

Genesys Data Processing Addendum

Controller to Processor Standard Contractual Clauses

This Data Processing Addendum (“DPA”) is entered into by and between Genesys Cloud Services B.V. and Customer, below defined, as of the date last executed by the Parties. This Addendum adds to, and is governed by, the Master Agreement (as further defined), and takes the form of the *Standard Contractual Clauses* (SCC) as issued by Decision (EU) 2021/915.¹

These SCC were drafted to oversee the relationship between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

For this Addendum to be effective, it is required that all contracting Parties reside within the European Union.

In the event that the Parties include a new company to this DPA through the contractual mechanism included for that purpose, and such company acts as Data Exporter for a restricted transfer of data from the United Kingdom, the Parties shall enter into Annex V to this DPA.

Genesys

Genesys Cloud Services B.V.

(the “Processor”)

Prins Bernhardplein 200, 1097 JB Amsterdam,
The NetherlandsDataPrivacy@genesys.com

[Genesys Signature]

Customer

[Customer]

(the “Controller”)

[Customer Address]

[Customer email]

[Customer Signature]

[Genesys Signatory]

Authorized Representative’s Name

[Genesys Signatory Title]

Title

[Month Day, Year]

[Customer Signatory]

Authorized Representative’s Name

[Customer Signatory Title]

Title

[Month Day, Year]

¹ Translations of such Standard Contractual Clauses to other languages are available in the following link: <https://eur-lex.europa.eu/legal-content/DE-EN/TXT/?from=de&uri=CELEX%3A32021D0915>

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

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

Clause 7

Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

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

7.3. Duration of the processing of personal data

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

7.4. Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

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

7.6. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

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

7.7. Use of sub-processors

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

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

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

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

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

7.8. International transfers

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

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

Clause 8

Assistance to the controller

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

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

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

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

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

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

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

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

Clause 9

Notification of personal data breach

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

9.1 Data breach concerning data processed by the controller

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

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

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

9.2 Data breach concerning data processed by the processor

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

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

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

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

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer/

1. Name:

Address:

Contact person's name, position and contact details:

Signature and accession date:

2.

(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer/

1. Name: Genesys Cloud Services B.V.

Address: Prins Bernhardphein 200, 1097 JB Amsterdam, The Netherlands

Contact person's name, position and contact details: William Dummett, Chief Privacy Officer. Shahzad Ahmad,

Data Privacy Officer. DataPrivacy@genesys.com

Signature and accession date:

2.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

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

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

Categories of personal data processed

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

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

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

Nature of the processing

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

Purpose(s) for which the personal data is processed on behalf of the controller

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

Duration of the processing

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

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

Genesys Cloud services are hosted by third party data center providers. Premise services operate on systems controlled and operated by the Customer. Genesys may share personal data with any affiliated Genesys entities under common control with Genesys for (i) troubleshooting and (ii) support.

Genesys may utilize sub-processors, depending on what services, features, and functionality the customer utilizes. Additional sub-processors may be selected by Customer in a customized environment, and if so, such sub-processor will be listed in a Statement of Work or Order Form.

Customer acknowledges that signature of such Statement of Work or Order Form constitutes written consent for use of such sub-processor named therein. Note that third party integrations, such as AppFoundry, **require a direct relationship** between the third party and the Customer.

The sub-processors listed at the following website (along with its subsidiary companies) may be utilized, depending on what services and functionality is selected by the Customer. Customer acknowledges that changes to this website shall constitute notice of changes to sub-processors in accordance with section 7.7 Use of Sub-processors of this DPA.

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

ANNEX III

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

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

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

Genesys Minimum Security Controls

This Appendix describes the minimum-security requirements generally applicable to Customer's use of Genesys Services. Additional controls for specific services or modules can be found in the applicable Agreement. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Therefore, Processor will use necessary reasonable technical, organizational and security measures designed to protect Personal Data of Customer in possession of Processor or otherwise processed by Processor against unauthorized access, alteration, disclosure or destruction, as further described in this Appendix:

1. Security Program

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

a. Security Awareness and Training

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

b. Policies and Procedures

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

c. Malware Prevention

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

2. Network Security

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

3. User Access Control

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

4. Business Continuity and Disaster Recovery

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

5. Security Incident Response

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

Cloud Services

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

1. Security Program

- 1.1. Security Standards. Genesys has implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect Customer Data, as appropriate to the nature and scope of the Cloud Services provided.
- 1.2. Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass. Specifically, with regard to Customer Data access, this includes annual compliance, information security, privacy, HIPAA security & privacy, and PCI training. Access to Genesys’ code repository requires additional annual training in secure development.
- 1.3. Policies and Procedures. Genesys will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated as necessary.
- 1.4. Change Management. Genesys will utilize a change management process based on Industry Standards to ensure that all changes to the Cloud Services environment are appropriately reviewed, tested, and approved.
- 1.5. Data Storage and Backup. Genesys will create backups of critical Customer Data. Customer Data will be stored and maintained using cloud provider-based Server-Side Encryption (SSE). Backup data will not be stored on portable media. Customer Data backups will be protected from unauthorized access.
- 1.6. Anti-virus and Anti-malware. Industry Standard anti-virus and anti-malware protection solutions are used on systems commonly affected by malware to protect the infrastructure that supports the Cloud Services against malicious software, such as Trojan horses, viruses, and worms. Genesys deploys File Integrity Management (FIM) solutions on all production systems, as well as robust monitoring of system access and command use. Cloud Services server instances are primarily Linux, which is a system not commonly affected by malware. Where Windows-based server instances are used, Industry Standard anti-malware software is deployed.
- 1.7. Vulnerability and Patch Management. Genesys will maintain a vulnerability management program that ensures compliance with Industry Standards. Genesys will assess all critical vulnerabilities to the Cloud Services production environment for access/vector complexity, authentication, impact, integrity, and availability. If the resulting risk is deemed to be “Critical” to Customer Data by Genesys, Genesys will endeavour to patch or mitigate affected systems within 7 working days. Certain stateful systems cannot be patched as quickly due to interdependencies and customer impact but will be remediated as expeditiously as practicable.
- 1.8. Data Deletion and Destruction. Genesys will, and will ensure that subprocessors will, follow Industry Standard processes to delete obsolete data and sanitize or destroy retired equipment that formerly held Customer Data. Recording retention policies are determined by Customer and can be used as part of a routine deletion process for recorded interactions. For instance, a recording retention policy can be created to delete conversations that occurred within a range of dates. All deletion within the Cloud Services is a simple deletion. Secure data deletion is not applicable in a virtual disk environment.
- 1.9. Penetration Testing. On at least an annual basis, Genesys will conduct a vulnerability assessment and penetration testing engagement with an independent qualified vendor. Issues identified during the engagement will be appropriately addressed within a reasonable time-frame commensurate with the identified risk level of the issue. Test results will be made available to Customer upon written request and will be subject to non-disclosure and confidentiality agreements.

2. Product Architecture Security

- 2.1. Logical Separation Controls. Genesys will employ effective logical separation controls based on Industry Standards to ensure that Customer Data is logically separated from other customer data within Cloud Services environment.
- 2.2. Firewall Services. Genesys uses firewall services to protect the Cloud Services infrastructure. Genesys maintains granular ingress and egress rules, and changes must be approved through Genesys’ change management system. Rulesets are reviewed semi-annually.
- 2.3. Intrusion Detection System. Genesys has implemented intrusion detection across the Cloud Services environment that meets PCI DSS requirements.
- 2.4. No Wireless Networks. Genesys will not use wireless networks within the Cloud Services environments.
- 2.5. Data Connections between Customer and the Cloud Services Environment. All connections to browsers, mobile apps, and other components are secured via Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS v1.2) over public Internet (note some Cloud Voice telephony cannot be due to carrier limitations).
- 2.6. Data Connections between the Cloud Services Environment and Third Parties. Transmission or exchange of Customer Data with Customer and any Genesys vendors will be conducted using secure methods (e.g., TLS 1.2, HTTPS, SFTP).

- 2.7. Encrypted Recordings. Genesys encrypts call recordings and chat sessions. Customer may elect to implement Local Key Encryption and maintain Customer's own keys for voice and screen recordings. To the extent required by applicable law or Customer's policies, Customer is responsible for the content of recordings and ensuring PCI Sensitive Authentication Data is not recorded, using applicable security features or other tools made available by Genesys.
- 2.8. Encryption Protection. Genesys uses Industry Standard methods to support encryption, with AES and TLS 1.2. Digital Recording encryption is addressed in Sections 2.7 and 7.6.
- 2.9. Logging and Monitoring. Genesys will log security events from the operating perspective for all infrastructure providing the Cloud Services to Customer. Genesys will monitor and investigate events that may indicate a Security Incident or problem. Event records will be retained at least one year. Limited audit data is accessible to customers via the User Interface (UI) and Application Programming Interface (API).

3. User Access Control

- 3.1. Access Control. Genesys will implement appropriate access controls to ensure only authorized Users have access to Customer Data within the Cloud Services environment.
- 3.2. Customer's User Access. Customer is responsible for managing User access controls within the application. The Cloud Services application password requirements are configurable by Customer for minimum length, minimum letters, minimum numerals, minimum special characters, password expiration, and minimum age. Genesys has a lockout period after several invalid attempts. Most Users experience a lockout period after 5 bad attempts, but Customer can automatically try again in 5 minutes. These settings are not configurable. Customer defines usernames and roles in a granular access permissions model. Customer is entirely responsible for any failure by itself, its agents, contractors or employees (including without limitation all its users) to maintain the security of all usernames, passwords and other account information under its control. Except in the event of a security lapse caused by Genesys' gross negligence or willful action or inaction, Customer is entirely responsible for all use of the Cloud Services through Customer's usernames and passwords, whether or not authorized by Customer, and all charges resulting from such use. Customer will immediately notify Genesys if Customer becomes aware of any unauthorized use of the Cloud Services.
- 3.3. Genesys' User Access. Genesys will create individual user accounts for each of Genesys' employees that have a business need to access Customer Data or Customer's systems within the Cloud Services environment. The following guidelines will be followed regarding Genesys' user account management:
 - 3.3.1. User accounts are requested and authorized by Genesys management.
 - 3.3.2. Strong password controls are systematically enforced.
 - 3.3.3. Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days and multi-factor authentication.
 - 3.3.4. Session time-outs are systematically enforced.
 - 3.3.5. User accounts are promptly disabled upon employee termination or role transfer that eliminates a valid business need for access.

4. Business Continuity and Disaster recovery

- 4.1. Disruption Protection. The Cloud Services will be deployed and configured in a high-availability design and will be deployed across separate Data Centers to provide optimal availability of the Cloud Services. The Cloud Services environment is physically separated from Genesys' corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the Cloud Services.
- 4.2. Business Continuity. Genesys will maintain a corporate business continuity plan designed to ensure that ongoing monitoring and support services will continue in the event of a disruption event involving the corporate environment.
- 4.3. Disaster Recovery. The Cloud Services platforms take advantage of the distributed nature of the infrastructure to enable full multi-site disaster recovery by operating in multiple availability zones ("AZ's"); distinct locations that are engineered to be insulated from each other. Independent application stacks are run in multiple AZ's. In the event of the loss of a single AZ or data center, the remaining Cloud Services remain operational and are designed to auto-scale to replace the lost system capacity.

5. Security Incident Response

- 5.1. Security Incident Response Program. Genesys will maintain a Security Incident response program based on Industry Standards designed to identify and respond to Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.
- 5.2. Notification. In the event of a Security Incident or other security event requiring notification under applicable law, Genesys will notify Customer within twenty-four (24) hours and will reasonably cooperate so that Customer can make any required notifications relating to such event, unless Genesys specifically requested by law enforcement or a court order not to do so.

- 5.3. **Notification Details.** Genesys will provide the following details regarding any Security Incidents to Customer: (i) date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions Genesys has already taken; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.
- 5.4. **Ongoing Communications.** Genesys will continue providing appropriate status reports to Customer regarding the resolution of the Security Incident and continually work in good faith to correct the Security Incident and prevent future such Security Incidents. Genesys will cooperate, as reasonably requested by Customer, to further investigate and resolve the Security Incident.
6. **Data Center Protections.** Genesys contracts with Data Centers for Platform as a Service (PaaS). Security and compliance certifications and/or attestation reports for Data Centers must be obtained directly from the Data Center. Data Center may require Customer to execute additional non-disclosure agreements.
7. **Use of the Cloud Services**
- 7.1. **Use Restrictions.** Customer will not, and will not permit or authorize others to, use the Cloud Services for any of the following: (i) to violate applicable law; (ii) to transmit malicious code; (iii) to transmit 911 or any emergency services (or reconfigure to support or provide such use); (iv) to interfere with, unreasonably burden, or disrupt the integrity or performance of the Cloud Services or third-party data contained therein; (v) to attempt to gain unauthorized access to systems or networks; or (vi) to provide the Cloud Services to non-User third parties, including, by resale, license, lend or lease.
- 7.2. **Customer Testing Restrictions.** Customer will not perform any type of penetration testing, Vulnerability Assessment, or Denial of Service attack on the Cloud Services production, test, or development environments.
- 7.3. **Prohibited Use.** Customer will use commercially reasonable efforts to prevent and/or block any prohibited use by Users.
- 7.4. **Customer Safeguards.** Customer will maintain a reasonable and appropriate administrative, physical, and technical level of security regarding its account ID, password, antivirus and firewall protections, and connectivity with the Cloud Services.
- 7.5. **VoIP Services Lines.** Customer shall maintain strict security over all VoIP Services lines. Customer acknowledges that Genesys does not provide Customer the ability to reach 911 or other emergency services, and Customer agrees to inform any individuals who may be present where the Cloud Services are used, or who use the Cloud Services, of the non-availability of 911 or other emergency dialling.
- 7.6. **Security Features.** If the Cloud Services will be used to transmit or process Personal Data, Customer will ensure that all Personal Data is captured and used solely via the use of security features made available by Genesys.
- 7.7. **Recordings.** Customer acknowledges that use of recordings is solely within Customer's discretion and control. Without limiting the foregoing: (i) Customer accepts sole responsibility for determining the method and manner of performing recording such that it is compliant with all applicable laws and for configuring and using the Cloud Services accordingly; and (ii) Customer shall ensure that recordings shall be made only for purposes required by and/or in compliance with, all applicable laws. Customer will ensure that: (a) recordings will not knowingly include any bank account number, credit card number, authentication code, Social Security number or Personal Data, except as permitted by all applicable laws; or (v) recordings are encrypted at all times. Customer shall not modify, disable, or circumvent the recording encryption feature within the Cloud Services.
8. **Industry-Specific Certifications.** Genesys security and operational controls are based on Industry Standard practices and are certified to meet the guidelines of PCI, SOC 2 Type 2, ISO 27001, and HIPAA. Nevertheless, Customer is solely responsible for achieving and maintaining any industry-specific certifications required for Customer's business.
9. **Audit.** Subject to Genesys' reasonable confidentiality and information security policies, Customer or a qualified third party chosen by Customer, shall have the right, not more than once a year and upon thirty (30) days' written notice, to perform a security assessment of Genesys' compliance with the terms of these Cloud Security Terms, provided that Customer has demonstrated that it has a reasonable belief that Genesys is not in compliance. During normal business hours, Customer or its authorized representatives may inspect Genesys policies and practices implemented to comply with these Cloud Security Terms, which may include a site visit and a review of reasonable supporting documentation, provided that Customer agrees that such right shall not include the right to on-site inspections or audits of any of Genesys' subcontractors, including Genesys' third-party hosting facilities and equipment. No such assessment shall violate Genesys' obligations of confidentiality to other customers or partners or reveal Genesys' intellectual property. Any assessment performed pursuant to this Section shall not interfere with the normal conduct of Genesys' business. Genesys shall cooperate with any reasonable requests made by Customer during the course of such assessments. Genesys reserves the right to charge Customer a reasonable fee for Genesys' costs incurred (including internal time spent) in connection with any Customer assessments, whether the assessment was performed remotely or on-site.

PureConnect Cloud

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

1. SECURITY PROGRAM

1.1 Security Certifications. Genesys has implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect the Customer Data as appropriate to the nature and scope of the Genesys PureConnect Cloud Services provided. Genesys has developed and will maintain an information security and awareness program that is delivered to all its employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

1.2 Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

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

1.4 Change Management. Genesys will utilize a change management process based on industry standards to ensure that all changes to Customer’s environment are appropriately reviewed, tested, and approved.

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

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

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

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

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

2. NETWORK SECURITY

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

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

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

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

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

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

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

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

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

3. USER ACCESS CONTROL

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

3.2 Customer's User Access. Customer is responsible for managing user access controls within the application. Customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for its users. Customer is entirely responsible for any failure by itself, its agents, contractors or employees (including without limitation all its users) to maintain the security of all usernames, passwords and other account information under its control. Except in the event of a security lapse caused by Genesys' gross negligence or willful action or inaction, Customer is entirely responsible for all use of the Genesys PureConnect Cloud Service through its usernames and passwords whether or not authorized by Customer and all charges resulting from such use. Customer will immediately notify Genesys if Customer becomes aware of any unauthorized use of the Genesys PureConnect Cloud Service.

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

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

(B) Strong password controls are systematically enforced.

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

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

(E) Session time-outs are systematically enforced.

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

4. BUSINESS CONTINUITY AND DISASTER RECOVERY

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

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

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

5. SECURITY INCIDENT RESPONSE

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

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

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

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

6. DATA CENTER PROTECTIONS

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

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

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

7. RIGHT TO AUDIT

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

8. PRIVACY

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

9. INDUSTRY SPECIFIC CERTIFICATIONS

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

10. PREMIUM SERVICES

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

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

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

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

Premise Support Security

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

1. SECURITY PROGRAM

1.1 Security controls. Genesys has implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect the Customer Data as appropriate to the nature and scope of the services provided. Genesys has developed and will maintain an information security and awareness program that is delivered to all its employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

1.2 Security Awareness and Training. Genesys has developed and will maintain an information security and awareness program that is delivered to all employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

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

1.4 Change Management. Genesys will utilize a change management process based on industry standards to ensure that all changes to Customer's environment are appropriately reviewed, tested, and approved.

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

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

2. USER ACCESS CONTROL

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

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

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

(B) Strong password controls are systematically enforced.

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

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

(E) Session time-outs are systematically enforced.

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

3. BUSINESS CONTINUITY AND DISASTER RECOVERY

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

4. SECURITY INCIDENT RESPONSE

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

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

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

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

Genesys DX Security

1. Products and Services

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

2. Product Architecture

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

2.1 Storage and Service

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

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

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

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

3. Genesys DX Technical Security Controls

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

3.1 Logical Access Control

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

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

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

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

3.2 Perimeter Defense and Intrusion Detection

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

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

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

3.3 Data Segregation

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

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

3.4 Physical Security

Data center Physical Security

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

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

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

3.5 Data Backup, Disaster Recovery, Availability

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

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

3.6 Malware Protection

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

3.7 Encryption

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

In-Transit Encryption

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

At-Rest Encryption

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

3.8 Vulnerability Management

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

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

3.9 Logging and Alerting

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

4. Organizational Controls

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

4.1 Security Policies and Procedures

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

4.2 Standards Compliance

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

- International Organization for Standardization – ISO/IEC 27001:2013 Information Security Management System (ISMS) Certification
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)

- Payment Card Industry Data Security Standard (PCI DSS) Compliance for Genesys' eCommerce and Payment Environments

4.3 Security Operations and Incident Management

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

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

4.4 Application Security

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

4.5 Personnel Security

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

4.6 Security Awareness and Training Programs

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

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

5. Privacy Practices

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

5.1 Data Protection and Privacy Policy

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

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

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

5.2 GDPR

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

5.3 CCPA

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

5.4 Transfer Frameworks

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

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

5.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (or "SCCs") are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law. Genesys has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. Genesys offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of

personal data for in-scope Genesys services as part of its global DPA. Execution of the SCCs helps ensure that Genesys customers can freely move data from the EEA to the rest of the world.

5.5 Return and Deletion of Customer Content

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

5.6 Sensitive Data

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

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

5.7 Tracking and Analytics

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

6. Third Parties

6.1 Use of Third Parties

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

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

6.2 Contract Practices

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

ANNEX IV**List of sub-processors****EXPLANATORY NOTE:**

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

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

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

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

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

ANNEX V

UK International Data Transfer Agreement

This International Data Transfer Agreement (IDTA) has been incorporated to this DPA as issued by the Information Commissioner’s Office. Its purpose is to be used by Parties making restricted transfers. It shall be used where Customer envisages to engage a company based in the United Kingdom and where such company requires to perform personal data transfer activities as required by the Master Agreement.

The content of this IDTA is considered as providing appropriate safeguards for restricted data transfers. It shall be read together with the applicable TOMs as provided under Annex III to the DPA.

Part 1: Tables

Table 1: Parties and signatures

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties’ details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Importer Data Subject Contact		Job Title: Contact details including email:
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the Exporter set out above Signed: Date of signature: Full name: Job title:	Signed for and on behalf of the Importer set out above Signed: Date of signature: Full name: Job title:

Table 2: Transfer Details

UK country’s law that governs the IDTA:	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
--	--

Primary place for legal claims to be made by the Parties	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller <input type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	<input type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	<p>If the Importer is the Exporter's Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:</p> <p>Name of agreement: <input type="text"/></p> <p>Date of agreement: <input type="text"/></p> <p>Parties to the agreement: <input type="text"/></p> <p>Reference (if any): <input type="text"/></p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement: <input type="text"/></p> <p>Date of agreement: <input type="text"/></p> <p>Parties to the agreement: <input type="text"/></p> <p>Reference (if any): <input type="text"/></p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:</p> <p>Name of agreement: <input type="text"/></p> <p>Date of agreement: <input type="text"/></p> <p>Parties to the agreement: <input type="text"/></p> <p>Reference (if any): <input type="text"/></p>
Term	The Importer may Process the Transferred Data for the following time period: <input type="checkbox"/> the period for which the Linked Agreement is in force <input type="checkbox"/> time period: <input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.

<p>Ending the IDTA before the end of the Term</p>	<p><input type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.</p> <p><input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving: [redacted] months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).</p>
<p>Ending the IDTA when the Approved IDTA changes</p>	<p>Which Parties may end the IDTA as set out in Section 29.2:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
<p>Can the Importer make further transfers of the Transferred Data?</p>	<p><input type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p> <p><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p>
<p>Specific restrictions when the Importer may transfer on the Transferred Data</p>	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input type="checkbox"/> to: [redacted]</p> <p><input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in:</p> <p><input type="checkbox"/> there are no specific restrictions.</p>
<p>Review Dates</p>	<p><input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data</p> <p>First review date: [redacted]</p> <p>The Parties must review the Security Requirements at least once:</p> <p><input type="checkbox"/> each [redacted] month(s)</p> <p><input type="checkbox"/> each quarter</p> <p><input type="checkbox"/> each 6 months</p> <p><input type="checkbox"/> each year</p> <p><input type="checkbox"/> each [redacted] year(s)</p> <p><input type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment</p>

Table 3: Transferred Data

<p>Transferred Data</p>	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <p><input type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
--------------------------------	---

<p>Special Categories of Personal Data and criminal convictions and offences</p>	<p>The Transferred Data includes data relating to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> racial or ethnic origin <input type="checkbox"/> political opinions <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input type="checkbox"/> none of the above <input type="checkbox"/> set out in: <p>And:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
<p>Relevant Data Subjects</p>	<p>The Data Subjects of the Transferred Data are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
<p>Purpose</p>	<ul style="list-style-type: none"> <input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes: <input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <ul style="list-style-type: none"> <input type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

<p>Security of Transmission</p>	
<p>Security of Storage</p>	
<p>Security of Processing</p>	
<p>Organisational security measures</p>	

Technical security minimum requirements	
Updates to the Security Requirements	<input type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

To include if any.

Part 4: Mandatory Clauses

Information to interpret this IDTA.

1. The IDTA and related Agreements

- 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
- 1.2 This IDTA is made up of:
 - 1.2.1 Part one: Tables;
 - 1.2.2 Part two: Extra Protection Clauses;
 - 1.2.3 Part three: Commercial Clauses; and
 - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. Provision of all the information required

- 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
 - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
 - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. Signature of the IDTA

- 4.1 The Parties may choose to each sign (or execute):
 - 4.1.1 the same copy of this IDTA;
 - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
 - 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

In addition to the above, the Parties may choose that the signature takes the form of an Amendment to the Data Processing Agreement under the Master Agreement.

5. Changes to this IDTA

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
 - 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
 - 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
 - 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
 - 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, **the ICO may publish a revised Approved IDTA** which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Applicable Law

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

8. Appropriate Safeguards

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
- 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
 - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:
- 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
 - 8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.
- 8.3 The Importer must:
- 8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the “Importer Information”);
 - 8.3.2 co-operate with the Exporter to ensure compliance with the Exporter’s obligations under the UK Data Protection Laws;
 - 8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
 - 8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
- 8.4 The Importer must ensure that at the Start Date and during the Term:
- 8.4.1 the Importer Information is accurate;
 - 8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
- 8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach. The Parties may wish to include these measures as an Annex to the DPA and it shall be referenced as applicable to the IDTA.

9. Reviews to ensure the Appropriate Safeguards continue

- 9.1 Each Party must:
- 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
 - 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
- 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

- 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
- 9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO as supervisory authority

- 10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
- 10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
- 10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

11. Exporter's obligations

- 11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
- 11.2 The Exporter must:
 - 11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
 - 11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
 - 11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.
- 11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
- 11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
- 11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

12. General Importer obligations

- 12.1 The Importer must:
 - 12.1.1 only Process the Transferred Data for the Purpose;
 - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
 - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
 - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
 - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
 - 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
- 12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

- 13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

- 13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
- 13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.
- 13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:
- Section 14 (Importer's obligations to comply with key data protection principles);
 - Section 15 (What happens if there is an Importer Personal Data Breach);
 - Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
 - Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).
- 14. Importer's obligations to comply with key data protection principles**
- 14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.
- 14.2 The Importer must:
- 14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
- 14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and
- 14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
- 15. What happens if there is an Importer Personal Data Breach**
- 15.1 If there is an Importer Personal Data Breach, the Importer must:
- 15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and
- 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
- 15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
- 15.2.1.1 a description of the nature of the Importer Personal Data Breach;
- 15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
- 15.2.1.3 likely consequences of the Importer Personal Data Breach;
- 15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
- 15.2.1.5 contact point for more information; and
- 15.2.1.6 any other information reasonably requested by the Exporter,
- 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

- 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
- 15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
- 15.3.1 a description of the nature of the Importer Personal Data Breach;
 - 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.3.3 likely consequences of the Importer Personal Data Breach;
 - 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.3.5 contact point for more information; and
 - 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
 - 16.1.2 the third party has been added to this IDTA as a Party; or
 - 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
 - 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
 - 16.1.5 the transfer is to the UK or an Adequate Country.

- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
- 17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. Exercise of Data Subjects Rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

- 20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
 - 20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Data Subject requests, the Importer must:
- 20.5.1 rectify inaccurate or incomplete Transferred Data;
 - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
 - 20.5.3 cease using it for direct marketing purposes; and
 - 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the “Decision-Making”), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
- 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
 - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
 - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.
- 21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor**
- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
- 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws**
- 22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
- 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or
 - 22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or
 - 22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.
- If the Importer refuses an individual’s request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.
- 23. Access requests and direct access**
- 23.1 In this Section 23 an “Access Request” is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and “Direct Access” means direct access to any Transferred Data by public authorities of which the Importer is aware.
- 23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
- 23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.
- 23.4 In so far as Local Laws allow, the Importer must:

- 23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and
- 23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

- 24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
- 24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
- 24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

- 25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:
 - 25.1.1 contain all the terms and conditions agreed by the Parties; and
 - 25.1.2 override all previous contacts and arrangements, whether oral or in writing.
- 25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- 25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- 25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
- 25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- 25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
 - 25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;
 - 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
 - 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

26. Breaches of this IDTA

- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
 - 26.1.1 has breached this IDTA; or
 - 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

- 26.2 In this IDTA “Significant Harmful Impact” means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.
- 27. Breaches of this IDTA by the Importer**
- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
- 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;
- 27.2.2 If the Importer is the Exporter’s Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
- 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
- 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and
- 27.2.3.2 if the third party receiver is the Importer’s Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
- 27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.
- 28. Breaches of this IDTA by the Exporter**
- 28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
- 28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.
- 29. Termination of the IDTA**
- 29.1 The IDTA will end:
- 29.1.1 at the end of the Term stated in Table 2: Transfer Details; or
- 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
- 29.1.3 at any time that the Parties agree in writing that it will end; or
- 29.1.4 at the time set out in Section 29.2.
- 29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 “Ending the IDTA when the Approved IDTA changes”, will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:
- 29.2.1 its direct costs of performing its obligations under the IDTA; and/or
- 29.2.2 its risk under the IDTA,
- and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. Termination for breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. Effects of Termination

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and related Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Applicable Law);
- **Section 10** (The ICO as supervisory authority);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);

- **Section 31** (Effects of Termination);
- **Section 32** (Liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

32. **Liability**

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, “Party One”) agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One’s breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One’s breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One’s Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party’s responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. **How Relevant Data Subjects and the ICO may bring legal claims**

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (Provision of all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter’s obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer’s obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer’s obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer’s responsibility if it authorises others to perform its obligations);

- **Section 18** (The right to a copy of the IDTA);
 - **Section 19** (The Importer's contact details for the Relevant Data Subjects);
 - **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
 - **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
 - **Section 23** (Access Requests and Direct Access);
 - **Section 26** (Breaches of this IDTA);
 - **Section 27** (Breaches of this IDTA by the Importer);
 - **Section 28** (Breaches of this IDTA by the Exporter);
 - **Section 30** (Termination for breach);
 - **Section 31** (Effects of Termination); and
 - any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.
- 33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10, Sections 11.1 and 11.2, Section 12.1.6 and Section 13.
- 33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
- 33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
- 33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.
- 34. Courts legal claims can be brought in**
- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).
- 35. Arbitration**
- 35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.
- 35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.
- 35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

- 35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.
- 35.5 The English language must be used in the arbitral proceedings.
- 35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	Legal definition
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: <ul style="list-style-type: none"> • a territory; • one or more sectors or organisations within a third country; • an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.

Word or Phrase	Legal definition
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.

Word or Phrase	Legal definition
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
--------------------------	--