DATA PROCESSING AGREEMENT

Version: 1.1
Effective Date: 1 June 2026
Document Owner: Greenhouse IT

This Data Processing Agreement ("DPA") forms part of the Principal Agreement between the customer identified in the applicable order, subscription confirmation or account registration
(the "**Controller**")

and

Greenhouse IT Pte. Ltd.
1 Scotts Road, Shaw Centre #21-10
Singapore 228208
UEN: 202345780W
(the "**Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Controller acts as the Controller of Personal Data within the meaning of the GDPR.
(B) The Controller wishes to engage the Processor to provide certain cloud-based software services involving the Processing of Personal Data on behalf of the Controller.
(C) The Parties wish to implement this DPA in order to comply with Article 28 of Regulation (EU) 2016/679 (General Data Protection Regulation - "GDPR") and other applicable Data Protection Laws.
(D) The Parties wish to lay down their rights and obligations.

1. Definitions and Interpretation

1.1. The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
1.2. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
1.2.1. "**Controller Personal Data**" means any Personal Data processed by the Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement;
1.2.2. "**Data Protection Laws**" means Applicable Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
1.2.3. "**Data Transfer**" means a transfer of Controller Personal Data to a Subprocessor or any onward transfer by a Subprocessor where such transfer is subject to applicable Data Protection Laws;

1.2.4. "**EEA**" means the European Economic Area;
1.2.5. "**EU Data Protection Laws**" means the GDPR and all applicable laws implementing or supplementing the GDPR;
1.2.6. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation);
1.2.7. "**Principal Agreement**" means the Terms of Use agreed between the Parties, together with any applicable order, subscription confirmation, statement of work or other written agreement governing the provision and use of the Services;
1.2.8. "**Services**" means the aniSYS software-as-a-service platform and related hosting, maintenance, backup, monitoring and support services provided by the Processor;
1.2.9. "**Subprocessor**" means any third party appointed by or on behalf of the Processor to Process Controller Personal Data in connection with the Services.

2. Roles of the Parties

2.1. The Controller determines the purposes and means of the Processing of Controller Personal Data. The Processor Processes Controller Personal Data only on behalf of and in accordance with documented instructions from the Controller, unless required to do otherwise by applicable law.
2.2. The Principal Agreement, this DPA and any documented instructions provided by the Controller in connection with the use of the Services constitute the Controller's documented instructions to the Processor. The Controller acknowledges that its configuration and authorised use of the Services constitute documented instructions.

3. Subject Matter, Duration, Nature and Purpose of Processing

3.1. The subject matter, duration, nature and purpose of the Processing are the provision, operation, maintenance, security and support of the Services for the Controller.
3.2. The duration of Processing corresponds to the term of the Principal Agreement and any additional period required for data export, deletion, backup retention or legal compliance.
3.3. Further details shall be set out in Annex I (Details of Processing).

4. Processor Obligations

4.1. The Processor shall comply with applicable Data Protection Laws in relation to its Processing of Controller Personal Data.
4.2. The Processor shall not Process Controller Personal Data other than on the Controller's documented instructions, except where required by applicable law. In such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest.
4.3. The Processor shall immediately inform the Controller if it considers that an instruction infringes applicable Data Protection Laws.
4.4. The Processor shall ensure that persons authorised to Process Controller Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
4.5. The Processor shall implement and maintain appropriate technical and organisational measures as described in Annex II.

5. Processor Personnel

5.1. The Processor shall take reasonable steps to ensure the reliability of employees, contractors and other personnel who may have access to Controller Personal Data.
5.2. Access to Controller Personal Data shall be limited to personnel who require such access for the performance of the Services, support, maintenance, security or legal obligations.

6. Security of Processing

6.1. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6.2. Such measures may include, as appropriate, encrypted transmission, access controls, role-based permissions, logging, monitoring, firewalls, backup and restore procedures, security updates, logical separation of customer environments and protection against unauthorised access.

6.3. The Processor may modify, update or replace its technical and organisational measures from time to time in order to reflect technological developments, changes to the Services, security improvements or evolving industry practices, provided that such modifications do not materially reduce the overall level of protection afforded to Controller Personal Data.

7. Subprocessing

7.1. The Controller grants the Processor a general authorisation to engage Subprocessors for the provision of the Services, subject to the conditions of this clause.

7.2. The Processor shall maintain a list of authorised Subprocessors in Annex III or in another location made available to the Controller.

7.3. The Processor shall ensure that each Subprocessor is bound by written obligations that are no less protective, in substance, than those set out in this DPA, to the extent applicable to the nature of the services provided by the Subprocessor.

7.4. The Processor shall remain responsible to the Controller for the performance of its Subprocessors' obligations.

7.5. The Processor shall provide reasonable prior notice of any intended addition or replacement of Subprocessors and shall provide the Controller with an opportunity to raise reasonable objections where required under applicable Data Protection Laws.

8. Data Subject Rights

8.1. Taking into account the nature of the Processing, the Processor shall assist the Controller, by appropriate technical and organisational measures insofar as possible, in fulfilling the Controller's obligation to respond to requests for exercising Data Subject rights under Data Protection Laws.

8.2. If the Processor receives a request from a Data Subject relating to Controller Personal Data, the Processor shall promptly notify the Controller and shall not respond to the request except on the documented instructions of the Controller or as required by applicable law.

9. Personal Data Breach

9.1. The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Controller Personal Data.

9.2. The notification shall include information reasonably available to the Processor to assist the Controller in meeting any obligations to notify a Supervisory Authority or affected Data Subjects.

9.3. The Processor shall take reasonable steps to investigate, mitigate and remediate the Personal Data Breach and shall cooperate with the Controller in this regard.

10. Assistance with Compliance

10.1. Taking into account the nature of Processing and the information available to the Processor, the Processor shall provide reasonable assistance to the Controller with obligations under Articles 32 to 36 GDPR, including security of processing, breach notifications, data protection impact assessments and prior consultations with Supervisory Authorities.

10.2. The Processor may charge reasonable fees for assistance that is not included in the standard Services, unless such assistance is required due to a breach of this DPA by the Processor.

11. Deletion or Return of Controller Personal Data

11.1. Upon termination of the Services, the Processor shall make Controller Personal Data available for export for a period of one month, unless otherwise agreed in the Principal Agreement.

11.2. After the end of the export period, the Processor shall delete or anonymise Controller Personal Data in accordance with its deletion procedures, unless applicable law requires continued storage.

11.3. Backup copies shall be deleted in accordance with the Processor's regular backup lifecycle and retention procedures. During backup retention, the Processor shall continue to protect Controller Personal Data in accordance with this DPA.

11.4. Upon request, the Processor shall provide written confirmation of deletion after completion of the deletion process.

12. Audit and Information Rights

12.1. The Processor shall make available to the Controller information reasonably necessary to demonstrate compliance with this DPA.

12.2. Audits and inspections shall be subject to reasonable prior written notice, confidentiality obligations, appropriate security restrictions, and shall be conducted in a manner that does not unreasonably disrupt the Processor's business operations or compromise the security or confidentiality of other customers.

12.3. The Controller shall first rely on documentation, security information, certificates, reports or written responses made available by the Processor before requesting an on-site audit.

13. International Data Transfers

13.1. The Controller acknowledges that the Processor is established in Singapore and that Controller Personal Data may be processed in the European Union, Singapore and other locations where authorised Subprocessors provide services.

13.2. Where Controller Personal Data is transferred from the European Economic Area ("EEA") to a country that is not recognised by the European Commission as providing an adequate level of protection pursuant to Article 45 GDPR, the Parties shall rely on the Standard Contractual Clauses set out in Appendix A to this DPA (Commission Implementing Decision (EU) 2021/914, Module Two (Controller to Processor)), or any successor transfer mechanism recognised under applicable Data Protection Laws.

13.3. The Standard Contractual Clauses contained in Appendix A are hereby incorporated into and form an integral part of this DPA. The Parties agree that the information required by Annexes I, II and III to the Standard Contractual Clauses is provided by Annex I (Details of Processing), Annex II (Technical and Organisational Measures) and Annex III (Approved Subprocessors) of this DPA, which are incorporated into the Standard Contractual Clauses by reference.

14. Confidentiality

14.1. Each Party shall keep confidential all information received from the other Party in connection with this DPA that is marked confidential or should reasonably be understood to be confidential.

14.2. This obligation does not apply to information that is publicly available, already lawfully known, independently developed, or required to be disclosed by law.

15. Liability

15.1. Liability arising under or in connection with this DPA shall be governed by the liability provisions of the Principal Agreement, unless mandatory Data Protection Laws provide otherwise.

16. Order of Precedence

16.1. In the event of a conflict between this DPA and the Principal Agreement with regard to the Processing of Controller Personal Data, this DPA shall prevail to the extent of that conflict.

16.2. In the event of a conflict between this DPA and applicable Standard Contractual Clauses, the Standard Contractual Clauses shall prevail to the extent of that conflict.

17. Governing Law and Jurisdiction

17.1. This DPA shall be governed by the governing law specified in the Principal Agreement.

17.2. The courts specified in the Principal Agreement shall have jurisdiction, subject to mandatory provisions of applicable Data Protection Laws and any jurisdiction rules contained in applicable Standard Contractual Clauses.

ANNEX I

DETAILS OF PROCESSING

This Annex forms part of the Data Processing Agreement (DPA) between the Controller and Greenhouse IT Pte. Ltd. It describes the scope, nature and purpose of the Processing of Controller Personal Data carried out by the Processor in connection with the aniSYS cloud platform.

1. Subject Matter of the Processing

The Processor provides the cloud-based aniSYS software-as-a-service platform together with hosting, maintenance, monitoring, backup, restore and technical support services. aniSYS is designed for animal shelters and animal welfare organisations and supports the operational, administrative and veterinary activities of the Controller.

The Services enable the Controller to manage animal records, veterinary documentation, adoptions, foster homes, volunteers, donors, members, cooperation partners, transport activities, public website publication and related organisational processes.

2. Duration of the Processing

Processing begins when the Controller subscribes to the Services and continues for the duration of the Principal Agreement.

Following termination, Controller Personal Data remains available for export for one (1) month. Thereafter the Processor deletes or anonymises Controller Personal Data in accordance with the DPA, applicable law and documented backup retention procedures. Backup copies may remain until their scheduled expiry but remain protected by the same security measures.

3. Nature of the Processing

Processing activities performed by the Processor include:

1. Collection, recording and organisation of data entered by authorised users.
2. Storage, hosting and logical segregation of customer environments.
3. Retrieval, consultation, display and search.
4. Role-based access control and authentication.
5. Publication of selected information under the Controller's instructions.
6. Creation and retention of backups and restoration where required.
7. Export of Controller Personal Data.
8. Deletion or anonymisation of data.
9. Technical support, maintenance, monitoring and security operations.

4. Purpose of the Processing

1. Controller Personal Data is processed solely for providing and securing the Services.
2. Animal shelter administration
3. Animal admission and intake
4. Veterinary treatments and medication records
5. Animal adoption management
6. Foster home management
7. Volunteer management
8. Membership and donor administration
9. Management of cooperation partners
10. Website publication of animals

11. User authentication and authorisation
12. Backup, disaster recovery and information security
13. Customer support

5. Categories of Data Subjects

1. Prospective adopters
2. Adopters
3. Foster homes
4. Members
5. Donors
6. Employees and authorised users
7. Volunteers
8. Veterinarians and veterinary clinics
9. Transport providers
10. Partner organisations
11. Municipal and public authority contacts
12. Persons reporting found animals
13. Flight sponsors
14. Other cooperation partners

6. Categories of Personal Data

6.1 Identity and contact data:

- Name
- Postal address
- Email address
- Telephone number
- Preferred language
- Date of birth (where provided)

6.2 Account and authentication data:

- Username
- Password hash
- Assigned roles and permissions
- Account status

6.3 Operational data:

- Donation history
- Membership information
- Adoption records
- Comments, notes and free-text information entered by authorised users

6.4 Uploaded content:

- Contracts
- Reports
- PDF documents
- Word documents
- Excel documents

- Photographs
- Links to supported video platforms

Technical information:

The Processor does not intentionally store IP addresses or browser fingerprints as part of the Services. Limited browser information, such as preferred language settings, may be processed temporarily to provide the user interface.

7. Special Categories of Personal Data

The Services are not designed for the collection or management of special categories of Personal Data within the meaning of Article 9 GDPR or personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR. The Processor does not provide dedicated functionality for the collection or management of such data.
The Controller remains solely responsible for determining the categories and content of Personal Data processed through the Services and for ensuring that such Processing complies with applicable Data Protection Laws.

8. User and Permission Model

User accounts are created and managed exclusively by the Controller. Each user must activate the account through an email confirmation process. The Controller assigns one or more roles to each user. The Processor provides a role-based permission model that enables the Controller to restrict access to Controller Personal Data according to job responsibilities.

- Animal keeper
- Veterinary
- Animal agent
- Office staff
- Shelter management
- Chairman
- Publisher
- Photographer
- Veterinary authority
- Vet helper
- Other custom role combinations configured by the Controller

9. Website Publication

The Services allow the Controller to publish animal profiles through embedded website galleries. Publication is always controlled by the Controller. Optional publication of foster home names may be enabled by the Controller. Users may create website texts and upload media. The Processor does not review or moderate customer-generated content.

The Controller remains solely responsible for determining whether any Personal Data is published through the Services and for ensuring that such publication complies with applicable Data Protection Laws.

10. Technical Support

Support requests are initiated through the Processor's ticketing system. Access to Controller Personal Data for support purposes occurs only where necessary to resolve a reported issue and only by authorised personnel. Ticket content may contain Personal Data provided by the Controller.

11. International Processing and Subprocessors

Controller Personal Data may be processed within the European Union and Singapore in connection with the provision of the Services. The Processor currently engages the Subprocessors identified in Annex III for specific infrastructure and support services. The Processor remains responsible for the acts and omissions of its Subprocessors in accordance with the DPA.

Where Processing involves an international transfer of Controller Personal Data, such transfer shall be carried out in accordance with Section 13 of the DPA and, where applicable, the Standard Contractual Clauses contained in Appendix A. Processing takes place within the European Union and Singapore. Approved subprocessors currently include Amazon Web Services (hosting), Mailgun (email delivery). International transfers are governed by Section 13 of the DPA.

12. AI-assisted Features

The Processor may introduce optional AI-assisted features to support authorised users when drafting texts or completing forms. Such features will operate only under the Controller's instructions. Their scope and data flows will be documented before production use.

13. Data Export

Authorised users may export Controller Personal Data in commonly used electronic formats, including CSV, Microsoft Excel and PDF, subject to the permissions assigned by the Controller. The scope of exported data depends on the permissions configured by the Controller and the functionality available within the Services.

The Processor does not retain exported files after completion of the export process unless such files form part of routine backup procedures or are otherwise required for the provision of the Services. Authorised users may export Controller Personal Data in commonly used electronic formats including CSV, Microsoft Excel and PDF, subject to the permissions assigned by the Controller.

14. Additional Information

The Processor removes embedded image metadata from uploaded photographs, except where retention of the original capture date is required for functional purposes.

Videos are referenced via supported external platforms and are not stored directly within the Services. The Controller remains solely responsible for determining which external video content is referenced through the Services and for ensuring that such references and any associated Processing of Personal Data comply with applicable Data Protection Laws.

The Processor removes embedded image metadata from uploaded photographs, except where retention of the original capture date is required for functional purposes. Videos are referenced via supported external platforms and are not stored directly within the Services.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

This Annex forms part of the Data Processing Agreement (DPA) between the Controller and Greenhouse IT Pte. Ltd. It describes the technical and organisational measures implemented to protect Controller Personal Data in accordance with Article 32 GDPR.

1. **Information Security Governance**
   - Formally appointed Data Security Officer.
   - Employees and contractors are bound by confidentiality obligations and receive security and data protection guidance.
   - Least-privilege access principles are applied.
2. **Physical Security**
   - No on-premises infrastructure is operated.
   - Physical security is provided by Amazon Web Services.
3. **Infrastructure Security**
   - Amazon EKS with managed node groups and Amazon Linux.
   - Private Kubernetes clusters and private VPC subnets.
   - Application Load Balancers with TLS termination.
   - Private administration through VPN and hardened bastion host.
   - Security Groups and Network ACLs follow AWS best practices.
4. **Identity and Access Management**
   - AWS IAM roles and service accounts following least privilege.
   - MFA for administrative AWS accounts.
   - Secrets stored in encrypted Vaults.
   - Credential rotation process being introduced.
5. **Encryption**
   - TLS 1.2/1.3 enforced using AWS ELB security policy.
   - AWS ACM managed certificates.
   - EFS encryption at rest.
   - S3 Server-Side Encryption (SSE-S3).
   - AWS Backup encrypted with AWS KMS.
   - SSH key authentication only.
6. **Application Security**
   - Laravel and PHP with regular security updates.
   - Laravel validation, Eloquent ORM, CSRF and XSS protection.
   - Custom rate limiting.
   - 60 minute session timeout.

7. **Authentication and Authorisation**
    - Strong password policy.
    - Secure password hashing.
    - Mandatory email verification.
    - Role-Based Access Control.
    - Customer administrators may disable accounts and reset passwords.
8. **Customer Data Isolation**
    - Dedicated web instance, Database instance and namespace per customer.
9. **Logging and Monitoring**
    - Application logs retained for three months.
    - Last login information recorded.
    - Continuous infrastructure and application monitoring.
    - Administrative access only via VPN and bastion host.
10. **Backup and Disaster Recovery**
    - Daily backups.
    - Three-month daily retention and 365-day monthly retention.
    - AWS KMS encrypted backups.
    - Quarterly restore tests.
    - Operational recovery objectives currently target an RPO of up to 24 hours and an RTO of approximately 30 minutes. These objectives represent internal operational targets only and do not constitute contractual service level commitments.
11. **Vulnerability Management**
    - Regular security updates.
    - Critical updates generally deployed within one week.
    - Container vulnerability scanning implemented.
12. **Incident Response**
    - Automated monitoring.
    - Email and telephone alerting.
    - Documented recovery procedures with automation.
13. **Business Continuity**
    - Continuous availability and performance monitoring.
    - Automated alerting.
14. **Data Deletion**
    - Authorised deletion within the application.
    - Automated backup deletion according to retention.
    - Complete environment deletion after termination and export period.

15. Personnel Security

- Confidentiality obligations.
- Support access only for authorised ticket-based requests.

16. Secure Development

- Source code is maintained in a private version control system with access restricted to authorised personnel.
- Secure CI/CD pipelines are used for software build and deployment.
- Code changes are subject to peer review under the four-eyes principle.
- Container images are stored in private container registries with restricted access.
- Future AI Services
  - No AI processing of Controller Personal Data is currently performed.
  - Any future AI-assisted feature will be documented and, where required by applicable Data Protection Laws, subject to an update of this DPA.

17. Continuous Improvement

- Technical and organisational measures are reviewed and improved on an ongoing basis.

ANNEX III

APPROVED SUBPROCESSORS

This Annex forms part of the Data Processing Agreement (DPA) between the Controller and Greenhouse IT Pte. Ltd.. It identifies the Subprocessors authorised by the Processor to Process Controller Personal Data in connection with the aniSYS Services.

1. General

The Processor carefully selects its Subprocessors based on technical competence, security standards, operational reliability and compliance with applicable Data Protection Laws. Before engaging any Subprocessor, the Processor ensures that appropriate contractual safeguards are in place. The Processor remains fully responsible for the performance of its Subprocessors to the extent required under Article 28 GDPR and the DPA.

2. Approved Subprocessors

Subprocessor	Service	Processing Activities	Categories of Personal Data	Processing Location	Transfer Mechanism
Amazon Web Services	Cloud infrastructure and hosting	Hosting, compute, storage, networking, backup, disaster recovery, monitoring and supporting infrastructure.	Potentially all categories of Controller Personal Data depending on the AWS service.	European Union (Frankfurt Region) Singapore Region	Standard Contractual Clauses (where required).
Mailgun Technologies	Transactional email delivery (Mailgun Send API)	Delivery of account activation emails, password resets, contact form verification and user notifications.	Recipient name, email address, email content, activation links, password reset tokens and other data contained in transactional emails.	European Union (EU region only) Configured by the Processor to process data exclusively within the European Union.	All email processing configured exclusively within the EU region.

3. Additional Information

Internal business systems including the Processor's CRM platform, version control system, support system and monitoring platform are operated directly by the Processor within its own AWS infrastructure and are therefore not separate Subprocessors.

The Services may use third-party APIs, such as Google Places API, solely to validate address information entered by users. Such API providers do not Process Controller Personal Data on behalf of the Controller within the meaning of Article 28 GDPR and are therefore not listed as Subprocessors.

4. Changes to Approved Subprocessors

The Processor may update this Annex from time to time in accordance with Section 7 of the DPA. Where required by applicable Data Protection Laws, the Processor shall provide reasonable prior notice before adding or replacing a Subprocessor. The current version of this Annex shall be made available to the Controller upon request or through the communication channels provided by the Processor, including the Services where applicable.

APPENDIX A

EU STANDARD CONTRACTUAL CLAUSES
(Commission Implementing Decision (EU) 2021/914)

The following Standard Contractual Clauses form an integral part of this Data Processing Agreement.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c)The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

Transfer controller to processor

(a)GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in

writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

Transfer controller to processor

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

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

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

Clause 11

Redress

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

Transfer controller to processor

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

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

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

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

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

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

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

Clause 12

Liability

Transfer controller to processor

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

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

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

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

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

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

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

Clause 13

Supervision

Transfer controller to processor

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

Transfer controller to processor

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

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

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

(ii)the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

Transfer controller to processor

15.1 Notification

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

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall

include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

Transfer controller to processor

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

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

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

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

ANNEX I

A. LIST OF PARTIES

Data Exporter:

The Controller identified in the Principal Agreement, applicable Order,

subscription confirmation or account registration through which this

DPA was accepted.

Data Importer:

Greenhouse IT Pte. Ltd.

Singapore

These SCC are incorporated by reference into this DPA and become effective upon execution or acceptance of the DPA.

B. DESCRIPTION OF TRANSFER

The information required by this Annex is set out in Annex I (Details of Processing) of the Data Processing Agreement and is incorporated herein by reference.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be the supervisory authority determined in accordance with Clause 13 of these Clauses and Article 55 GDPR.

ANNEX II

The Technical and Organisational Measures described in Annex II (Technical and Organisational Measures) of the Data Processing Agreement shall constitute Annex II to these Standard Contractual Clauses.

ANNEX III

The list of approved Subprocessors contained in Annex III (Approved Subprocessors) of the Data Processing Agreement shall constitute Annex III to these Standard Contractual Clauses.

APPENDIX B

Transfer Impact Assessment

(Informational document supporting Clause 14 of the SCCs)

1. Purpose

This Transfer Impact Assessment documents the assessment performed by Greenhouse IT Pte. Ltd. regarding transfers of personal data from EEA controllers to Singapore in support of the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, Module Two).

2. Transfer Scenario

Data Exporter: Customer acting as Controller. Data Importer: Greenhouse IT Pte. Ltd., Singapore, acting as Processor. Service: aniSYS SaaS platform.

3. Categories of Data

The transferred data corresponds to Annex I of the DPA and includes identity and contact data, account data, operational records, uploaded documents and photographs. The service is not intended for Article 9 GDPR special categories.

4. Purpose

Transfers are necessary to provide hosting, maintenance, support, monitoring, backups and operation of aniSYS.

5. Transfer Mechanism

Transfers rely on the EU Standard Contractual Clauses (Module Two) together with the DPA and its Annexes.

6. Assessment of Singapore

Singapore has an established legal framework including the Personal Data Protection Act (PDPA), an independent judiciary and a stable rule of law. Greenhouse IT is not aware of laws preventing compliance with the SCCs.

7. Technical Safeguards

Dedicated customer environments, AWS EKS infrastructure, TLS encryption, encrypted EFS/S3/AWS Backup, least-privilege IAM, MFA, VPN administration, RBAC, logging, monitoring, vulnerability scanning and backups.

8. Organisational Safeguards

Confidentiality obligations, least-privilege access, ticket-based support, documented operational procedures and continuous security improvements.

9. Government Access

If Greenhouse IT receives a legally binding disclosure request, it will assess legality, challenge unlawful requests where appropriate and comply with SCC notification obligations unless legally prohibited.

10. Residual Risk

Taking into account the SCCs, TOMs and Singapore's legal framework, the residual transfer risk is assessed as low.

11. Conclusion

Greenhouse IT concludes that transfers to Singapore for operation of aniSYS provide a level of protection that is not undermined by the applicable legal framework when combined with the SCCs and the implemented safeguards.

12. Review

This assessment should be reviewed following material legal, technical or organisational changes.

Electronic Acceptance

This DPA, including Annexes I to III and Appendices A and B, forms part of the Principal Agreement and becomes binding upon execution or electronic acceptance of the Principal Agreement, an applicable Order, or this DPA.

No separate signature is required.