probax

GDPR DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA" supplements the existing agreement between the Customer and Probax governing the Customer's use of the Services provided by Probax. This DPA is an agreement is a legally binding agreement between Probax Pty Ltd ABN 82 114 360 388 / Probax USA, INC (hereinafter referred to as "Probax", "us", "our" and/or "we") and the Customer (being an entity subscribing to Probax for the provision of cloud data protection Services). You agree that by accessing Probax Services, you (hereinafter referred to as "the Customer", "the Controller", "you" and/or "your") accept, without limitation or qualification, the terms and conditions contained within this Agreement.

Data Processing

1.1 **Scope and Roles**. This DPA applies when the Customer's Data or its End User's Data is processed by Probax. In this context, the parties acknowledge and agree that the Customer is the Controller of Customer Data and Probax is the Processor of that data.

1.2 **Security and Controls.** The Services provide the Customer with a number of controls, including security features and functionalities, that the Customer may use to retrieve, correct, delete or restrict Customer or End User Data. Without prejudice to Section 5.1, the Customer may use these controls as technical and organisational measures to assist in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects.

1.3 **Details of Data Processing.**

(a) **Subject Matter.** The subject matter of the data processing under this DPA is Customer or End User Data.

(b) **Type of Data.** Customer or End User Data uploaded to Probax for the supply and delivery of Services to the Customer or their End User.

(c) **Categories of Data Subjects.** The data subjects may include the Customer's employees and End Users.

(d) **Durations.** Data will be processed for the duration of the Agreement.

(e) **Purpose and Nature of Processing.** The data processing under this DPA is for the provision of data protection Services initiated by the Customer from time to time.

1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

1.5 **Own Costs.** The parties agree to bear their own costs in relation to this DPA.

Responsibilities

2.1 **Controller Responsibility**

(a) **Compliance with Statutory Requirements.** Within the scope of the Agreement and in its use of the Services, the Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Customer Data to the Processor and the Processing of Customer Data. For the avoidance of doubt, the Controller's instructions for the Processing of Customer Data shall comply with the Data Protection Law. This DPA is the Customer's complete and final instruction to Probax in relation to Customer Data and that additional instructions outside the scope of this DPA would require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time, thereafter, be amended, amplified or replaced by the Controller in separate written instructions (as individual instructions).

(b) **Notification of Errors.** The Controller shall inform the Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Customer Data.

(c) **Security**. The Customer may elect to implement technical and organisational measure in relation to Customer Data. Such technical and organisational measures include the following:

(i) pseudonymisation and encryption to ensure an appropriate level of security;

(ii) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and Services that are being operated by the Customer;

(iii) measures to allow the Customer to backup archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical and technical incident; and

(iv) processes for regular testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by the Customer.

2.2 **Processor Responsibility**

(a) **Compliance with Instructions.** The Processor shall collect, process and use Customer Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If the Processor cannot process Customer Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Processor will:

(i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and

(ii) cease all Processing (other than merely storing and maintaining the security of the

affected Customer Data) until such time as the Controller issues new instructions with which the Processor is able to comply. If this provision is invoked, the Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable Services until such time as the Controller issues new instructions in regard to the Processing.

(b) **Security of Data Processing.** The Processor shall take the appropriate technical and organisational measures to adequately protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data, described under Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not limited to:
   (i) the prevention of unauthorised persons from gaining access to Customer Data Processing systems;
   (ii) the prevention of Customer Data Processing systems from being used without Authorisation;
   (iii) ensuring that persons entitled to use a Customer Data Processing system gain access only to such Customer Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Customer Data cannot be read, copied, modified or deleted without authorisation;
   (iv) ensuring the establishment of an audit trail to document whether and by whom Customer Data have been entered into, modified in, or removed from Customer Data Processing systems; and
   (v) ensuring that Customer Data is processed solely in accordance with the Customer's instructions.

(c) **Confidentiality.** The Processor will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law. The Processor will restrict its personnel from processing Customer Data without authorisation and will ensure that the appropriate contractual obligations are in place with its personal, with regards to confidentiality and security.

(d) **Customer Data Breach**
   (i) The Processor shall notify the Controller without undue delay upon Processor becoming aware of a Customer Data Breach affecting Company Customer Data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Customer Data Breach under the Data Protection Laws.
   (ii) The Processor shall co-operate with the Controller and take reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Customer Data Breach.

(e) **Deletion or Return of Customer Data**
Subject to this section 2.2(e), the Processor shall promptly and in any event within 10 business days of the date of termination of the Agreement, delete or return all Customer Data (including copies therefore) processed pursuant to this DPA. Any additional cost arising in connection with the return or deletion of Customer Data after the termination or expiration of the Agreements shall be borne by the Controller.

(f) **Data Protection Impact Assessment and Consultation with Supervisory Authorities**
The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

Data Subject Rights

3.1 Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

3.2 If the Controller does not have the ability to address a Data Subject request, then upon Controller's request Processor shall provide reasonable assistance to the Controller to facilitate such Data Subject request to the extent able and only as required by applicable Data Protection Law. Controller shall reimburse Processor for the commercially reasonable costs arising from this assistance.

Audit Rights

4.1 Subject to this section 4, the Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Company Customer Data by the Contracted Processors.

4.2 The Processor shall, upon the Controller's written request and on at least 30 days' notice to the Processor, provide the Controller with all information necessary for such audit, to the extent that such information is within Processor's control and the Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

4.3 Information and audit rights of the Controller only arise under section 4.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

Subprocessing

5.1 The Controller agrees that Probax may use subprocessors to fulfil its contractual obligations under this DPA or to provide certain services on its behalf. The Probax Subprocessors Page lists subprocessors that are currently engaged by Probax to carry out processing activities Customer Data.

5.2 At least 30 days before Probax engages any new subprocessor to carry out processing activities on Customer Data on behalf of the Controller, Probax will update the applicable website and provide the Controller with a mechanism to obtain notice of that update.

5.3 The Processor will give the Controller the opportunity to object to the engagement of the new subprocessors within 30 days after being notified. The objection must be based on reasonable grounds. If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.

5.4 Where Probax authorises any subprocessors, Probax will restrict the subprocessor's access to Customer Data only to what is necessary to maintain and deliver the Services to the Customer and any End Users.

Data Transfer

6.1 The Controller acknowledges and agrees that, in connection with the performance and delivery of the Services under the Agreement, Customer Data will be transferred to Probax in Australia and the United States. The Processor may access and perform Processing of Customer Data on a global basis as necessary to provide the Services to the Customer.

6.2 The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

6.3 The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if AWS has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

Confidentiality

7.1 Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

Termination

8.1 This DPA shall continue in force until the termination of the Agreement.

Entire Agreement

9.1 Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control.

Definitions

10.1 Unless otherwise defined, capitalised terms and expressions used in this DPA shall have the following meaning:

Company Data means the "personal data" (as defined in the GDPR).

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Customer Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data transmitted, stored or otherwise processed.

Data Protection Law means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms "process", "processes" and "processed" will be construed accordingly.

Data Subject means the individual to whom Personal Data relates.

GDPR means the General Data Protection 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.

Processing has the meaning give to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Standard Contractual Clauses means the clauses attached hereto as Annex 1 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Subprocessors Page means Probax' Subprocessors Page available at https://www.probax.io/subprocessors

ANNEX 1 – STANDARD CONTRACT CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer, as defined in the DPA of Service (the "data exporter"); and

Probax Pty Ltd, L33/250 St Georges Terrace, Perth WA 6000, Australia (the "data importer"),

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 - Definitions

'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 – Details of the Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 – Third-party Beneficiary Clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 – Obligations of the Data Exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration,

unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 – Obligations of the Data Importer

The data exporter agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(ii) any accidental or unauthorised access, and
(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 – Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach

by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 – Mediation and Jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 – Cooperation with Supervisory Authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 – Cooperation with Supervisory Authorities

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 – Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 – Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 – Obligation after the Termination of Personal Data Processing Services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

APPENDIX 1 – DETAILS OF PROCESSING

Data exporter
The data exporter is the entity identified as "Customer" in the DPA

Data importer
The data importer is Probax Pty Ltd, a provider of cloud data protection services.

Data subjects
Data subjects are defined in Section 1.3 of the DPA.

Categories of data
The personal data is defined in Section 1.3 of the DPA.

Processing operations
The processing operations are defined in Section 1.3 of the DPA

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Probax currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Probax may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

1. **Network Security.** The Probax Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Probax will maintain access controls and policies to manage what access is allowed to the Probax Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Probax will maintain corrective action and incident response plans to respond to potential security threats.

2. **Access Control**

    (a) **Physical and Environmental Security**: Probax hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications

    (b) **Authentication:** Probax has implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

    (c) **Authorisation:** Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of Probax's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set

    Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorisation.

3. **Transmission Control.** Where technically possible, Probax will encrypt customer data during transit and at rest. Some Services that use 3rd party software will require the Customer to enable encryption when configuring the 3rd party software. Probax cloud-to-cloud Services including Office 365 Backup and Dropbox Backup & Archive uses SSL/TLS during data transfer and AES 256-bit encryption at rest.

4. **Continued Evaluation.** Probax will conduct periodic reviews of the security of its Probax Network as measured against industry security standards and its policies and procedures. Probax will continually evaluate the security of its network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.