DRAGOS PARTNER DATA PROCESSING AGREEMENT ("DPA")
Last Updated May 14, 2024

This Partner Data Processing Agreement (the "**DPA**") is incorporated into the agreement(s) entered into by you ("**Partner**") and Dragos, Inc. ("**Dragos**"), and governs the data sharing between you and Dragos (but excluding customer agreements between Partner and Dragos that govern Partner's purchase and use of Dragos products and services) ("**Partner Agreement**").

This DPA covers the processing of: (1) Personal Data that the Partner transfers or otherwise provides to Dragos in connection with a Partner Agreement; and (2) Personal Data that Dragos transfers or otherwise provides to Partner in connection with the Partner Agreement.

Collectively, this DPA (including the SCCs, as defined below) and the Partner Agreement are referred to in this DPA as the "Agreement." In the event of any conflict or inconsistency between any of the terms of the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the SCCs (b) this DPA; and (c) the Partner Agreement.

The Purpose of this DPA is to establish a framework to address scenarios where:

A. Dragos and Partner may each be Controllers of Personal Data, and transfer that Personal Data to the other party for that other party to act as a Controller of that Personal Data;

B. Dragos and Partner may each be Controllers of Personal Data, and transfer that Personal Data to the other party for that other party to provide certain services to the Controller as a Processor of that Personal Data;

C. Dragos and Parter may each be Processors of a Joint Customer's Personal Data, and transfer that Personal Data to the other party for the party to provide certain services to the Processor as a Subprocessor of that Personal Data; or

D. Dragos and Partner may each be Processors of Personal Data, and transfer that Personal Data to the other party for that party to act as a Controller of that Personal Data.

1. DEFINITIONS

"**Business**" and "**Service Provider**" will have the meanings given to them in the CCPA.

"**California Personal Information**" means Personal Data that is subject to the protection of the CCPA.

"**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018), as amended by the California Privacy rights Act of 2020 or "CPRA".

"**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.

"**Data Protection Laws**" means all applicable worldwide legislation or regulations relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws and the CCPA; in each case as amended, repealed, consolidated or replaced from time to time. "Europe" means the

European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"**European Data Protection Laws**" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act of 2020 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

"**European Personal Data**" means Personal Data that is subject to the protection of European Data Protection Laws.

"**Joint Customer**" means a customer of either Partner or Dragos or both in connection with the Partner Agreement.

"**Joint Customer Personal Data**" means any Personal Data for which a Joint Customer acts as a Controller.

"**Dragos Personal Data**" means any Personal Data for which Dragos acts as a Controller.

"**Partner Personal Data**" means any Personal Data for which Partner acts as a Controller.

"**Personal Data**" means any information relating to an identified or identifiable individual where such information is contained within Dragos Personal Data, Partner Personal Data or Joint Customer Personal Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

"**Personal Data Breach**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"**Processing**" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed 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**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced.

"**Subprocessor**" means any entity which provides Processing services to a Processor.

"**Supervisory Authority**" means an independent public authority which is established by a member state of the European Economic Area, Switzerland or the United Kingdom.

"**UK Addendum**" means the International Data Transfer Addendum (Version B.1.0) issued by the UK ICO under s119A of the Data Protection Act 2018, as it may be amended, superseded or replaced.

2. COMPLIANCE WITH LAWS

The parties shall each represent and warrant that they will comply with their respective obligations and duties under applicable Data Protection Laws.

3. CONTROLLER-TO-CONTROLLER SCENARIOS

Each party, to the extent that it, along with the other party, acts as a Controller with respect to Personal Data, will reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in applicable Data Protection Laws. The parties acknowledge and agree that each is acting independently as a Controller with respect of Personal Data and the parties are not joint controllers as defined under European Data Protection Laws.

4. CONTROLLER-TO-PROCESSOR SCENARIOS

A. Relationship of the parties. The rights, responsibilities, and obligations of the parties with regard to Sections 7 – 10 of this DPA shall be as follows:

For Processing operations where Partner processes Personal Data on Dragos's behalf and at Dragos's direction, the term "Processor" refers to Partner, the term "Controller" refers to Dragos, and the term "Personal Data" refers to Dragos Personal Data. For Processing operations where Dragos processes Personal Data on Partner's behalf and at Partner's direction, the term "Processor" refers to Dragos, the term "Controller" refers to Partner, and the term "Personal Data" refers to Partner Personal Data.

B. Scope of Processing.

In the context of the scenarios described in Section 4.A above, each party agrees to process Personal Data only for the purposes set forth in the applicable Partner Agreement and/or the agreement(s) with the Joint Customer. For the avoidance of doubt, the categories of Personal Data processed and the categories of data subjects subject to this DPA are described in Schedule 1 to this DPA.

5. PROCESSOR-TO-PROCESSOR SCENARIOS

A. Relationship of the parties. The rights, responsibilities, and obligations of the parties with regard to Sections 7 – 10 of this DPA shall be as follows:

For Processing operations where Partner processes Personal Data as a Subprocessor on Dragos's behalf and Dragos is a Processor of the Joint Customer, the term "Processor" refers to Partner, the term "Controller" refers to Dragos, and the term "Personal Data" refers to Joint Customer Personal Data. For Processing operations where Dragos processes Personal Data as a Subprocessor on Partner's behalf and Partner is a Processor of the Joint Customer, the term "Processor" refers to Dragos, the term "Controller" refers to Partner, and the term "Personal Data" refers to Joint Customer Personal Data.

B. Scope of Processing.

In the context of the scenarios described in Section 5.A above, each party agrees to process Personal Data only for the purposes set forth in the applicable Partner Agreement and/or the agreement(s) with the Joint Customer. For the avoidance of doubt, the categories of Personal Data processed and the categories of data subjects subject to this DPA are described in Schedule 1 to this DPA.

6. PROCESSOR-TO-CONTROLLER SCENARIOS

A. Relationship of the parties. The rights, responsibilities, and obligations of the parties with regard to Sections 7 – 10 of this DPA shall be as follows:

For Processing operations where Partner processes Personal Data on Dragos's behalf and at Dragos's direction, the term "Processor" refers to Partner, the term "Controller" refers to Dragos, and the term "Personal Data" refers to Dragos Personal Data. For Processing operations where Dragos processes Personal Data on Partner's behalf and at Partner's direction, the term "Processor" refers to Dragos, the term "Controller" refers to Partner, and the term "Personal Data" refers to Partner Personal Data.

B. Scope of Processing.

In the context of the scenarios described in Section 6.A above, each party agrees to process Personal Data only for the purposes set forth in the applicable Partner Agreement and/or the agreement(s) with the Joint Customer. For the avoidance of doubt, the categories of Personal Data processed and the categories of data subjects subject to this DPA are described in Schedule 1 to this DPA.

7. CONTROLLER OBLIGATIONS

The parties in their capacity as a Controller agree to:

A. Provide instructions to the Processor and determine the purposes and means of the Processor's processing of Personal Data in accordance with the Agreement; and

B. Comply with its protection, security and other obligations with respect to Personal Data prescribed by applicable Data Protection Laws for a Controller by: (i) establishing and maintaining a procedure for the exercise of the rights of the individuals whose Personal Data are processed on behalf of the Controller; (ii) processing only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses; and (iii) ensuring compliance with the provisions of this DPA by its personnel or by any third party accessing or using Personal Data on its behalf.

8. PROCESSOR OBLIGATIONS

A. Processing Requirements. The parties in their capacity as a Processor agree to:

a. Process Personal Data (i) only for the purpose of providing, supporting and improving the Processor's product and services (including to provide insights and other reporting), using appropriate technical and organizational security measures; and (ii) in compliance with the instructions received from the Controller. The Processor will not use or process Personal Data for any other purpose. The Processor will promptly inform the Controller in writing if it cannot comply

with the requirements under Sections 7 – 10 of this DPA, in which case the Controller may terminate the Agreement, and any applicable Partner Agreement, or take any other reasonable action, including suspending data processing operations;

b. Inform the Controller promptly and without undue delay if, in the Processor's opinion, an instruction from the Controller violates applicable Data Protection Laws;

c. If the Processor is collecting Personal Data from individuals on behalf of the Controller, follow the Controller's instructions regarding such Personal Data collection;

d. Take commercially reasonable steps to ensure that (i) persons employed by it and (ii) other persons engaged to perform on the Processor's behalf comply with the terms of the Agreement, and applicable Partner Agreements;

e. Represent and warrant that its employees, authorized agents and any Subprocessors are subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the personal data who is not under such a duty of confidentiality;

f. If it intends to engage Subprocessors to help it satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors, (i) provide a list of Subprocessors currently engaged by the Processor to the Controller (such list for Dragos is available online at https://www.dragos.com/subprocessors/), and notify the Controller of the engagement of any new Subprocessors at least 30 days in advance, giving the Controller the opportunity to object; (ii) remain liable to the Controller for the Subprocessors' acts and omissions with regard to data protection where such Subprocessors act on the Processor's instructions; and (iii) enter into contractual arrangements with such Subprocessors binding them to provide the same level of data protection and information security to that provided for herein;

B. Notice to the Controller. The Processor will immediately and without undue delay inform the Controller if the Processor becomes aware of:

a. Any non-compliance by Processor or its employees with Sections 7 – 10 of this DPA or applicable Data Protection Laws relating to the protection of Personal Data processed under this DPA;

b. Any legally binding request for disclosure of Personal Data by a law enforcement or government authority, unless the Processor is otherwise forbidden by law to inform the Controller, for example to preserve the confidentiality of an investigation by law enforcement authorities;

c. Any notice, inquiry or investigation by a Supervisory Authority with respect to Personal Data, unless prohibited by applicable law; or

d. Any complaint or request (in particular, requests for access to, rectification or blocking of Personal Data) received directly from data subjects of the Controller. The Processor will not respond to any such request without the Controller's prior written authorization unless otherwise required by applicable law.

C. Assistance to the Controller. The Processor will provide timely and reasonable assistance to the Controller regarding:

a. Responding to any request from an individual to exercise rights under applicable Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable) and the Processor agrees to promptly inform the Controller if such a request is received directly;

b. The investigation of Personal Data Breaches and the notification to the Supervisory Authority and the Controller data subjects regarding such Personal Data Breaches; and

c. Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

D. Required Processing.

If the Processor is required by Data Protection Laws to process any Personal Data for a reason other than in connection with the Agreement, the Processor will inform the Controller of this requirement in advance of any processing, unless the Processor is legally prohibited from informing the Controller of such processing (e.g., as a result of secrecy requirements that may exist under applicable EU member state laws).

E. Security. The Processor will:

a. Maintain appropriate organizational and technical security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Personal Data while in transit and at rest) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Personal Data;

b. Be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all of the Processor's personnel with respect to Personal Data and liable for any failure by such Processor personnel to meet the terms of this DPA;

c. Take appropriate steps to confirm that all of the Processor's personnel are protecting the security, privacy and confidentiality of Personal Data consistent with the requirements of this DPA; and

d. Notify the Controller of any Personal Data Breach by the Processor, its Subprocessors, or any other third parties acting on the Processor's behalf without undue delay upon becoming aware of a Personal Data Breach.

F. Additional Provisions for California Personal Information.

When the Processor Processes California Personal Information in accordance with the instructions received from the Controller, the parties acknowledge and agree that the Controller is a Business and the Processor is a Service Provider for the purposes of the CCPA. The parties agree that the Processor will Process California Personal Information as a Service Provider strictly for the purpose of providing, supporting and improving the Processor's services (including to provide insights and other reporting) (the "Business Purpose") or as otherwise permitted by the CCPA. Further, the Processor (i) will not Sell or Share California Personal Information; (ii) will not retain, use, disclose, or Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; and (iii) will not combine the California Personal Information with personal information

collected or received from another source (other than information received from another source in connection with Processor's obligations under the applicable Partner Agreement and/or the agreement(s) with the Joint Customer).

9. AUDIT, CERTIFICATION

A. Supervisory Authority Audit.

If a Supervisory Authority requires an audit of the data processing facilities from which the Processor processes Personal Data in order to ascertain or monitor compliance with Data Protection Laws, the Processor will cooperate with such audit. The Controller will reimburse the Processor for its reasonable expenses incurred to cooperate with the audit, unless such audit reveals the Processor's noncompliance with this DPA.

B. Processor Certification.

The Processor must, upon the Controller's request provide a certification of compliance to the Controller (not to exceed one request per calendar year) by email (where Dragos is the Processor, such emails shall be sent to privacy@dragos.com; where Partner is the Processor, Partner shall establish and provide to Dragos upon request a single point of contact for email correspondence regarding data protection), certify compliance with this DPA in writing. Such certification may be in the form of (i) the results of a self-audit, (ii) internal company rules of conduct including external evidence of compliance, (iii) certificates on data protection and/or information security (e. g. ISO 27001), (iv) approved codes of conduct, or (v) other appropriate certificates.

10. DATA RETURN AND DELETION

The parties agree that on the termination of the data processing services and upon the Controller's reasonable request, the Processor shall and shall take reasonable measures to cause any Subprocessors to, at the choice of the Controller, return all the Personal Data and copies of such data to the Controller or securely destroy them and demonstrate to the satisfaction of the Controller that it has taken such measures, unless applicable Data Protection Laws prevent the Processor from returning or destroying all or part of the Personal Data disclosed. In such case, the Processor agrees to preserve the confidentiality of the Personal Data retained by it and that it will only actively process such Personal Data after such date in order to comply with applicable laws.

11. DATA TRANSFERS

Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

A. European Partner Data. For transfers of Partner Personal Data that is subject to European Data Protection Laws ("European Partner Data") from Partner to Dragos for processing by Dragos in a jurisdiction outside Europe that does not provide an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), the parties agree that if European Data Protection Laws require that appropriate safeguards are put in place, the parties agree to abide by and Process European Partner Data in compliance with the SCCs as incorporated below.

B. European Dragos Data. For transfers of Dragos Personal Data that is subject to European Data Protection Laws ("European Dragos Data") from Dragos to Partner for processing by Partner in a jurisdiction outside Europe that does not provide an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), the parties agree if European Data Protection Laws require that appropriate safeguards are put in place, the parties agree to abide by and process European Dragos Data in compliance with the SCCs as incorporated below.

C. Standard Contractual Clauses. The Parties acknowledge and agree that for the purposes of the SCCs: (i) with respect to European Personal Data exported by Partner, the "data exporter" shall be Partner and the "data importer" shall be Dragos (acting on behalf of itself and its Affiliates); (ii) with respect to European Personal Data exported by Dragos, the "data exporter" shall be Dragos (acting on behalf of itself and its Affiliates) and the "data importer" shall be Partner; (iii) the Module One terms shall apply where both parties are Controllers, the Module Two terms shall apply where the party receiving Personal Data under the SCCs is acting as a Processor on behalf of the other party as a Controller, the Module Three terms shall apply where the party receiving the Personal Data under the SCCs is acting as a Subprocessor on behalf of the other party as a Processor, and the Module Four terms shall apply where the party transferring Personal Data under the SCCs is acting as a Processor on behalf of the other party as a Controller; (iv) in Clause 7, the optional docking clause shall apply; (v) in Clause 9, Option 2 of Module Two and Module Three shall apply and the data importer shall obtain authorization for Subprocessors in accordance with Section 8.A.f of this DPA; (vi) in Clause 11, the optional language shall be deleted; (vii) in Clause 17 and Clause 18(b), the SCCs shall be governed by the laws of and disputes shall be resolved before the courts of the Republic of Ireland or the EEA member state in which the Dragos legal entity that has entered into the Agreement is established or, if such Dragos is not established in the EEA, the Republic of Ireland; (viii) in Annex I of the SCCs, the details of the parties is set out in the Agreement; and (ix) the remaining information in Annex I and Annex II of the SCCs shall be deemed completed with the information set out in Schedule 1 of this DPA.

D. UK Transfers. In relation to Personal Data that is subject to the UK GDPR, the SCCs shall apply in accordance with Section 11.C above and the following additional modifications: (i) the SCCs shall be amended as specified by the UK Addendum, which shall be incorporated by reference; (ii) Tables 1 to 3 in Part 1 of the UK Addendum shall be populated with relevant information set out in Schedule 1 of this DPA; (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither"; and (iv) any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

E. Swiss Transfers. In relation to Personal Data that is subject to the Swiss DPA, the SCCs shall apply in accordance with Section 11.C above and the following additional modifications: (i) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein; (ii) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland"; (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland"; and (iv) in Clause 17 and Clause 18(b), the SCCs shall be governed by the laws of and disputes shall be resolved before the courts of Switzerland.

F. The parties shall promptly notify each other of any inability to comply with the provisions of this Section 11.

12. TERM

This DPA shall remain in effect as long as either party carries out Personal Data processing operations on the Personal Data uploaded or otherwise provided by the other party pursuant to and in accordance with the Partner Agreement.

SCHEDULE 1

A. LIST OF PARTIES

As specified in the Partner Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects:
The Personal Data may concern the following categories of data subjects, depending on the agreement between the data importer and data exporter:

- Employees and other personnel of Partner or Dragos
- Contacts of potential and actual customers of Partner or Dragos
- Contacts of sales and marketing leads of Partner or Dragos
- Any other persons whose Personal Data are processed by a party in accordance with the Partner Agreement

Categories of Personal Data:
The Personal Data may concern the following categories of data, where applicable:

- Contact details
- Login credentials
- End customer machine and user logs (solely to the extent Partner is a delivery/support partner)
- Any other Personal Data which are processed by a party in accordance with the Partner Agreement

Sensitive data (if applicable):
The Personal Data transferred concern the following sensitive data:

- None

Frequency of transfer:
The Personal Data is transferred continuously.

Nature of the processing:
The transfer is made for the following purposes:
The transfer is intended to enable the relationship of the parties contemplated by the Partner Agreement. The "Partner Agreement" is the agreement(s) entered into by the data importer and the data exporter that govern data sharing between those parties (but excluding customer agreements between Partner and Dragos that govern Partner's purchase of Dragos products and services).

Period for which Personal Data will be retained:
The personal data transferred between the parties may only be retained for the period of time permitted under the Partner Agreement. The parties agree that each party will, to the extent that it, along with the other party, acts as a Controller with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in Data Protection Laws.

Subject matter, nature, and duration of the processing:
The subject matter, nature and duration of the processing is as described in the Agreement, including this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

For the purposes of the SCCs, the competent supervisory authority is the authority of the EEA member state in which Partner or Partner's EEA representative is established (with respect to Partner Personal Data) or the Irish Data Protection Commissioner (with respect to Dragos Personal Data). For the purposes of UK and Swiss transfers, the competent supervisory authority is the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable).

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Dragos's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

Documentation and accountability

Implementation of accountability principles and documentation of operations related to data processing and data security, This is accomplished through:

- Drafting, implementing and monitoring an extensive company-wide IT Security Policy and Standards for IT Assets; and
- Applying Confidentiality and Non-Disclosure Agreements where appropriate and as described in Dragos Policies.

Access control of processing areas

Implementation of suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment used to process the Personal Data. This is accomplished through:

- Keys and card key systems;
- building security; and
- CCTV.

Access control to data processing systems

Implementation of suitable measures to prevent data processing systems from being used by unauthorised persons. This is accomplished through:

- Individual user ID's and strong passwords subject to minimum security requirements for staff members;
- Mandatory password changes on regular intervals;
- Acceptable use policies for IT Assets such as PC's and mobile phones and applications;
- Strict on- and off-boarding policies for staff members;
- Lock out of user accounts after a limited number of failed log-in attempts; and
- Advanced firewalls, PEN testing, anti-virus and spam scanning.

Access control to use specific areas of data processing systems

The persons entitled to use its data processing systems are only able to access the data within scope and to the extent covered by their respective access permission (authorisation) and that the Personal Data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by:

- Access management on strict need-to-know principles, job duties, project responsibilities and actual business activities; and
- Strict VPN corporate network requirements.

Transmission control

Implementation of suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged. This shall be accomplished by:

- Firewall and encryption technologies to protect gateways through which the data travels; and
- Monitoring of encryption technologies.

Access and input control

Implementation of suitable measures to ensure that it is possible to check and establish whether, when, by whom and for what reason Personal Data have been input into data processing systems or otherwise processed. This shall be accomplished by:
Authentication of the authorised users via user ID and passwords;

- Restricted physical access to processing areas; and
- System time-out after non-activity for a pre-determined time period.

Instructional control

Personal data may only be processed in accordance with the DPA and Partner's instructions. This shall be accomplished by information & security training and policies & procedures for staff.

Availability control

Implementing suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This shall be accomplished by:

- Backup and disaster recovery management; and
- Offsite backup storage.

Separation of processing for different purposes

Implementing suitable measures to ensure that Personal Data that are intended for different purposes can be processed separately. This shall be accomplished by:

- Access to Personal Data being restricted via user authorization passwords;
- Function separation of Personal Data of different customers; and
- Use of Personal Data being application specific.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

As set forth in Section 8.A.f of the DPA.