under its control, or in the possession or under the control of an importer of an onward disclosure or transfer of the Personal Data, it shall notify the Data Exporter under the conditions set forth in the DPA.

3.8 The Data Importer shall promptly notify and consult with the Data Exporter regarding any investigation regarding the collection, use, transfer, disclosure, security, or disposal of the Personal Data transferred under this contract, unless otherwise prohibited under law.

3.9 The Data Importer shall provide prompt assistance to the Data Exporter upon request for the purposes of clause 2.4; and where the Data Importer has agreed in writing, to respond to enquiries and requests from Data Subjects or Enforcement Authorities regarding its Processing of Personal Data when notified by the Data Exporter.

COMMERCIAL COMPONENTS

The remaining clauses are of a general commercial nature, not specific to data protection obligations, and therefore are offered for inclusion only in the event that the contract between the Parties is a stand-alone data protection contract and does not already include such provisions. These commercial components are offered for reference and the Parties are free to make amendments to the terms that are not data protection related.

4. **Choice of Law; Disputes:**

4.1 This contract shall be interpreted according to the laws of Thailand.

4.2 If there is any conflict or inconsistency between clauses in this contract and AMS Law, then the applicable AMS law shall prevail.

5. **Suspension of Transfer**

5.1 In the event that the Data Importer is in breach of its obligations under this contract or applicable AMS Law, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the Processing under this contract is terminated.

6. **Termination of Contract**

6.1 In the event that:

6.1.1 the transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than *6 months* pursuant to Clause 5.1;

6.1.2 compliance by the Data Importer with this contract would put it in breach of its obligations under the law in the country in which it is Processing the Personal Data;

6.1.3 the Data Importer is in material breach of any obligations under this contract;

6.1.4 there is a final decision from which no further appeal is possible of a competent court that there has been a breach of this contract by the Data Importer; or

6.1.5 the Data Importer ceases its operations voluntarily or involuntarily, announces its intent to cease operations, or transfers all or substantially all of its assets to a non-affiliated entity, then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer shall be entitled to terminate this contract. In cases covered by (6.1.1), (6.1.2), or (6.1.4) above the Data Importer may also terminate this contract.

6.2 In the event that:

6.2.1 compliance by the Data Exporter with this contract would put it in breach of its obligations under the law;

6.2.2 the Data Exporter is in material breach of any obligations under this contract;

6.2.3 there is a final decision from which no further appeal is possible of a competent court that there has been a breach of this contract by the Data Exporter; or

6.2.4 the Data Exporter ceases its operations voluntarily or involuntarily, announces its intent to cease operations, or transfers all or substantially all of its assets to a non-affiliated entity, then the Data Importer, without prejudice to any other rights which it may have against the Data Exporter, shall be entitled to terminate this contract. In cases covered by (6.2.1), or (6.2.3) above, the Data Exporter may also terminate this contract.

6.3 The Parties agree that the termination of this contract at any time, in any circumstances and for whatever reason does not exempt them from the obligations of this contract regarding the return or deletion of the Personal Data transferred.

7. **General Undertakings**

7.1 Each Party warrants, represents and undertakes to the other Party that it has full capacity and authority to enter into and to perform its obligations under and in accordance with this contract.

7.2 Each Party agrees to comply with all applicable AMS Law in connection with the performance of its obligations under this contract.

8. **Variation**

8.1 The Parties may, by written agreement, adopt or modify this contract where consistent with the principles set forth in the ASEAN Framework on Personal Data Protection, or as required by applicable AMS Law. This does not preclude the Parties from adding or amending clauses, by written agreement, as appropriate for their commercial or business arrangements.

9. **Description of the Transfer**

9.1 The details of the transfer and the Personal Data involved are specified in Appendix A. The Parties agree that Appendix A may contain confidential business information which they shall not disclose to third parties, except as in accordance with Clause 3.2.

Additional Terms for Individual Remedies

This section contains the additional provisions and should be read as forming part of the attached contract between the Parties. Words and phrases given a defined meaning in these additional terms have the same meaning in the attached contract. If there is any inconsistency between these additional terms and the contract, these additional terms shall prevail.

Individual Remedies:

1.1 The Parties acknowledge that the law of Thailand confers a right on Data Subjects to enforce the data protection warranties and undertakings of this contract as third-party beneficiaries. The Parties agree that this contract shall uphold such rights of Data Subjects under Thailand law.

1.2 Data Subjects can enforce against the Data Exporter Clauses 2.1 and 2.4 as third-party beneficiary.

1.3. Data Subjects can enforce against the Data Importer Clauses 3.5.

1.4. Data Subjects can enforce against Sub-Processors Clauses 2.1, 2.4 and 3.5 when both the Data Exporter and Data Importer have ceased operations, ceased to exist in law, or transferred all or substantially all of their assets to a non-associated entity such that the non-associated entity has assumed the legal obligations of the Data Exporter by contract or operation of law.

1.5. To the extent authorized by applicable AMS Law, Data Subjects may obtain compensation for breaches of this contract by either the Data Importer and/or Data Exporter (as prescribed by applicable AMS Law or, if such law is silent on the allocation of compensation, then from both the Data Importer and Data Exporter in equal shares).

1.6. The Parties do not object to a Data Subject being represented by another body if the Data Subject expressly wishes so and such representation is permitted by applicable law.

APPENDIX A: TEMPLATE FOR DATA EXPORTERS AND IMPORTERS TO DESCRIBE PURPOSES FOR THE TRANSFER OF PERSONAL DATA

The Appendix A "**Parties of List**" of these Clauses shall be deemed completed as follows:

i. The names of the Data Exporter and the Data Importer shall be deemed completed with the information set out in the Master Agreement.

ii. The description of the data subjects and groups of data subjects shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of data subjects").

iii. The description of purposes for the processing of personal data shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Nature and purpose of the processing").

Annex 4k – New Zealand Transfer Clauses

New Zealand Agreement for cross-border transfer of personal information

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under New Zealand Privacy Legislation. The parties are entering into this agreement for the purpose of satisfying the provisions of New Zealand Privacy Legislation. The parties agree that by signing this DPA, these New Zealand Transfer Clauses shall be deemed signed and completed with the contact details information set out in the Master Agreement.

Introduction

What is this agreement about?

This agreement is between two parties: the Discloser and the Recipient.

The Discloser has personal information that it wants to share with the Recipient.

The Recipient is based outside New Zealand. The Discloser needs to comply with New Zealand's Privacy Act 2020 when sending personal information to the Recipient.

The Recipient may be a 'foreign person or entity' under Information Privacy Principle 12 ("IPP12") of the Privacy Act. If so, IPP12 requires that where the Discloser sends personal information to the Recipient, the Discloser must have a reasonable basis to believe that the personal information will still be covered by safeguards comparable to those in the Privacy Act, even if the Recipient is not subject to the Privacy Act. This agreement is designed to provide safeguards to meet the requirements of IPP12.

How do I find my way around this agreement?

This agreement is made up of the Details in Part 1, and the General Terms in Part 2.

The Details in Part 1 are for you to fill out. It may take a bit of thought to get the Details right. This is all part of ensuring your business or organisation has the right privacy settings in place. But if you follow the step-by-step instructions you should be done in no time.

The General Terms in Part 2 are standard legal clauses designed to work with the Details filled out in Part 1. You should read the General Terms to make sure you understand them, but there is nothing you need to fill out. However, before you sign make sure to delete the explanatory comment bubbles providing guidance on the General Terms. The parties can agree additions and modifications to the General Terms, but keep in mind that any changes that undermine the protections provided by the standard template version of this document may affect the Discloser's ability to comply with IPP12 of the Privacy Act.

Some notes on terminology before we get started...

In this agreement, terms that start with a capital letter and appear as headings in the Details (for example, Start Date, Discloser and Recipient) have the meanings given in the Details. Also...

End Date means the date this agreement is terminated in accordance with its terms.

Individual means an individual to whom the transferred information relates.

Personal information means information about an identifiable individual.

Privacy Act means the Privacy Act 2020 (NZ).

Privacy Commissioner means the Privacy Commissioner holding office under the Privacy Act.

Transferred information has the meaning given in the Details, but also includes any personal information about an Individual that is inferred or derived from the transferred information after it is disclosed to the Recipient (whether inferred or derived solely from the transferred information, or with a meaningful contribution from the transferred information).

Part 1: Details

Start Date

When will the cross-border transfer of personal information start?

The starting date of the cross-border transfer of personal information shall be deemed the same as the Effective Date set out in this DPA.

Discloser

What is the full legal name of the individual or organisation **sending** the personal information? If you can, provide any other helpful identifying details, e.g. NZBN, company number or registered address.

The full legal name of the individual or organisation sending the personal information shall be deemed the same as set out in the Master Agreement.

Recipient

What is the full legal name of the overseas individual or organisation **receiving** the personal information? If you can, provide any other helpful identifying details, company number or registered address.

The full legal name of the individual or organisation receiving the personal information shall be deemed the same as set out in the Master Agreement.

Related agreements

If the sending of personal information by the Discloser to the Recipient is part of one or more other agreements between the two parties, you can list the other agreement(s) here, to create a link between this agreement and the other agreement(s).

The related agreements shall be deemed the ones set out in the definition of 'Master Agreement' in this DPA.

If one or more related agreements are listed above, then this agreement will terminate automatically once all those agreements have been terminated or expired. This will not affect the continuing obligations under clause 7.4 of the General Terms.

Transferred information

Identify what personal information will be covered by this agreement. To keep things short, this is referred to everywhere else as "transferred information".

One-off disclosure (tick if applicable) ☐ The transferred information consists of the following personal information disclosed by the Discloser to the Recipient on a one-off basis: The transferred information shall be deemed the same as described in the Annex 1 of this DPA.

Ongoing or periodic disclosure (tick if applicable)

☐ The transferred information consists of **all** personal information disclosed by the Discloser to the Recipient while this agreement is in place, i.e. from the Start Date up to and including the End Date.

☐ The transferred information consists of the following personal information disclosed by the Discloser to the Recipient while this agreement is in place, i.e. during the period from the Start Date up to and including the End Date: (tick one or more)

- ☐ Personal information disclosed in connection with the related agreement(s)
- ☑ Personal information disclosed in connection with the following activities or arrangements:

  The categories of personal information disclosed shall be deemed the same as described in the Annex 1 of this DPA.
- ☐ Other categories of personal information, as follows:

  Describe the personal information.

Permitted Uses

How is the Recipient allowed to use the transferred information?

Applies to...	The Recipient can use the transferred information as follows...	Plus any directly related use?
All Transferred Information	The Recipient will use the transferred information as indicated in the Annex 1 of this DPA.	☐
Choose an option...		☐
Choose an option...		☐

Permitted Disclosures

Are there third parties with whom the Recipient is allowed to share the transferred information? If so, list those third parties here, along with details of the purposes for which those third parties can receive the information, plus any conditions on the third parties' handling of the information.

Applies to...	Third party recipients	Purpose and/or conditions	Plus any directly related purpose?
All Transferred Information	The third party recipients shall be deemed the same as indicated in Annex 2 of this DPA, as the Affiliates in the sense of this DPA and/or the Master Agreement.	The purpose shall be deemed the same as indicated in the Annex 1 of this DPA.	☐
Choose an option.			☐
Choose an option.			☐

Security

Are there any specific security requirements that the Recipient must put in place to protect the transferred information, over and above what is required by clause 1.3 of the General Terms?

The security requirements shall be deemed the same as the ones indicated in the Annex 3 of this DPA.

Sensitive Information

Does the transferred information include any particularly sensitive information? For example, information that relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation or sex life, criminal convictions or offences, or an individual's genetic, biometric or health data.

If so, the parties may want to consider whether the Recipient should be required to apply additional precautions to protect the sensitive information. Use the table below to specify any additional precautions if required.

Description of Sensitive Information	Additional Precautions
The transferred sensitive information shall be deemed the same as indicated in Annex 1 of this DPA.	

Privacy Breach Notification

Who is responsible for giving notice to Individuals affected by a notifiable privacy breach? By default, the General Terms make the Recipient responsible. However, the parties can agree to change this below by changing Recipient to Discloser below.

The Recipient is responsible for giving notice to Individuals affected by a notifiable privacy breach

Deletion

When transferred information is no longer required for any of the permitted uses, the Recipient must promptly and securely destroy or delete that transferred information, as required by clause 1.5 of the General Terms. In addition, if a particular event or date is specified in the table below, then when that event occurs or that date arrives, the Recipient will promptly destroy or delete the relevant transferred information as specified in the table.

Deletion Event / Date	Transferred information to be deleted
The deletion and data retention periods shall be deemed the same as indicated in the Annex 1 of this DPA.	

Local data law

What data protection laws apply in the Recipient's home country? Name the country and list the laws.

The Recipient's home country and the data protection laws shall be deemed the same as indicated in the Master Agreement.

Termination

Do you want to include any rights for the parties to terminate this agreement, over and above what is already included in clause 7 of the General Terms? You can skip these options if none of them apply.

The termination provisions shall be deemed the same as indicated in the Master Agreement.

☐ If this option is ticked, the Discloser may terminate this agreement on not less than 30 days' notice
☐ If this option is ticked, the Recipient may terminate this agreement on not less than 30 days' notice

Consequences of termination

On termination of this agreement, the parties' obligations will continue in relation to any transferred information already sent by the Discloser to the Recipient, but anything sent after that point in time will not be covered by the terms. What else should happen on termination? You can skip these options if none of them apply.

The consequences of termination shall be deemed the same as indicated in the Master Agreement.

☐ If this option is ticked, then all the related agreements listed above will also terminate on the End Date
☐ If this option is ticked, then promptly following the End Date, the Recipient will securely delete or destroy all the transferred information, and notify the Discloser that it has done so

Details for giving notice under the Agreement

Any notice given by a party under this agreement must be sent to the other party's address as notified by the other party from time to time, and each party expressly authorises the service of legal proceedings by email or physical delivery to their notified address. As at the Start Date, each party's address is:

The details for giving notice shall be deemed the same as indicated in the Master Agreement.

Discloser	Recipient
Attention: Enter name or job title.	Attention: Enter name or job title.
Address: Enter address.	Address: Enter address.
Email: Enter email.	Email: Enter email.

Special Terms

Are there any other rights or obligations you want to include in the Agreement? If so, you can set them out in the space provided below. Where these contradict or overlap with the other provisions of the Agreement, the terms you set out below will take priority. Be aware that any extra terms that undermine the protections provided by the standard template version of this document may affect the Discloser's ability to comply with IPP12 of the Privacy Act. Alternatively, you can leave this section blank.

1 What safeguards must the Recipient have in place?

1.1 Limits on collection

The Recipient must only collect transferred information as reasonably necessary for lawful purposes connected with its functions or activities. The Recipient must ensure that its methods of collection are lawful, fair and do not intrude unreasonably on the affairs of any Individual.

1.2 Limits on use and disclosure

The Recipient will not use or disclose transferred information except as permitted in the Details.

1.3 Security

The Recipient will protect the transferred information by implementing and maintaining best practice safeguards against any loss of the transferred information, and any unauthorised access, use, modification or disclosure of the transferred information. The Recipient will also meet any additional security requirements specified in the Details.

Best practice means at least the standard of practice generally expected globally in the same or similar circumstances, from a reasonable and prudent processor of personal information that is the same or of a similar nature to the transferred information.

1.4 Accuracy

The Recipient will take reasonable steps to ensure that the transferred information is accurate, up to date, complete, relevant and not misleading ("**Accurate**") before using it.

1.5 Deletion

The Recipient will promptly and securely destroy or delete the transferred information once it is no longer reasonably required by the Recipient for any use permitted in the Details. The Recipient will also do this as required by any "deletion event / date" specified in the Details. The Recipient will promptly notify the Discloser when it has deleted the transferred information.

1.6 Additional precautions for Sensitive Information

The Recipient acknowledges and agrees that a failure to protect the "sensitive information" identified in the Details is particularly likely to cause harm to Individuals. The Recipient will have in place the additional precautions set out in the Details in relation to the sensitive information.

1.7 Privacy officer

The Recipient will maintain a person with responsibility for monitoring and ensuring the Recipient's compliance with this agreement ("**Privacy Officer**"). The Recipient will ensure that the Privacy Officer provides reasonable co-operation to Individuals and the Discloser for the purposes of clauses 3 and 4. The Recipient will notify the Discloser of its Privacy Officer and will keep the Discloser updated with the details of any new Privacy Officer if this changes.

1.8 Discloser may suspend transfers of information if Recipient is in breach

If the Recipient is in breach of this agreement, the Discloser may suspend any further disclosure of transferred information to the Recipient, until the Recipient has corrected the breach.

2 What if the Recipient shares information with others?

2.1 Where third parties process personal information for the Recipient

Without taking away from clause 1.2, if the Recipient discloses transferred information to a third party, then if the third party's use and disclosure of the information is solely as an agent for the Recipient and not for the third party's own purposes:

- the Recipient must use all reasonable endeavours to prevent unauthorised use or disclosure of the transferred information, including by ensuring that the third party is obliged not to use or disclose the transferred information except as authorised by the Recipient, and is obliged to have in place safeguards consistent with the requirements of clause 1.3;

- for the purposes of this agreement the transferred information held by the third party will be treated as being in the control of the Recipient, and the Recipient is responsible for the third party's acts and omissions in relation to the transferred information.

2.2 Where third parties process personal information for their own purposes

Without taking away from clause 1.2, if the Recipient discloses transferred information to a third party, then if the third party uses or discloses the information for its own purposes and not solely as agent of the Recipient:

- the Recipient must ensure that the third party enters into a binding and enforceable agreement with the Recipient, imposing on the third party substantially the same obligations in respect of that transferred information as are imposed on the Recipient under this agreement, and giving Individuals substantially the same rights to enforce those obligations as they have under this agreement; and

- if the Recipient fails to ensure that the third party enters into such an agreement, then under this agreement the transferred information held by the third party will be treated as being in the control of the Recipient, and the Recipient will be responsible for the third party's acts and omissions in relation to the transferred information.

This clause 2.2 does not apply to any disclosure required by law, or any disclosure to a third party that is subject to the Privacy Act or other laws that overall provide comparable safeguards.

3 What happens if there is a privacy breach?

3.1 The responsible party must notify affected Individuals of a notifiable privacy breach

The responsible party identified in the Details must notify each affected Individual as soon as practicable after becoming aware that a notifiable privacy breach has occurred, but:

- if it is not reasonably practicable for that party to directly notify an affected Individual or each member of a group of affected Individuals, that party may give public notice of the privacy breach so long as that party ensures the public notice does not identify any affected Individual;
- that party may delay notification and/or public notice to the extent and for so long as it believes this is necessary because notification or public notice would increase the risk to the security of transferred information and the risk outweighs the benefits of informing affected Individuals;
- that party is not required to give any notification or public notice where that would not be required from the Recipient under the Privacy Act if the Recipient was subject to the Act.

Notifiable privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected Individual or Individuals or is likely to do so.

Privacy breach means any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, transferred information, or any action that prevents the Recipient from accessing transferred information on either a temporary or permanent basis.

3.2 The Discloser may notify affected individuals if the Recipient fails to do so

If the Recipient is responsible for notifying Individuals under clause 3.1 but fails to give notice when required under that clause, the Discloser may give notice on behalf of the Recipient.

3.3 The Recipient may need to notify privacy breaches under local data laws

Nothing in this clause 3 reduces any obligation the Recipient may have to notify a privacy breach under the local data law specified in the Details, to the extent this is permitted by clause 5.2.

3.4 The Recipient must notify the Discloser if the Recipient learns of a privacy breach

The Recipient will promptly notify the Discloser as soon as the Recipient becomes aware that a notifiable privacy breach has occurred, and if the Discloser is responsible for notifying Individuals of privacy breaches will provide all assistance and information reasonably required by the Discloser to meet its obligations under this clause 3.

4 What happens if an individual asks to see or correct their personal information?

4.1 Each Individual has rights of access and correction

The Recipient agrees that each Individual has a right to access, and to seek correction of, their personal information held by the Recipient that is included in the transferred information.

4.2 How to handle a request for access

If an Individual requests access to their transferred information, then subject to clauses 4.4 and 4.5, the Recipient will confirm whether or not it holds any transferred information about them and, if it does, will provide them with access to the information and advise them that they may request correction of their information.

4.3 How to handle a request for correction

Where an Individual requests correction of their transferred information, the Recipient will take reasonable steps to ensure that the information is Accurate (as defined in clause 1.4) taking into account the permitted uses specified in the Details. If the Recipient is not willing to correct the information as requested, the Recipient will take reasonable steps to ensure a statement of the requested correction is attached to the information, so as to ensure it will always be read with the information. Where the Recipient corrects any transferred information or attaches a statement of correction, the Recipient must take reasonable steps to inform any person to whom the Recipient has disclosed the relevant transferred information.

4.4 Timeframes for responding to requests for access or correction

The Recipient must respond to an Individual's request for access to or correction of their transferred information as soon as reasonably practicable and no later than 30 days after receiving the request. The Recipient must provide reasonable assistance to the Individual in relation to each request.

4.5 When can a request be refused?

In relation to any request from an Individual under this clause 4, the Recipient may refuse access, extend the timeframe for complying with the request, and/or charge the Individual for complying with the request, to the extent that this would be permitted if the request was made under the Privacy Act and the Recipient was subject to the Privacy Act.

5 What about complying with laws?

5.1 The Discloser will comply with its own laws

At the time of sending to the Recipient, the Discloser undertakes that the transferred information has been collected, processed and sent to the Recipient in compliance with all laws applying to the Discloser.

5.2 The Recipient will comply with its own laws

The Recipient will ensure that its treatment of the transferred information is consistent with the "local data law" specified in the Details. However, where a requirement of the local data law is less protective than the other requirements of this agreement, to the extent permitted by law the Recipient will comply with the requirement that is the most protective of the transferred information and the interests of the relevant Individuals.

5.3 The Recipient must notify the Discloser about any use or disclosure compelled by law

If the Recipient is required by a court or government agency under any law to disclose or use the transferred information in a way that would not otherwise be permitted by this agreement, then to the extent law allows the Recipient must notify the Discloser to give it the opportunity to contest that legal requirement (for example, by taking the matter to court).

5.4 The Recipient is not aware of any local laws that would undermine this agreement

The Recipient confirms that at the time of entering into this agreement it has made reasonable efforts to identify whether it is covered by any law that could reasonably be expected to have a substantial adverse effect on the protections intended by this agreement, and is not aware of any such law. The Recipient will use reasonable efforts to ensure that, if any such law applies to it in the future, it will promptly notify the Discloser.

6 What can Individuals do if there is a breach?

6.1 Individuals can claim compensation or other court orders

If the Recipient breaches any obligation(s) under clauses 1, 3 or 4, and the breach is an Interference with Privacy of an Individual, the Individual will be entitled to one or more of the following remedies, with the choice and extent of remedy determined by the tribunal hearing the matter, as it considers just and equitable:

- monetary compensation from the Recipient for loss suffered as a result of the Interference with Privacy, which may include monetary compensation for humiliation, loss of dignity, and/or injury to the feelings of the Individual, or for any adverse effect on the Individual's rights, benefits, privileges or obligations;

- an order restraining the Recipient from continuing or repeating the Interference with Privacy, or from engaging in, or causing or permitting others to engage in, conduct of the same kind, or conduct of any similar kind specified in the order;

- an order that the Recipient perform any acts specified in the order with a view to remedying the Interference with Privacy, or redressing any loss or damage suffered by the aggrieved individual or aggrieved individuals as a result of the interference, or both.

However, the Individual will not be entitled to any damages or other relief beyond the damages or other relief that could reasonably be expected to be granted under the Privacy Act in the same circumstances, if the Recipient was subject to the Privacy Act.

Interference with Privacy in relation to an Individual, means:

- any breach by the Recipient of clause 1 that has or may have a detrimental impact on the Individual, including any loss, damage or injury to them, or any adverse effect on their rights, benefits, obligations or privileges, or significant humiliation, significant loss of dignity, or significant injury to their feelings;
- any breach by the Recipient of clause 3.1 in relation to a privacy breach involving that Individual's transferred information; and/or
- any breach by the Recipient of clause 4 in relation to a request by that Individual for access to or correction of their transferred information.

6.2 Individuals have these rights even though they are not party to this agreement

The entitlement to a remedy under clause 6.1 is directly enforceable by each Individual in accordance with Part 2 of the Contract and Commercial Law Act 2017 (NZ). The Discloser and Recipient may amend the terms of this agreement without the consent of any Individual, so long as the amendment either increases the protections provided by this agreement, or ensures that if the protections are reduced they remain at such a level that any transferred information disclosed to the Recipient by the Discloser before the amendment could still be disclosed to the Recipient after the amendment in compliance with the Privacy Act.

6.3 The Discloser can claim on behalf of Individuals if requested

The Discloser may bring a claim or claims under clause 6.1 on behalf of one or more Individuals, at the request of those Individuals, although the Discloser is not obliged to do so.

7 When does this agreement start and end?

7.1 When does this agreement start?

Once signed by both parties, this agreement begins on the Start Date and continues until the End Date. If the Start Date is earlier than the date of signing, this agreement will apply as if it had been signed on the Start Date.

7.2 When can the Discloser end this agreement?

In addition to any termination rights set out in the Details, the Discloser can terminate this agreement by giving notice to the Recipient if:

- a suspension under clause 1.8 has continued for more than 30 days;
- the Recipient has persistently or materially breached this agreement, the Discloser has notified the Recipient requiring the matter to be addressed, and at the end of 30 days following that notice the Recipient has failed to demonstrate to the Discloser's reasonable satisfaction that all necessary changes have been made to prevent a recurrence;
- the Discloser reasonably considers that the Recipient is subject to one or more laws that have a material adverse effect on the protections intended by this agreement; or
- compliance by the Recipient with its obligations under this agreement would put it in breach of one or more laws that apply to the Recipient; or
- the Recipient undergoes an Insolvency Event.

Insolvency Event means that the Recipient: ceases, or threatens to cease, all or substantially all of its business; is insolvent or bankrupt, or has a receiver, liquidator, administrator, bankruptcy trustee, statutory manager or similar officer appointed; and/or makes an assignment for the benefit of its creditors, or makes any arrangement or composition with its creditors.

7.3 When can the Recipient end this agreement?

In addition to any termination rights set out in the Details, the Recipient may terminate this agreement by giving notice to the Discloser, if the Discloser has persistently or materially breached this agreement, the Recipient has notified the Discloser requiring the matter to be addressed, and at the end of 30 days following that notice the Discloser has failed to demonstrate to the Recipient's reasonable satisfaction that all necessary changes have been made to prevent a recurrence.

7.4 What happens when this agreement ends?

Despite any termination or expiry, all terms of this agreement will continue to apply to the transferred information that the Discloser sent to the Recipient during the period from the Start Date up to and including the End Date. The terms will stop applying once the Recipient has securely and permanently deleted or destroyed all of the transferred information.

8 Anything else I should be aware of?

8.1 This agreement is governed by New Zealand law. The parties submit to the non-exclusive jurisdiction of the New Zealand courts.

8.2 This agreement takes priority over all other agreements between the Discloser and Recipient, except as specifically stated otherwise in any Special Terms set out in the Details.

8.3 Each party will keep this agreement confidential, provided that:

- this will not prevent any disclosure required by law;
- either party may voluntarily disclose this agreement to the Privacy Commissioner, but only if they first inform the Privacy Commissioner that the disclosure is made on the basis that the Agreement is to be kept confidential as far as permitted by law;
- each party will disclose this agreement to an Individual who requests it, provided that the party has first consulted with the other party and redacted any information that the other party reasonably identifies as commercially sensitive and not necessary for the Individual to receive in order to enforce their rights under this agreement. If requested, the party will provide the Individual with reasons for the redactions, to the extent possible without revealing any of the redacted information.

8.4 Each party undertakes that it has full power, capacity and authority to execute, deliver and perform its obligations under this agreement.

8.5 Each party undertakes that it has, and will continue to have, all the necessary consents, permissions, licences and rights to enter into and perform its obligations under this agreement.

8.6 Each party undertakes that its obligations as set out in this agreement are legal, valid, binding, and enforceable in accordance with their terms.

8.7 Neither party may assign, transfer or otherwise dispose of any of its rights or obligations under this agreement except with the prior written consent of the other party.

8.8 No amendment to this agreement will be effective unless in writing and signed by the Discloser and the Recipient.

8.9 If a party fails to exercise, or delays or holds off exercising, a power or right under this agreement, that is not a waiver of the power or right. A single or partial exercise of such a power or right does not preclude further exercises of that power or right or any other.

8.10 A determination that any provision of this agreement is illegal, void or unenforceable will not affect any other part of this agreement.

8.11 This agreement may be executed in any number of counterparts. Once each party has received a counterpart signed by the other (or a digital copy of that signed counterpart), those counterparts will together be treated as if they were a single signed copy of the Agreement.

8.12 In this agreement, unless the context requires otherwise:

- a requirement to notify or give notice is to give notice in writing, which may include email;
- a clause reference in the General Terms is to a clause of the General Terms, and not to a clause in the Details;
- a reference to a party to this agreement includes that party's personal representatives, successors and permitted assigns;
- a reference to any law is a reference to that law as amended, or to any law substituted for that law;
- as far as possible, the provisions of this agreement will be interpreted so as to promote consistency with the Privacy Act.

Annex 4l – Turkey Transfer Clauses

This Annex applies to cross border transfers of Personal Customer Data or Partner Data between Genesys and Partner under Turkey Privacy Legislation. The parties are entering into this agreement for the purpose of satisfying the provisions of Turkey Privacy Legislation. The Annex 1 and 2 attached to this Turkey Transfer Clauses apply simultaneously to the following Turkey Standard Contract 2 (from controller to processor), 3 (from processor to processor) and 4 (from processor to controller). The parties agree that by signing this DPA, these Turkey Transfer Clauses shall be deemed signed and completed with the contact details information as described the Master Agreement.

STANDARD CONTRACT - 2
FOR
THE TRANSFER OF PERSONAL DATA ABROAD
(FROM CONTROLLER TO PROCESSOR)

PART I
General Provisions

Clause 1. **Purpose and Scope**

(a) The purpose of this standard contract is to ensure compliance with the provisions of Personal Data Protection Law No. 6698 dated 24/3/2016 (hereinafter referred to as 'the Law') and the By-Law on Procedures and Principles for the Transfer of Personal Data Abroad (hereinafter referred to as 'the By-Law'), which entered into force following its publication in the Official Gazette dated 10/7/2024 and numbered 32598.

(b) The data controller transferring personal data abroad (hereinafter referred to as 'data exporter') and the data processor in a foreign country receiving personal data from the data exporter (hereinafter referred to as 'data importer') have agreed to this standard contract (hereinafter referred to as 'the Contract').

(c) This Contract applies with respect to the transfer of personal data abroad as specified in Annex I.

(d) The Appendix to this Contract containing the annexes (hereinafter referred to as 'Annexes') forms an integral part of this Contract.

Clause 2. **Effect and Invariability of the Contract**

(a) This Contract sets out appropriate safeguards for the transfer of personal data abroad, including enforceable data subject rights and effective legal remedies in the country receiving the transfer as well, in accordance with Article 9(4) of the Law and the By-Law, provided that no additions, deletions, or modifications are made.t

(b) This Contract is without prejudice to obligations to which the data exporter is subject by virtue of the Law, the By-Law, and other relevant legislation.

Clause 3. **Third-Party Beneficiary Rights**

(a) Data subjects may invoke the clauses of this Contract, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, and Clause 6.

ii) Clause 7.1(b) and Clause 7.9(a), (c), (d), (e).

iii) Clause 8(a), (c), (d), (e).

iv) Clause 11(a), (d), (f).

v) Clause 12.

(b) Paragraph (a) is without prejudice to rights of data subjects under the Law.

Clause 4. **Interpretation**

(a) Where this Contract uses terms that are defined in the Law, the By-Law, and other relevant legislation, the definitions provided in the respective regulations shall apply.

(b) This Contract shall be interpreted in accordance with the Law, the By-Law, and other relevant legislation.

(c) This Contract shall not be interpreted in a way that conflicts with rights and obligations provided for in the Law, the By-Law, and other relevant legislation.

Clause 5. **Rule of Conflict**

In the event of a contradiction between the clauses of this Contract and the provisions of other relevant agreements between the Parties, existing at the time this Contract is agreed or entered into thereafter, the clauses of this Contract shall prevail.

Clause 6. **Description of the Transfer**

The details of the transfer of personal data abroad to be carried out under this Contract, and in particular the categories of personal data to be transferred, the legal basis for the transfer, and the purpose or purposes of the transfer, are specified in Annex I.

PART II
Obligations of the Parties

Clause 7. **Safeguards for Personal Data Protection**

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

Clause 7.1 **Instructions**

(a) The data importer shall process the personal data only in accordance with the instructions of the data exporter. The data exporter may give such instructions during the period in which the data importer carries out personal data processing on behalf of the data exporter.

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

Clause 7.2 **Being Relevant, Limited, and Proportionate to the Purpose**

The data importer shall process the personal data in a manner that is relevant, limited, and proportionate to the purpose/purposes specified in Annex I.

Clause 7.3 **Being Accurate and Kept up to Date Where Necessary**

If the data importer becomes aware that the personal data transferred 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 destroy or rectify the personal data.

Clause 7.4 **Duration of Processing and Complete Destruction or Return of Personal Data**

The data importer may only process personal data for the duration specified in Annex 1. After the end of the processing activities by the data importer on behalf of the data exporter, the data importer shall, at the choice of the data exporter, return all personal data processed on its behalf, together with its back-ups, or ensure the complete destruction of personal data. The data importer warrants that, even if there are legislative provisions that may prevent it from fulfilling this obligation, it will continue to ensure compliance with this Contract to take necessary technical and organisational measures to safeguard the confidentiality of the personal data subject to transfer, and to continue to processing activity only to the extent and for the duration required by legislation. Clause 13 is reserved. The data importer shall certify the destruction of the data for the data exporter. Until the data is returned or completely destroyed, the data importer shall continue to ensure compliance with this Contract.

Clause 7.5 **Obligation to Inform**

On request, the data exporter shall provide a copy of this Contract, including the Annexes completed by the Parties, to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures specified in Annex II and personal data, the data exporter may redact the Annexes included in the copy provided to the data subject and exclude certain portions of the text. However, the data exporter 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. The obligations of the data exporter under Article 10 of the Law and the Communiqué on Procedures and Principles to Be Followed in Fulfilment of the Obligation to Inform, published in the Official Gazette dated 10/3/2018 and numbered 30356, are reserved.

Clause 7.6 **Data Security**

(a) The data importer and, during transmission, also the data exporter shall implement all necessary technical and organisational measures to ensure an appropriate level of security corresponding to the nature of personal data, aiming to prevent unlawful processing of personal data, unlawful access to personal data, to ensure protection of personal data, and to safeguard personal data against accidental loss, destruction or damage. In determining such measures, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved in the processing to the fundamental rights and freedoms of data subjects. The data importer shall implement, at a minimum, technical and organisational measures set out in Annex II while fulfilling its obligations under this paragraph. 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 restrict its personnel's access to the personal data subject to the transfer only to the extent and scope strictly necessary for carrying out the processing activities on behalf of the controller, and ensure that such personal data can only be accessed by the relevant personnel. The data importer shall ensure that natural persons authorised by it to access personal data do not disclose the personal data they have learned to third parties in breach of this Contract and do not use the data for purposes other than those for which it was processed.

(c) In the event that personal data processed by the data importer under this Contract is obtained by others through unlawful means, the data importer shall take appropriate measures to address the data breach and mitigate its potential adverse effects. The data importer shall also notify, without undue delay, the data exporter of this breach. Such notification shall use the 'Data Breach Notification Form' determined by the Board and published on the official website of the Personal Data Protection Authority (hereinafter referred to as 'the Authority'). 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to fulfil its obligations under the Law, in particular to notify the Board and data subjects, taking into account the nature of the personal data processing activity and the information available to the data importer.

Clause 7.7 **Sensitive Personal Data**

(a) The data importer shall take additional technical and organisational measures specified in Annex II, appropriate to the nature of the sensitive personal data.

(b) In the processing of sensitive personal data, adequate measures as determined by the Board shall also be implemented.

Clause 7.8 **Onward Transfers**

(a) Personal data transferred to the data importer may be further transferred by the data importer to a third party located abroad (in the same country as the data importer or in another country) only with the instruction of the data exporter and under the following circumstances:

i) it is to a country benefitting from an adequacy decision pursuant to Article 9(1) of the Law,

ii) the third party to which the onward transfer will be made provides one of the appropriate safeguards set out in Article 9(4) of the Law,

iii) transfer of personal data is mandatory for the establishment, exercise or protection of any right in the context of specific administrative or judicial proceedings,

iv) transfer of personal data is necessary for the protection of life or physical integrity of a person himself/herself or of any other person who is unable to provide consent due to actual impossibility or whose consent is not legally valid,

(b) In any onward transfer, the data importer is obliged to comply with all the other safeguards under this Contract, in particular the principle of relevance, limitation, and proportionality with respect to the purposes.

(c) In cases where the recipients of onward transfers have been identified before notification of this Contract to the Authority, these recipients or recipient groups shall be specified in Annex

I. In the event of a change to the recipients or recipient groups of onward transfer, Annex I shall be updated accordingly, and the Authority shall be notified.

Clause 7.9 **Documentation and Compliance**

(a) The data importer shall promptly and adequately respond to enquiries from the data exporter that relate to the processing under this Contract.

(b) The Parties shall be able to demonstrate compliance with this Contract. The data importer is obliged to keep and maintain information, documents, and records related to the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information and documents necessary to demonstrate compliance with the obligations set out in this Contract and at the data exporter's request, allow for and contribute to audits of the processing activities covered by this Contract, at reasonable intervals, or if there are indications of non-compliance.

(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. Where appropriate, audits shall be carried out with reasonable notice.

(e) The Parties shall provide the information referred to in paragraphs (b) and (c), including the results of the audit conducted at the data importer, to the Board on request.

Clause 8. **Sub-Processors**

(a) The data importer may sub-contract its processing activities performed on behalf of the data exporter under this Contract to sub- processor(s) included in a list to which the data exporter has granted prior consent. The data importer shall inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least with a notice period in accordance with the time frame provided in Article 3.k of the DPA 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. The list of sub- processors authorised by the data exporter shall be provided in Annex III. In the event of a change to sub-processors after notification of this Contract to the Authority, Annex III shall be updated accordingly, and the Authority shall be notified thereof.

(b) Where the data importer sub-contracts its specific processing activities (on behalf of the data exporter), it shall conclude a written contract with the sub-processor. The contract shall provide for, at a minimum, the same data protection safeguards set out in this Contract, including third-party beneficiary rights for data subjects. The Parties agree that, by concluding such a contract, the data importer fulfils its obligations under Clause 7.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to this Contract.

(c) At the data exporter's request, the data importer shall provide, a copy of such a sub-processor contract and any subsequent amendments to it 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 copy to be shared by removing the relevant parts.

(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 with the sub-processor to include a third-party beneficiary clause in the contract for the benefit of the data exporter, which grants the data exporter – in the events such as the data importer has ceased to exist in law or has become insolvent – the right to terminate the sub-processor contract and to instruct the sub-processor to completely destroy or return the personal data together with its backups.

Clause 9. **Data Subject Rights**

(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 the data subjects' requests for the exercise of their rights under the Law. 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 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.

Clause 10. **Redress**

(a) In case of a dispute between a data subject and a data importer as regards third-party beneficiary rights under this Contract, the data subject may submit his/her requests to the data importer regarding the matter. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice to the data subjects or on its website, of a contact point authorised to handle requests. The data importer shall promptly address any requests it receives from data subjects.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with this Contract, that Party shall use its best efforts to resolve the issue amicably in the shortest time possible. 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 right of the data subject to lodge a complaint with the Board and to refer the dispute to the competent courts within the meaning of Clause 18.

(d) The data importer undertakes to abide by decisions that are legally binding under Turkish law.

(e) The data importer agrees that the data subject's use of any of the aforementioned methods to seek redress will not prejudice any other rights the data subject may assert in accordance with applicable legislation.

Clause 11. **Liability**

(a) Each Party shall be liable to the other Party for the damages arising from any breach of this Contract.

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

(c) Without prejudice to 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 this Contract. This is without prejudice to the liability of the data exporter under the Law.

(d) If the data exporter fully compensates the data subject for the damage caused by the data importer (or its sub-processor) under paragraph (c), it reserves the right of recourse against the other party in proportion to its fault.

(e) Where both Parties are responsible for any damage caused to the data subject as a result of a breach of this Contract, all responsible Parties shall be severally liable, and the data subject is entitled to bring an action in court against any of these Parties.

(f) If one Party fully compensates the data subject for the damage caused under paragraph (e), it reserves the right of recourse against the other party in proportion to its fault.

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

Clause 12. **Supervision**

The data importer agrees to cooperate with the Authority in any and all procedures at ensuring compliance with this Contract, to submit itself to the jurisdiction of the Board, and to comply with any decisions issued by the Board. In particular, the data importer agrees to provide the information and documents requested by the Board concerning the subject matter of the examination, to allow on-site examination when necessary, and to comply with the Board's instructions to rectify any identified violations. It shall submit to the Board information and documents certifying the fulfilment of the instructions.

PART III
National Law and Obligations in case of Access by Public Authorities

Clause 13. National Law and Practices Affecting Compliance with the Contract

The data importer agrees, declares and undertakes that there are no national regulations or practices in conflict with this Contract regarding the personal data to be transferred under this Contract. In the event of changes in legislation or practices that may impact the data importer's ability to fulfil its obligations under this Contract during its term, the data importer shall notify the data exporter promptly, and in such a case, the data importer agrees that the data exporter reserves the right to suspend the data transfer or terminate this Contract.

Clause 14. Obligations of the Data Importer in case of Access by Public Authorities

The data importer shall notify the data exporter promptly of any requests from administrative or judicial authorities regarding the personal data transferred under this Contract, or if it becomes aware of any direct access by administrative or judicial authorities to personal data transferred pursuant to this Contract. In such a case, the data importer agrees that the data exporter shall have the right to suspend the data transfer or terminate this Contract, depending on the nature of the request or access.

PART IV
Final Provisions

Clause 15. Non-compliance with the Contract and Termination

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

(b) In the event that the data importer is in breach of this Contract or unable to comply with this Contract, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the Contract is terminated. Provisions of Clause 13 and Clause 14 are reserved.

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

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with this Contract 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 this Contract,

iii) the data importer fails to comply with the decisions of a competent court or the Board regarding its obligations under this Contract.

In these cases, the data exporter shall inform the Board.

(d) In the event that the contract is terminated pursuant to paragraph (c), the data importer, at the choice of the data exporter, shall either return the personal data subject to transfer together with its backups to the data exporter or ensure the complete destruction of the personal data. The data importer warrants that, even if there are legislative provisions that prevent it from fulfilling this obligation, it will continue to ensure compliance with this Contract, take necessary technical and organisational measures to safeguard the confidentiality of the personal data subject to transfer, and continue to processing activity only to the extent and for the duration required by legislation. The data importer shall certify the destruction of the data for the data exporter. Until the data is returned or completely destroyed, the data importer shall continue to ensure compliance with this Contract.

Clause 16. Governing Law

This Contract shall be governed by Turkish law.

Clause 17. Competent Court

(a) Any dispute arising from this Contract shall be resolved by Turkish courts.

(b) General provisions shall apply in terms of competence.

(c) The Parties agree to submit themselves to the jurisdiction of Turkish courts.

STANDARD CONTRACT - 3
FOR
THE TRANSFER OF PERSONAL DATA ABROAD
(FROM PROCESSOR TO PROCESSOR)

PART 1
General Provisions

Clause 1. **Purpose and Scope**

(a) The purpose of this standard contract is to ensure compliance with the provisions of Personal Data Protection Law No. 6698 dated 24/3/2016 (hereinafter referred to as 'the Law') and the By-Law on Procedures and Principles for the Transfer of Personal Data Abroad (hereinafter referred to as 'the By-Law'), which entered into force following its publication in the Official Gazette dated 10/7/2024 and numbered 32598.

(b) The data processor transferring personal data abroad (hereinafter referred to as 'data exporter') and the data processor in a foreign country receiving personal data from the data exporter (hereinafter referred to as 'data importer') have agreed to this standard contract (hereinafter referred to as 'the Contract').

(c) This Contract applies with respect to the transfer of personal data abroad as specified in Annex I.

(d) The Appendix to this Contract containing the annexes (hereinafter referred to as 'Annexes') forms an integral part of this Contract.

Clause 2. **Effect and Invariability of the Contract**

(a) This Contract sets out appropriate safeguards for the transfer of personal data abroad, including enforceable data subject rights and effective legal remedies in the country receiving the transfer as well, in accordance with Article 9(4) of the Law and the By-Law, provided that no additions, deletions, or modifications are made.

(b) This Contract is without prejudice to obligations to which the data exporter is subject by virtue of the Law, the By-Law and other relevant legislation.

Clause 3. **Third-Party Beneficiary Rights**

(a) Data subjects may invoke the clauses of this Contract, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, and Clause 6.

ii) Clause 7.1(a), (c), (d) and Clause 7.9(a), (c), (d), (e), (f), (g).

iii) Clause 8(a), (c), (d), (e).

iv) Clause 11(a), (d), (f).

v) Clause 12.

(b) Paragraph (a) is without prejudice to rights of data subjects under the Law.

Clause 4. **Interpretation**

(a) Where this Contract uses terms that are defined in the Law, the By-Law, and other relevant legislation, the definitions provided in the respective regulations shall apply.

(b) This Contract shall be interpreted in accordance with the Law, the By-Law, and other relevant legislation.

(c) This Contract shall not be interpreted in a way that conflicts with rights and obligations provided for in the Law, the By-Law, and other relevant legislation.

Clause 5. Rule of Conflict

In the event of a contradiction between the clauses of this Contract and the provisions of other relevant agreements between the Parties, existing at the time this Contract is agreed or entered into thereafter, the clauses of this Contract shall prevail.

Clause 6. Description of the Transfer

The details of the transfer of personal data abroad to be carried out under this Contract, and in particular the categories of personal data to be transferred, the legal basis for the transfer, and the purpose or purposes of the transfer, are specified in Annex I.

PART II
Obligations of the Parties

Clause 7. Safeguards for Personal Data Protection

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

Clause 7.1 Instructions

(a) The data exporter shall inform the data importer that it acts as data processor under the instructions of the data controller/controllers, which the data exporter has notified the data importer prior to the processing activity.

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

(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 given by the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that the data importer will undertake the same data protection obligations as those undertaken by the data exporter in relation to the personal data processing activities the data exporter carries out on behalf of the controller.

Clause 7.2 Being Relevant, Limited, and Proportionate to the Purpose

The data importer shall process the personal data in a manner that is relevant, limited, and proportionate to the purpose/purposes specified in Annex I.

Clause 7.3 Being Accurate and Kept up to Date Where Necessary

If the data importer becomes aware that the personal data transferred 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 destroy or rectify the personal data.

Clause 7.4 Duration of Processing and Complete Destruction or Return of Personal Data

The data importer may only process personal data for the duration specified in Annex 1. After the end of the processing activities by the data importer on behalf of the data exporter, the data importer shall, at the choice of the data exporter, return all personal data processed on its behalf together with its back-ups, or ensure the complete destruction of personal data. The data importer warrants that, even if there are legislative provisions that may prevent it from fulfilling this obligation, it will continue to ensure compliance with this Contract, take necessary technical and organisational measures to safeguard the confidentiality of the personal data subject to transfer, and continue to processing activity only to the extent and for the duration required by legislation. Clause 13 is reserved. The data importer shall certify the destruction of the data for the data exporter. Until the data is returned or completely destroyed, the data importer shall continue to ensure compliance with this Contract.

Clause 7.5 **Obligation to Inform**

On request, the data exporter shall provide a copy of this Contract, including the Annexes completed by the Parties, 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 the Annexes included in the copy provided to the data subject and exclude certain portions of the text. However, the data exporter 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.

Clause 7.6 **Data Security**

(a) The data importer and, during transmission, also the data exporter shall implement all necessary technical and organisational measures to ensure an appropriate level of security corresponding to the nature of personal data, aiming to prevent unlawful processing of personal data, unlawful access to personal data, to ensure protection of personal data, and to safeguard personal data against accidental loss, destruction or damage. In determining such measures, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved in the processing to the fundamental rights and freedoms of data subjects. The data importer shall implement, at a minimum, technical and organisational measures set out in Annex II while fulfilling its obligations under this paragraph. 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 restrict its personnel's access to the personal data subject to the transfer only to the extent and scope strictly necessary for carrying out the processing activities on behalf of the controller, and ensure that such personal data can only be accessed by the relevant personnel. The data importer shall ensure that natural persons authorised by it to access personal data do not disclose the personal data they have learned to third parties in breach of this Contract and do not use the data for purposes other than those for which it was processed.

(c) In the event that personal data processed by the data importer under this Contract is obtained by others through unlawful means, the data importer shall take appropriate measures to address the data breach and mitigate its potential adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate, the controller. Such notification shall use the 'Data Breach Notification Form' determined by the Board and published on the official website of the Personal Data Protection Authority (hereinafter referred to as 'the Authority'). 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the Law, in particular to notify its controller, on whose behalf it carries out processing activity, so that the controller may in turn notify the Board and the data subjects, taking into account the nature of processing and the information available to the data importer.

Clause 7.7 **Sensitive Personal Data**

(a) The data importer shall implement specific technical and organisational measures set out in Annex II, appropriate to the nature of the sensitive personal data.

(b) In the processing of sensitive personal data, adequate measures as determined by the Board shall also be implemented.

Clause 7.8 **Onward Transfers**

(a) Personal data transferred to the data importer may be further transferred by the data importer to a third party located abroad (in the same country as the data importer or in another country) only with the instruction of the data exporter and under the following circumstances:

i) it is to a country benefitting from an adequacy decision pursuant to Article 9(1) of the Law,

ii) the third party to which the onward transfer will be made provides one of the appropriate safeguards set out in Article 9(4) of the Law,

iii) transfer of personal data is mandatory for the establishment, exercise or protection of any right in the context of specific administrative or judicial proceedings,

iv) transfer of personal data is necessary for the protection of life or physical integrity of a person himself/herself or of any other person who is unable to provide consent due to actual impossibility or whose consent is not legally valid,

(b) In any onward transfer, the data importer is obliged to comply with all the other safeguards under this Contract, in particular the principle of relevance, limitation, and proportionality with respect to the purposes.

(c) In cases where the recipients of onward transfers are identified before notification of this Contract to the Authority, these recipients or recipient groups shall be specified in Annex I. In the event of a change to the recipients or recipient groups of onward transfer, Annex I shall be updated accordingly and the Authority shall be notified.

Clause 7.9 **Documentation and Compliance**

(a) The data importer shall promptly and adequately respond to enquiries from the data exporter or the controller that relate to the processing under this Contract.

(b) The Parties shall be able to demonstrate compliance with this Contract. The data importer is obliged to keep and maintain information, documents, and records related to the processing activities carried out on behalf of the controller.

(c) The data importer shall provide the data exporter with all information and documents necessary to demonstrate compliance with the obligations set out in this Contract. The data exporter shall then forward this information to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by this Contract, at reasonable intervals or if there are indications of non-compliance with this Contract, or where the data exporter requests an audit on instructions of the controller.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall communicate the result of the audit 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. Where appropriate, audits shall be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of the audit conducted at the data importer, available to the Board on request.

Clause 8. **Sub-Processors**

(a) The data importer may sub-contract its processing activities performed on behalf of the data exporter under this Contract to sub- processor(s) included in a list to which the controller has granted prior consent. The data importer shall inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least with a notice period in accordance with the time frame provided in Article 3.k of the DPA 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 new sub-processors. The list of sub-processors authorised by the controller shall be provided in Annex III. In the event of a change to sub- processors after notification of this Contract to the Authority, Annex III shall be updated accordingly, and the Authority shall be notified thereof.

(a) Where the data importer sub-contracts its specific processing activities (on behalf of the controller), it shall conclude a written contract with the sub-processor. The contract shall provide for, at a minimum, the same data protection safeguards set out in this Contract, including third-party beneficiary rights for data subjects. The Parties agree that, by concluding such a contract, the data importer fulfils its obligations under Clause 7.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to this Contract.

(b) At the request of the data exporter or controller, the data importer shall provide a copy of such a sub-processor contract and any subsequent amendments to it to the data exporter or the controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the copy to be shared by removing the relevant parts.

(c) 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.

(d) The data importer shall agree with the sub-processor to include a third-party beneficiary clause in the contract for the benefit of the data exporter, which grants the data exporter – in the events such as the data importer

has ceased to exist in law or has become insolvent – the right to terminate the sub-processor contract and to instruct the sub-processor to completely destroy or return the personal data together with its backups.

Clause 9. **Data Subject Rights**

(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 the Law. 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 activity, by which the assistance shall be provided, as well as the scope 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.

Clause 10. **Redress**

(a) In case of a dispute between a data subject and a data importer as regards third-party beneficiary rights under this Contract, the data subject may submit his/her requests to the data importer regarding the matter. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice to the data subjects or on its website, of a contact point authorised to handle requests. The data importer shall promptly address any requests it receives from data subjects.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with this Contract, that Party shall use its best efforts to resolve the issue amicably in the shortest time possible. 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 right of the data subject to lodge a complaint with the Board and to refer the dispute to the competent courts within the meaning of Clause 18.

(d) The data importer undertakes to abide by decisions that are legally binding under Turkish law.

(e) The data importer agrees that the data subject's use of any of the aforementioned methods to seek redress will not prejudice any other rights the data subject may assert in accordance with applicable legislation.

Clause 11. **Liability**

(a) Each Party shall be liable to the other Party for the damages arising from any breach of this Contract.

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

(c) Without prejudice to 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 this Contract. This is without prejudice to the liability of the data exporter and the controller under the Law.

(d) If the data exporter fully compensates the data subject for the damage caused by the data importer (or its sub-processor) under paragraph (c), it reserves the right of recourse against the other party in proportion to its fault.

(e) Where both Parties are responsible for any damage caused to the data subject as a result of a breach of this Contract, all responsible Parties shall be severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) If one Party fully compensates the data subject for the damage caused under paragraph (e), it reserves the right of recourse against the other party in proportion to its fault.

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

Clause 12. **Supervision**

The data importer agrees to cooperate with the Authority in any and all procedures at ensuring compliance with this Contract, to submit itself to the jurisdiction of the Board, and to comply with any decisions issued by the Board. In particular, the data importer agrees to provide the information and documents requested by the Board concerning the subject matter of the examination, to allow on-site examination when necessary, and to comply with the Board's instructions to rectify any identified violations. It shall submit to the Board information and documents certifying the fulfilment of the instructions.

PART III
National Law and Obligations in case of Access by Public Authorities

Clause 13. **National Law and Practices Affecting Compliance with the Contract**

The data importer agrees, declares and undertakes that there are no national regulations or practices in conflict with this Contract regarding the personal data to be transferred under this Contract. In the event of changes in legislation or practices that may impact the data importer's ability to fulfil its obligations under this Contract during its term, the data importer shall notify the data exporter promptly. The data exporter provides this notification to the controller. In such a case, the data importer agrees that the data exporter reserves the right to suspend the data transfer or terminate this Contract.

Clause 14. **Obligations of the Data Importer in case of Access by Public Authorities**

The data importer shall notify the data exporter promptly of any requests from administrative or judicial authorities regarding the personal data transferred under this Contract, or if it becomes aware of any direct access by such authorities to personal data transferred pursuant to this Contract. The data exporter provides this notification to the controller. In such a case, the data importer agrees that the data exporter shall have the right to suspend the data transfer or terminate this Contract, depending on the nature of the request or access.

PART IV
Final Provisions

Clause 15. **Non-compliance with the Contract and Termination**

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

(b) In the event that the data importer is in breach of this Contract or unable to comply with this Contract, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the Contract is terminated. Provisions of Clause 13 and Clause 14 are reserved.

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

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with this Contract 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 this Contract,

iii) the data importer fails to comply with the decisions of a competent court or the Board regarding its obligations under this Contract.

In these cases, the data exporter shall inform the Board and the controller.

(d) In the event that the contract is terminated pursuant to paragraph (c), the data importer, at the choice of the data exporter, shall either return the personal data subject to transfer together with its backups to the data exporter or ensure the complete destruction of the personal data. The data importer warrants that, even if there are legislative provisions that prevent it from fulfilling this obligation, it will continue to ensure compliance with this Contract, take necessary technical and organisational measures to safeguard the confidentiality of the personal data subject to transfer, and continue to processing activity only to the extent and for the duration required by legislation. The data importer shall certify the destruction of the data for the data exporter. Until the data is returned or completely destroyed, the data importer shall continue to ensure compliance with this Contract.

Clause 16. **Governing Law**

This Contract shall be governed by Turkish law.

Clause 17. **Competent Court**

(a) Any dispute arising from this Contract shall be resolved by Turkish courts.

(b) General provisions shall apply in terms of competence.

(c) The Parties agree to submit themselves to the jurisdiction of Turkish courts.

STANDARD CONTRACT – 4
FOR
THE TRANSFER OF PERSONAL DATA ABROAD
(FROM PROCESSOR TO CONTROLLER)

PART 1
General Provisions

Clause 1. **Purpose and Scope**

(a) The purpose of this standard contract is to ensure compliance with the provisions of Personal Data Protection Law No. 6698 dated 24/3/2016 (hereinafter referred to as 'the Law') and the By-Law on Procedures and Principles for the Transfer of Personal Data Abroad (hereinafter referred to as 'the By-Law'), which entered into force following its publication in the Official Gazette dated 10/7/2024 and numbered 32598.

(b) The data processor transferring personal data abroad (hereinafter referred to as 'data exporter') and the data controller in a foreign country receiving personal data from the data exporter (hereinafter referred to as 'data importer') have agreed to this standard contract (hereinafter referred to as 'the Contract').

(c) This Contract applies with respect to the transfer of personal data abroad as specified in Annex I.

(d) The Appendix to this Contract containing the annexes (hereinafter referred to as 'Annexes') forms an integral part of this Contract.

Clause 2. **Effect and Invariability of the Contract**

(a) This Contract sets out appropriate safeguards for the transfer of personal data abroad, including enforceable data subject rights and effective legal remedies in the country receiving the transfer as well, in accordance with Article 9(4) of the Law and the By-Law, provided that no additions, deletions, or modifications are made.

(b) This Contract is without prejudice to obligations to which the data exporter is subject by virtue of the Law, the By-Law, and other relevant legislation.

Clause 3. **Third-Party Beneficiary Rights**

(a) Data subjects may invoke the clauses of this Contract, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, and Clause 6.

ii) Clause 7.1(b) and Clause 7.3(b).

iii) Clause 16

(b) Paragraph (a) is without prejudice to the rights of data subjects under the Law.

Clause 4. **Interpretation**

(a) Where this Contract uses terms that are defined in the Law, the By-Law, and other relevant legislation, the definitions provided in the respective regulations shall apply.

(b) This Contract shall be interpreted in accordance with the Law, the By-Law, and other relevant legislation.

(c) This Contract shall not be interpreted in a way that conflicts with rights and obligations provided for in the Law, the By-Law, and other relevant legislation.

Clause 5. **Rule of Conflict**

In the event of a contradiction between the clauses of this Contract and the provisions of other relevant agreements between the Parties, existing at the time this Contract is agreed or entered into thereafter, the clauses of this Contract shall prevail.

Clause 6. **Description of the Transfer**

The details of the transfer of personal data abroad to be carried out under this Contract, and in particular the categories of personal data to be transferred, the legal basis for the transfer, and the purpose or purposes of the transfer, are specified in Annex I.

PART II
Obligations of the Parties

Clause 7. **Safeguards for Personal Data Protection**

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

Clause 7.1 **Instructions**

(a) The data exporter shall process the personal data only in accordance with the instructions from the data importer acting as its controller for whom the data exporter carries out processing activities.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the Law, the By-Law, and other relevant legislation.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under the Law, including in the context of sub-processing or as regards cooperation with the Personal Data Protection Authority (hereinafter referred to as 'the Authority').

(d) After the end of data processing activities of the data exporter performed on behalf of the data importer; the data exporter warrants that, at the choice of the data importer, it will either return the personal data together with its backups to the data importer or ensure the complete destruction of the personal data processed on its behalf. The data exporter shall certify the destruction of the data for the data exporter.

Clause 7.2 **Data Security**

(a) The Parties shall implement all necessary technical and organisational measures, including during transmission, to ensure an appropriate level of security corresponding to the nature of personal data, aiming to prevent unlawful processing of personal data, unlawful access to personal data, to ensure the protection of personal data, and to safeguard personal data against accidental loss, destruction or damage. In determining such measures, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing and the risks involved in the processing to the fundamental rights and freedoms of data subjects.

(b) The data exporter shall assist the data importer in taking all technical and organisational measures to ensure appropriate security of the personal data in accordance with paragraph (a). In the event that the personal data processed by the data exporter under this Contract is obtained by others through unlawful means, the data exporter shall notify the data importer without undue delay after becoming aware of the breach and assist the data importer in taking necessary measures to mitigate possible adverse effects of the breach.

(c) The data exporter shall ensure that natural persons authorised to access the personal data do not disclose the personal data they have learned to third parties in breach of this Contract, and do not use the data for any purposes other than those for which it was processed.

Clause 7.3 **Documentation and Compliance**

(a) The Parties shall be able to demonstrate compliance with this Contract.

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

Clause 8. **Data Subject Rights**

The Parties shall assist each other in responding to the enquiries and requests made by data subjects under the local law applicable to the data importer, or for data processing activities of the data exporter residing in Türkiye, under the Law.

Clause 9. **Redress**

In case of a dispute between a data subject and a data importer concerning third-party beneficiary rights under this Contract, the data subject may submit his/her requests to the data importer regarding the matter. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice to the data subjects or on its website, of a contact point authorised to handle requests. The data importer shall promptly address any requests it receives from data subjects.

Clause 10. **Liability**

(a) Each Party shall be liable to the other Party for the damages arising from any breach of this Contract.

(b) Each Party shall be liable to the data subject. The data subject shall be entitled to receive compensation, for any material or non-material damages that the Parties cause the data subject by breaching the third-party beneficiary rights under this Contract. This is without prejudice to the liability of the data exporter under the Law.

(c) Where both Parties are responsible for any damage caused to the data subject as a result of a breach of this Contract, all responsible Parties shall be severally liable, and the data subject is entitled to bring an action in court against any of these Parties.

(d) If one Party fully compensates the data subject for the damage under paragraph (c), it reserves the right of recourse against the other party in proportion to its fault.

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

PART III
National Law and Obligations in case of Access by Public Authorities
(This section shall be included in the contract where the processor, transferring data, combines the personal data received from the controller, receiving data, with personal data collected in Türkiye)

Clause 11. **National Law and Practices Affecting Compliance with the Contract**

The data importer agrees, declares, and undertakes that there are no national regulations or practices in conflict with this Contract regarding the personal data to be transferred under this Contract. In the event of changes in legislation or practices that may impact the data importer's ability to fulfil its obligations under this Contract during its term, the data importer shall notify the data exporter promptly, and in such a case, the data importer agrees that the data exporter reserves the right to suspend the data transfer or terminate this Contract.

Clause 12. **Obligations of the Data Importer in case of Access by Public Authorities**

The data importer shall notify the data exporter promptly of any requests from administrative or judicial authorities regarding the personal data transferred under this Contract, or if it becomes aware of any direct access by administrative or judicial authorities to personal data transferred pursuant to this Contract. In such a case, the data importer agrees that the data exporter shall have the right to suspend the data transfer or terminate this Contract, depending on the nature of the request or access.

PART IV
Final Provisions

Clause 13. Non-Compliance with the Contract and Termination

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

(b) In the event that the data importer is in breach of this Contract or unable to comply with this Contract, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the Contract is terminated. Provisions of Clause 11 and Clause 12 are reserved.

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

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with this Contract 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 this Contract,

iii) the data importer fails to comply with the decisions of a competent court regarding its obligations under this Contract.

In these cases, the data exporter shall inform the Personal Data Protection Board.

(d) In the event that the contract is terminated pursuant to paragraph (c), the data importer shall completely destroy all personal data collected by the data exporter in Türkiye and transferred, including its backups. The data importer warrants that, even if there are legislative provisions that may prevent it from fulfilling this obligation, it will continue to ensure compliance with this Contract, take necessary technical and organisational measures to safeguard the confidentiality of the personal data subject to transfer, and continue to processing activity only to the extent and for the duration required by legislation. The data importer shall certify the destruction of the data for the data exporter. Until the data is returned or completely destroyed, the data importer shall continue to ensure compliance with this Contract.

Clause 14. Governing Law

This Contract shall be governed by Turkish law.

Clause 15. Competent Court

(a) Any dispute arising from this Contract shall be resolved by Turkish courts.

(b) General provisions shall apply in terms of competence.

(c) The Parties agree to submit themselves to the jurisdiction of Turkish courts.

APPENDIX

ANNEX I

DESCRIPTION OF TRANSFER

The Annex I "**Description of Transfer**" of this Contract shall be deemed completed as follows:

i. The paragraph "**Activities of the Data Exporter Regarding the Personal Data Transferred Under This Contract**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Nature and purpose of the processing").

ii. The paragraph "**Activities of the Data Importer Regarding the Personal Data Transferred Under This Contract**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Nature and purpose of the processing").

iii. The paragraph "**Group or Groups of Data Subjects**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of data subjects").

iv. The paragraph "**Categories of Personal Data Transferred**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of Personal Data").

v. The paragraph "**Categories of Sensitive Personal Data Transferred**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Categories of Personal Data").

vi. For the purpose of the paragraph "**Legal Basis for the Transfer**", the legal basis for the Transfer should be the agreement between the data exporter and the data importer.

vii. The paragraph "**Frequency of the Transfer**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Duration of the processing / data retention periods / frequency of transfers").

viii. The paragraph "**Nature of the Processing Activity**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Nature and purpose of the processing").

ix. The paragraph "**Purposes of the Data Transfer and Further Processing**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Nature and purpose of the processing").

x. The paragraph "**Personal Data Retention Period**" shall be deemed completed with the information set out in the Annex 1 of this DPA (see "Duration of the processing / data retention periods / frequency of transfers").

xi. For the purpose of the paragraph "**Recipients or Recipient Groups**", the personal data transfers as described in Annex 1 and Annex 2 of this DPA.

xii. For the purpose of the paragraph "**Data Controller Registry Information System (VERBIS) Details of the Data Exporter**", the registration obligation of the data exporter should be [to be completed]

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

The Annex II "**Technical and organisational measures**" of this Contract shall be deemed completed with the information set out in Annex 3 to this DPA.

Annex 5 – Local Requirements

To give effect to Section 5 of this DPA, the parties wish to apply relevant local requirements to ensure lawful processing of Personal Customer Data and Partner Data, which is subject to each of the below jurisdictions, as applicable.

Annex 5a – United States Local Requirements

1. ***Definitions.*** As used in this Annex:

    a. ”Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a data subject’s personal data for monetary or other valuable consideration.

    b. “Share” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a data subject’s personal data for Cross-Context Behavioral Advertising, whether or not for monetary or other valuable consideration, including transactions for cross-context behavioral advertising in which no money is exchanged.

    c. “Cross-Context Behavioral Advertising” means the targeting of advertising to a data subject based on the data subject’s personal data obtained from the individual’s activity across businesses, distinctly branded websites, applications, or services.

    d. “NPPI” means, as applicable, (i) “non-public personal information” as such term is defined in the Gramm-Leach-Bliley Act or regulations promulgated thereunder governing the processing of NPPI and (ii) similar terms as defined under other US Privacy Legislation.

2. With respect to Personal Customer or Partner Data subject to US Privacy Legislation:

    a. Genesys shall comply with US Privacy Legislation, as applicable, and provide the same level of privacy protection as is required by US Privacy Legislation;

    b. Genesys shall promptly notify Partner if it makes a determination that it can no longer meet its obligations under US Privacy Legislation;

    c. The nature and purpose of Genesys’ processing is as set out in the section(s) of the DPA addressing the scope of services and term;

    d. The parties agree that no monetary or other valuable consideration is being provided by Genesys to Partner in exchange for Personal Customer or Partner Data, and Personal Customer or Partner Data is not being provided for purposes of Cross-Context Behavioral Advertising.

    e. Genesys shall not, except as otherwise permitted by US Privacy Legislation, the Master Agreement or this DPA:

        i. Sell or Share Personal Customer or Partner Data;

        ii. Retain, use or disclose Personal Customer or Partner Data (i) for any purpose or commercial purpose other than as reasonably necessary for the business purpose(s) of performing the services under the Master Agreement, or (ii) outside the direct business relationship between Genesys and Partner; or

        iii. Combine Personal Customer or Partner Data received pursuant to the Master Agreement with personal data received from or on behalf of another person(s), or collected from Genesys’ own interactions with individuals, except as necessary to perform the business purpose(s) of the services.

    f. To ensure that Genesys uses Personal Customer or Partner Data in a manner consistent with Customer’s or Partner’s obligations under US Privacy Legislation, and to stop and remediate any unauthorized use of Personal Customer or Partner Data, Genesys grants Customer or Partner the right to take the reasonable and appropriate steps of, upon appropriate notice, (i) requiring Genesys to provide responses to reasonable written privacy and cybersecurity audit questionnaires of reasonable length and scope and (ii) suspending any ongoing transfers of Personal Customer or Partner Data to Genesys.

    g. At Partner’s reasonable request, Genesys will reasonably assist Partner with Partner’s obligation to comply with individual requests to exercise rights under the U.S. Data Protection Laws applicable to Partner.

3. ***US Financial Privacy Laws.*** Genesys expressly understands and acknowledges that it may have access to, or that Partner may disclose to Genesys, NPPI. Without limiting any other obligations in this DPA, Genesys agrees that: (i) Genesys will use or disclose Customer or Partner NPPI only as necessary to carry out

the purposes for which Partner is disclosing NPPI to Genesys; and (ii) Genesys has implemented and will continue to maintain safeguards designed to do the following:

a. Ensure the security and confidentiality of Customer or Partner NPPI;

b. Protect against any anticipated threats to or hazards to the security or integrity of Customer or Partner NPPI; and

c. Protect against unauthorized access to or use of Customer or Partner NPPI that could result in harm or inconvenience to any individual.