DATA PROCESSING TERMS

Updated: July 12, 2022

These Data Processing Terms ("DPA" or "Data Processing Terms"), when incorporated by reference into a commercial agreement ("Agreement") between The Descartes Systems Group Inc. or one of its affiliates (hereafter referred to as "Descartes") and a Customer, as defined in the Agreement, apply to any Processing of Personal Data performed by Descartes on Customer's behalf as part of Descartes provision of GLN Services, Data Services, or other services (collectively "Services"). All capitalized terms used in these Data Processing Terms shall have the meaning set out in the Agreement unless otherwise defined in these Data Processing Terms.

Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement and any other attachments thereto and the Data Processing Terms, the Data Processing Terms shall take precedence but only to the extent of the conflict. For greater certainty, where an obligation is not addressed in these Data Processing Terms which is addressed in the Agreement, a conflict shall not be deemed to have arisen.

Where Descartes is deemed to be a Controller and not a Processor under Data Protection Regulations, Descartes will comply with its own privacy policy (https://www.descartes.com/legal/privacy-center) in the handling of any applicable Personal Data.

These Data Processing Terms do not apply to the Processing of any data that does not qualify as Personal Data under Data Protection Regulations.

1. Relationship Between the Parties

Descartes provides one or more Services to Customer under an existing commercial relationship. Descartes and Customer are separate legal entities with independent obligations under Data Protection Regulations. Customer understands that it may have an obligation under Data Protection Regulations to independently determine whether its use of Services complies with Data Protection Regulation. Customer acknowledges that Descartes has not made, and explicitly disclaims, any representations that the use of Services will cause Customer to become compliant with Data Protection Regulations.

2. Definitions

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; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to Descartes be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

"Data Subject" means an identified or identifiable living natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Data Protection Regulations" means (a) Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) along with any supplementary or replacement bills enacted into law by the Government of Canada (collectively "PIPEDA"); (b) the General Data Protection Regulation (Regulation (EU) 2016/679) and applicable laws by EU member states which either supplement or are necessary to implement the GDPR (collectively "GDPR"); (c) the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.198(a)), along with its various amendments (collectively "CCPA"); (d) the GDPR as applicable under section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended) (collectively "UK GDPR"); (e) the Swiss Federal Act on Data Protection of June 19, 1992 and as it may be revised from time to time (the "FADP"); and (f) any other applicable law related to the protection of Personal Data.

“Model Clauses” means the standard contractual clauses annexed to the EU Commission Decision (EU) 2021/914 of 4 June 2021 for the Transfer of Personal Data to Processors established in Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision.

“Personal Data” means any information that relates to a Data Subject that Customer or its Administrative User or Permitted Users provide to Descartes to Process under the Agreement.

“Process” or **“Processing”** means any operation or set of operations, whether or not by automated means, which is performed upon Personal Data that is stored on computers, servers, or mobile devices owned or maintained by Descartes, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination of otherwise making available, alignment or combination, blocking, erasure or destruction.

“**Processor List**” means the list of Descartes’ Affiliates and/or Third Party Processors who may assist Descartes with some or all of the Processing of Personal Data of the Customer, a copy of the list being accessible at https://www.descartes.com/legal/privacy-center/supplemental-privacy-information.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the FADP applies, a transfer of Personal Data from Switzerland to any other country which has not been determined to have a legislation that guarantees an adequate level of data protection by the Federal Council.

“Third Party Processor” means a third party subcontractor, other than a Descartes’ Affiliate, engaged by Descartes, which, as a part of the subcontractor’s role in providing services under the Agreement, will Process Personal Data of the Customer.

“UK Addendum” means the "International Data Transfer Addendum to the European Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018.

3. Controller and Processor of Personal Data

Customer shall remain the Controller of the Personal Data for the purposes of the Agreement, including under this DPA. Customer is responsible for compliance with its obligations as a Controller under the Data Protection Regulations and, in particular, for ensuring a valid legal basis for any transmission of Personal Data to Descartes (including by obtaining any required consents and authorizations and providing any necessary notices), and for its decisions and actions concerning the Processing and use of Personal Data. Customer will not provide Descartes with access to any special categories of Personal Data, as defined under the Data Protection Regulations, or any health, payment card, or similar information that imposes specific data security obligations for the processing of such Personal Data unless permitted in the Agreement.

Descartes is a Processor of the Personal Data for the purposes of the Agreement. Descartes will Process Personal Data as necessary for the purposes of the Agreement in accordance with this DPA and will not disclose Personal Data to third parties other than to Descartes’ Affiliates or Third Party Processors for the aforementioned purposes or as required by law.

4. Types of Personal Data

Customer authorizes and requests that Descartes Process the necessary types of Personal Data required to fulfill the Agreement, which shall include only:

a) personal contact information of Customer’s employees, trading partners or contractors (such as name, home address, home telephone number, mobile number or email address, etc.);
b) transactional data (such as details of goods and services purchased, value of purchase, VAT registration number, delivery addresses, or names and contact information of shippers, receivers, or other individuals involved in the transportation or movement of the goods); and
c) where required, identification data (such as government ID numbers if required by a government when information is submitted to or received from that government).

5. Processing Instructions.

Customer authorizes Descartes to Process Personal Data for the following purposes only:

a) providing the requested Descartes product or service under the Agreement;
b) communicating about the Descartes product or service including confirming the provision of all or part of the product or service;
c) handling or preparing for disputes or litigation;
d) complying with Customer’s written instructions in accordance with Section 5;
e) to comply with Descartes’ legal or regulatory obligations; and
f) for no other reason unless provided for under the Data Protection Regulations.

To the extent Descartes receives additional instructions for the Processing of Personal Data, Descartes will comply with such instructions to the extent necessary for: (i) Descartes to comply with its Processor obligations under the Data Protection Regulations; and (ii) to assist Customer in complying with its Controller obligations under the Data Protection Regulations in relation to the Agreement, which may include but is not limited to reasonably assisting Controller in the performance of any required data protection impact assessment or prior consultation with regulatory authority specified under Data Protection Regulations as it relates to the Processing or intended Processing by Descartes. Without prejudice to Descartes’ obligations under this Section 5, the parties will negotiate in good faith with respect to any charges or fees that may be incurred by Descartes to comply with Customer’s instructions with regard to the Processing of Personal Data that require the use of resources different from, or in addition to, those normally required for the provision of the product or services under the Agreement.

Customer will ensure that its instructions to Descartes for the Processing of Personal Data will, at all times, be lawful and in compliance with the Data Protection Regulations. Descartes will notify Customer if it reasonably believes any instruction or request from the Customer will require Descartes to take any action that Descartes reasonably believes will not be in compliance with the Data Protection Regulations. Descartes shall have no other obligation to act beyond sending such notice to the Customer and is not responsible for performing legal research or providing legal advice.

6. Requests from Data Subjects

In the event Descartes receives any requests from Data Subjects to access, remove, release, restrict, modify, or otherwise limit the Processing of Personal Data, Descartes will promptly provide to Customer a copy of that request to Customer’s designated contact in the Agreement. Descartes will not be responsible for responding directly to the Data Subject’s request, unless otherwise required by law.

Where the Services already provide Customer with sufficient means to comply with any such requests, Customer agrees that it will utilize those means to respond to any Data Subject requests. Customer is responsible for using those means properly in accordance with any documentation or written guidelines provided by Descartes from time to time, and will not hold Descartes responsible for any improper use.

If in the event the Services do not provide any means for Customer to self-manage a specific Data Subject request, Descartes will use commercially reasonable efforts, on Customer’s written instruction, to effect that specific Data Subject request. Notwithstanding the above, at no time shall Descartes have any obligation to alter any records that are maintained as system of record of past transactions, to make any change to any records that would be inconsistent with the purpose for which the Personal Data was originally provided to Descartes for Processing, or to alter any record that Descartes is required or entitled to keep by any law or for any regulatory purposes. If Customer requires Descartes to develop or implement any additional or specific means or methods related to the access, deletion, release, correction, modification, or blocking of access to Personal Data on behalf of Customer, Customer and Descartes will mutually agree on the scope of the work that Descartes may be willing to undertake and the reasonable fees, if any, for such work.

7. Restricted Transfers

The Parties agree that to the extent any transfer of Personal Data to Descartes from Customer is consider a Restricted Transfer, as set out under this DPA, it will be subject to the appropriate protections set out under this section 7. In the event that any provision of this DPA contradicts, directly or indirectly, the Model Clauses, the Model Clauses shall prevail.

7.1. Personal Data covered under the GDPR

In relation to Personal Data protected by the GDPR, the Model Clauses will apply, completed as follows:

a) Module 2 of the Model Clauses will apply and with the following options selected: clause 7, option 2 for clause 9a, option 2 for clause 17;
b) the time period referenced in clause 9a shall be four weeks;
c) the relevant member state for the purposes of clause 17 and 18 shall be Belgium;
d) Annex 1 to the Model Clauses shall be deemed completed with the information set out in Schedule 1 to this DPA, with appropriate modifications to the party names and contact information as may be required so that the parties to the Model Clauses reflect the parties to the relevant Agreement. For the avoidance of doubt, Descartes shall be listed as the data importer and Customer shall be listed as the data exporter;
e) Annex 2 of the Model Clauses shall be deemed completed with the information set out in Schedule 2 to this DPA.

7.2. Personal Data covered under the UK GDPR

In relation to Personal Data protected by the UK GDPR, the UK Addendum will apply, completed as follows:

a) The Model Clauses, completed as set out above in section 7.1 of this DPA shall also apply to transfers of such Personal Data, subject to sub-clause (b) below;
b) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the Model Clauses, completed as set out above, and the options "importer" and "exporter" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

7.3. Personal Data covered under the FADP

For the purposes of the FADP, Model Clauses, completed as set out above in section 7.1 of this DPA, will apply with the amendments listed in the following sub-clauses (a)-(g). Insofar as the Restricted Transfer is subject to both the FADP and the GDPR or UK GDPR, the amendments in sub-clauses (a)-(g) shall only apply with respect to the FADP and shall not affect the application of the Model Clauses for the purposes of the GDPR or UK GDPR:

a) References to "Regulation (EU) 2016/679" or "that Regulation" are to be interpreted as references to the FADP to the extent applicable;
b) References to "Regulation (EU) 2018/1725" are removed;
c) References to "Union", "EU", and "EU Member State" shall be interpreted to mean Switzerland;
d) Clause 13 (a) and Part C of Annex I are not used; the competent supervisory authority is the FDPIC insofar as the transfers are governed by the FADP;
e) Clause 17 is replaced to state that "These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by the FADP";
f) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to the FADP shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which they have their habitual residence. The parties agree to submit themselves to the jurisdiction of such courts".

g) As long as the FADP of 19 June 1992 is in force, the Model Clauses shall also protect Personal Data of legal entities and legal entities shall receive the same protection under the Model Clauses as natural persons.

8. Additional Processors

Some or all of Descartes obligations under the Agreement may be performed by Descartes' Affiliates and/or Third Party Processors. Descartes maintains a Processor List, which lists all Descartes' Affiliates and Third Party Processors that may Process Personal Data on behalf of Descartes. To the extent required by applicable Data Protection Regulations, Customer consents to the use by Descartes of the Descartes Affiliates and Third Party Processors listed at https://www.descartes.com/legal/privacy-center/supplemental-privacy-information.

The Descartes' Affiliates and Third Party Processors are required to abide by substantially the same obligations as Descartes under this DPA as applicable to the Processing of the Customer's Personal Data and, in any event, in a manner that is compliant with the Data Protection Regulations.

Descartes remains responsible at all times for compliance with the terms of this DPA by Descartes' Affiliates and Third Party Processors. Customer consents to Descartes use of Descartes' Affiliates and Third Party Processors in the performance of the Services in accordance with this DPA.

If additional Descartes' Affiliates or Third Party Processors are required to process Customer's Personal Data in connection with Descartes' performance under an Agreement, Customer will be notified in advance of changes to the Processor List by way of a subprocessor list update, as described above. The Customer may refuse to consent to the involvement of a Descartes' Affiliate or a Third Party Subprocessor under this DPA by sending written notice to Descartes of their refusal within ten (10) business days of receipt of notice and providing reasonable and justified, objective grounds relating to such Descartes' Affiliate or Third Party Processor's ability to adequately protect Personal Data in accordance with this DPA. In the event that the Customer's objection is justified, Descartes and Customer will work together in good faith to find a mutually acceptable resolution to address Customer's objection(s). If Descartes and Customer are unable to reach a mutually acceptable solution within a reasonable timeframe, Customer may immediately terminate the Agreement without obligation, if any is provided under the Agreement, for the payment of any further Fees that otherwise may be due as result of early termination of the Agreement.

9. Security Measures

In addition to those measures as set out in Schedule 2 to this DPA, Descartes shall implement appropriate physical, administrative, organizational, technical, and personal security measures based on the type and nature of the Personal Data being processed and the level of risk associated with it and as required by Data Protection Regulations. Descartes shall retain all Personal Data, including Personal Data that is contained on back-up media, in a logically secure environment that protects it from unauthorized access, modification, theft, misuse and destruction. Descartes shall ensure that platforms hosting the Personal Data are configured to conform to industry standard security requirements and that hardened platforms are monitored for unauthorized change. Descartes' security policy shall not allow electronic files containing Personal Data to be stored on personal desktops, laptops, or removable data storage devices, unless the device is password protected and the Personal Data is encrypted using industry standard encryption technology. Descartes shall ensure that all employees with access to Personal Data are subject to a duty of confidence and/or written confidentiality agreement.

10. Breach Management and Notification

For the purposes of this section, "Security Breach" means the misappropriation or unauthorized Processing of Personal

Data located on Descartes' systems, including by a Descartes employee, that compromises the security, confidentiality or integrity of such Personal Data or otherwise results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Unless prohibited by applicable law, upon becoming aware of the Security Breach, Descartes will: (i) within seventy two (72) hours, or sooner as required by applicable law, provide to Customer a notification of the occurrence of the Security Breach; (ii) within five (5) business days, or sooner as required by applicable law, provide to Customer a summary report of the Security Breach containing details of the Security Breach, its impact on the services under the Agreement and the Personal Data and the initial steps taken by Descartes to address the Security Breach; and (iii) within fifteen (15) business days, or sooner as required by applicable law, provide to Customer a detailed incident report analyzing the Security Breach and a rectification plan which sets out what steps, if any are appropriate, will be taken to stop and further prevent the Security Breach occurring in the future.

In investigating any Security Breach, Descartes will work to provide to Customer a root cause analysis in order to prevent a recurrence. In addition, unless prohibited by applicable law, Descartes will provide Customer with a summary of the Security Breach and share information about the Security Breach as it becomes available.

11. Security Breach Public Statements

In the event of a Security Breach, the parties agree to coordinate in good faith on developing the content of any related public statements or required notices for the affected Data Subjects and/or notices to the relevant data protection authorities. Unless agreed to otherwise, the controller shall at all times be responsible for communicating with the data subject and any relevant data protection authorities and processor shall refrain from doing so, except that neither party may make any statements or issue any notices that purport to be on the behalf of the other party. Notwithstanding the above, nothing in this DPA shall be interpreted as limiting or restricting either party's obligations to report to or otherwise communicate with any relevant data protection authority or data subject as required under any applicable Data Protection Regulations.

12. Audit

During the Term of the Agreement, on an annual basis, Descartes will conduct, at no charge to Customer, an SSAE 18 SOC 2, Type 2 audit of controls relating to the network operations of Descartes through which Personal Data is processed by Descartes under an Agreement. The results of that audit ("Audit Report") is considered the confidential information of Descartes and will be provided by Descartes to Customer on request only. The audit will be performed by an independent qualified third party auditor (or similarly qualified person). If a deficiency is identified as result of such audit, Descartes will remediate, as Descartes deems reasonable given the circumstances, within an agreed to and reasonable timeframe. All costs of remediation will be the responsibility of Descartes.

In the event Customer wishes to audit Descartes' compliance with this DPA, an independent third party auditor mutually agreed to by the parties (the "Auditor") may, on behalf of Customer and at the expense of Customer, audit Descartes' compliance with the terms of this DPA up to once per year. The Auditor may perform more frequent audits of the data center facility that Processes Personal Data to the extent required by laws applicable to Customer. Prior to the commencement of any audit, the Auditor must execute a written confidentiality agreement acceptable to Descartes.

To request an audit, Customer must submit a detailed audit plan to Descartes at least four weeks in advance of the proposed audit date, unless a shorter period is required under Data Protection Regulations. The audit plan must describe the proposed scope, duration, and start date of the audit. Descartes will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Descartes' security, privacy, employment or other relevant policies). Descartes will work cooperatively with Customer to agree on a final audit plan. If the requested audit scope is addressed in an existing Audit Report that was prepared for Descartes within the prior twelve (12) months and Descartes confirms there are no known material changes in the controls audited, Customer agrees, unless restricted by law or other regulatory requirements, to accept those findings in lieu of requesting an audit of the controls already covered by the report, unless prohibited by Data Protection Regulations from doing so.

The audit must be conducted during regular business hours at the applicable facility, subject to Descartes' policies, and may not unreasonably interfere with Descartes' business activities.

Customer will provide Descartes any audit reports generated in connection with any audit under this section, unless prohibited by law. The parties agree that the audit report shall be treated as if it was the confidential information of the other parties and be subject to the same protections and obligations as is set out under the Agreement, except that neither party can compel the other to delete, destroy, or return the report. Descartes may use the audit reports only for the purpose of assessing or analyzing the contents of the reports, verifying the conclusions reached in the report, and making changes, modifications, or adjustments to Descartes overall data protection or data security practices. Customer may use the audit reports only for the purpose of confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits requested by Customer are at the Customer's expense. Any request for Descartes to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from, or in addition to, those required for the provision services under the Agreement. Descartes will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

13. Legally Required Disclosures

Except as otherwise required by law, Descartes will promptly notify Customer of any requirement of a governmental agency or by operation of law (a "Demand") that it receives and which relates to the Processing of Personal Data. At Customer's request, Descartes will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Descartes has no responsibility to interact directly with the entity making the Demand, unless required by Data Protection Regulations or other applicable law to do so.

14. Destruction of Personal Data

In addition to complying with Descartes standard data retention practices which shall reasonably ensure that Personal Information is properly disposed of within a reasonable period of time after termination or expiration of the Agreement, if requested by Customer at any time during the term of the Agreement, Descartes will, within a commercially reasonable period of time, destroy or render unreadable all Personal Data received by Descartes from Customer that is and still under the control of Descartes, using appropriate methods of data destruction based on current industry standards, except where the Data Protection Regulations or local law provide for that Personal Data to be preserved or maintained. Written confirmation that the Personal Data was destroyed or rendered unreadable can be provided upon request.

15. CCPA Specific Provisions

For the purposes of the CCPA, Descartes and Customer agree that:

a) Descartes is service-provider to the Customer;
b) Descartes, as a for-profit entity, processes the Personal Data provided to it by Customer on behalf of Customer, solely for the purposes of fulfilling the Agreement and at Customer's direction, which Customer shall always provide to Descartes in writing; and
c) Descartes will not sell, trade, rent, loan, or otherwise exchange for consideration, whether monetary or otherwise, any Personal Data provided to it by Customer with any other third-party.

16. General

Should any provision of this DPA be determined to be invalid or unenforceable by a court of competent jurisdiction or applicable regulatory authority, the remainder of this DPA shall remain valid and in force unless expressly stated by that same court or regulatory authority, as the case may be. The invalid or unenforceable provision shall either be (a) amended as necessary to ensure its validity and enforceability, while preserving each party's intentions as closely as possible, or if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

[End of Data Processing Terms, Schedules to immediately follow.]

Schedule 1 to Data Processing Terms

ANNEX I

B. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: …

   Address: …

   Contact person’s name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date:

   Role (controller/processor): controller

Data importer(s):

1. Name: Descartes Systems (USA) LLC

   Address: Power Ferry Business Park, 2030 Powers Ferry Road SE,
   Suite 350
   Atlanta, Georgia, U.S.A. 30339-5066

   Contact person’s name, position and contact details: Peter Nguyen, Data Privacy Officer, c/o 120 Randall Drive, Waterloo, ON, N2V 1C6, Canada

   Activities relevant to the data transferred under these Clauses: management of access control where required, provision of support services including troubleshooting and diagnostics on request.

   Signature and date:

   Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Only the following categories of data subjects, which list may be further reduced depending on the applicable product or service being contracted for:

- Employees, contractors, trading partners, and customers of data exporter (who are natural persons).
- Users authorized by data exporter to access the products and services provided by data importer.
- Employees of third parties contracted by data exporter to deliver products.

Categories of personal data transferred

Only the following types of personal information, which list may be further reduced depending on the applicable product or service being contracted for:

- Names (which may include first, last, or full names)
- Contact information (such as telephone numbers and email addresses)
- Delivery addresses
- User order details (such as items to be delivered, delivery date and time)
- Signatures
- Location data of delivery drivers
- Any personal information that can be inferred from or incidental to any photographs taken by the delivery driver in connection with their delivery to a user

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

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous or regular intervals during life of the written agreement, except where only a one-time transfer is required for the duration of the written agreement.

Nature of the processing

- Receipt, storage, display within interface upon request, and provision to other parties at the request of Customer only.

Purpose(s) of the data transfer and further processing

- To provided services as requested by data exporter and set out in a written agreement between data exporter and data importer

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Duration of the written agreement between data exporter and data importer which incorporates these standard contractual clauses.

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

Subprocessor Name	Type of PII	Duration	Purpose
Not applicable, unless specified in the Order Form.			

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Belgian Data Protection Authority (GBA)

Schedule 2 to Data Processing Terms

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational security measures implemented by Descartes

Technical and Organizational Measures

The paragraphs in this section describe the security and computer operations measures implemented by the data importer (“Descartes”) that apply when handling Personal Data in its role as a data importer as set out under the Data Processing Terms.

Descartes may change these measures at any time without notice, provided that these changes ensure a comparable or better level of security.

1.1 Logical Security

Descartes has an Information Security and Document Retention Policy and an End-User Security Policy for staff (together, “Security Policy”) which is enforced within the data processing systems that handle **Personal Data**. The policy documents the key security components of the data processing systems.

A process to review and update the Security Policy as required is in place. Evidence of security policy changes and details of modifications are recorded in the “Revision History” section of the security policy. Policy updates are reviewed and approved by Senior Management and communicated to employees through the corporate intranet.

Relevant Information Security updates (policies, practices and standards) are provided as needed, through regular Descartes corporate communications channels and situation relevant training sessions when needed. Employees confirm Information Security End User policies as part of HR processes at time of hire and when those policies are updated.

1.2 Access and Authorization

Systems’ resource access to the data processing systems that handle **Personal Data** is granted upon a documented and approved request, for example at time of hire, leave or role change. `Systems’ resource access is revoked in a timely manner after termination or role change by IT Operations. HR, Employees and Employee managers can request authorization by Descartes service-request ticket. Approval is granted based on what is allowed for a role or approval from the employee’s manager, and the authorization reviewer or Descartes data-owner.

Password composition and protection processes are in compliance with the defined user ID and password features per the Security Policy. Service and application accounts are exempt from the periodic password change policy.

Firewall technology is in place to protect the internal network. Logs are configured to generate automated alerts. Automated alerts are queued for investigation which is reported in summary form to Descartes Information Security management.

Log records documenting access to operating systems, or selected functions are created and retained for review or use during investigation of unauthorized access per the Security Policy. Additionally, access violations resulting from invalid logon attempts or systematic attacks are logged, monitored, investigated, where necessary, and retained per the Security Policy. Access to these logs is restricted to a limited number of authorized individuals.

Operating system patch notifications are applied according to recommendations from the operating systems vendor and implemented in a timely manner by service delivery staff after being tested in the pre-production environment. The process to deploy patches follows the Descartes change management procedures below.

1.3 Technical Monitoring

Descartes monitors systems and services for operational and security interest events. Designated devices and designated systems have extra technical monitoring configured. Those have logs encrypted, shipped to an offsite location with separate technical administration where the logs are preserved and monitored by automated alerting mechanisms and responded to by dedicated information security team who escalates to Descartes service teams as required. Summary reports are prepared and regular service meetings coordinate activities between the security team and Descartes service teams.

1.4 Security Monitoring

Logical Security monitoring, reporting and course correction follows the same processes as Incident and Problem management described below.

2.1 Change Management

Descartes Change Management is based upon IT Infrastructure Library (ITIL) change management. It is used to ensure standardized methods and procedures are used for efficient and prompt handling of system or software changes in order to minimize the impact of change related incidents upon service quality. Descartes utilizes a formal, documented change management process. The process is designed to manage changes across relevant functions, to deliver and manage the integration of processes, procedures and technologies. It includes procedures for handling standard, normal and emergency changes.

The following controls exist for change management:

- Changes are formally requested and tracked through the change management systems;

- Risk evaluation is performed to determine the change risk;

- A business and technical assessment is performed where applicable;

- All approvals must be obtained prior to implementation or the change will be considered unauthorized. Documented approval from the Emergency Change Board prior to implementation is acceptable for emergency changes; and

- Changes must be closed within the approved change window for implementation (see stability requirements below).

All access to the production environment system resources is logged.

3.1 Incident Management

Descartes Incident Management is based on ITIL. It is used to restore normal service operation and minimize adverse impact on business operations. A formal incident management process has been documented and is used across functional groups. Incidents are tracked through an incident management tool. Incident tickets are created for each reported event. Descartes recognizes two types of incidents: infrastructure and user. Incident escalation contacts and procedures are defined.

Infrastructure incidents: Infrastructure incidents are created to log unexpected changes in the Descartes service. Infrastructure incidents are escalated to technical expertise center for investigation and resolution. Critical Infrastructure incidents are managed and owned by the Descartes Incident Management Center whose role is to monitor infrastructure and related services and to coordinate incident response activities. Other Infrastructure Incidents are managed and owned by technical expertise Center.

Service requests and end user reported incidents: User incidents are managed and owned by the Descartes Service Desk within the Customer Support team. User incidents may be resolved directly by service desk representatives or customer support expertise center. User Incidents may result in an Infrastructure Incident escalation or an issue being registered in the R&D Secure Development Lifecycle (SDL) management tool.

Escalation and resolution of incidents and service requests: Infrastructure Incident escalations follow Incident Management policies and procedures and or Change Management policies and procedures. R&D escalated issues are resolved by SDL policies and procedures which follow Change Management procedures.

3.2 Problem Management

Descartes Problem Management is based on ITIL. It is used to improve service levels pertaining to reoccurrence of incidents. A formal problem management process has been documented and is used across functional groups. Problems are tracked in a problem management tool. Problem tickets are created to investigate incidents that are recurring or subject to recurrence in the future. A request for problem management can be initiated by any technical service team or Descartes management. The problem manager approves and assigns problem tickets to technical service teams. Technical service team managers assign resources to investigate and document a problem.

3.3 Common elements used in Incident and Problem Management

Cause determination: A root cause analysis is performed on significant incidents to identify and remedy, if possible, the source(s) and to minimize chance of recurrence. The review includes analysis of the cause, contributing factors and strategy to address the issue.

The following information is populated in the incident tickets (and/or the related problem ticket) to assist in tracking problems, reducing the number of issues and minimizing problem life cycles:

- Customer information;
- Date and time problem was identified;
- Date and time problem was reported, symptom description and type of problem;

- Classification of the event;
- Failing resource/component;
- Actions taken to resolve the event, including date and time action was taken; and
- Analysis of initial information to determine appropriate problem record assignment.

4.1 Computer Operations Management

Computer operations procedures have been defined and documented. Descartes infrastructure incorporates fault tolerance technologies that facilitate the timely recovery of data in case of storage media and hardware failure.

Failures and irregularities are monitored by a central monitoring tool and converted to incident tickets for action by system administrators who certify that systems services return to normal operation.

A daily health report records system state in comparison with a predetermined secure baseline. Daily health reports are stored on a central system.

4.2 Automated Scheduling

Automated scheduling is used whenever practicable so that the correct processing sequence is taking place. Notification and correction procedures are in place for instances where the job scheduler is unable to execute jobs in sequence. Only approved computer operations personnel can create and modify distributed systems job schedules. Procedures are in place so that job schedules as well as changes to these schedules are appropriately authorized and procedures are in place to identify, investigate and approve departures from standard job schedules.

4.3 Backup and Restoration

Backup and restoration processes have been implemented such that critical system information can be recovered. Backup procedures are formally documented.

A multi-tiered data backup solution is used. Data backups are generated first to a local file system then transferred to central backup staging servers, then to media for transportation to an off-site storage location.

Backups are stored in an encrypted form.

Backups are performed using a pre-defined schedule. Systems administrators are notified of irregularities in completion or termination of a backup job. In case of failures, systems administrators review failures and re-run backup jobs after addressing the cause of the failure. Automated monitoring is used. An incident management system and daily sign-off document is used to track issues and ensure successful backup completion.

Descartes has contracted a reputable third party to provide media transportation and secured media storage.

5.1 Physical and Environmental Controls

Descartes has contracted with a reputable third party service providers to provide data center 'co-location' facilities. The service providers control access to the facilities and Descartes controls access to the segregated areas housing Descartes' infrastructure. The service providers provides Descartes with a Service Organization Controls Report, or equivalent, covering Physical and Environmental Security for the data centres in which Descartes' infrastructure is located. Descartes management reviews:

- The scope, control objectives and control descriptions related to physical and environmental security, to determine whether report identifies physical security and environmental controls relevant;

- Report auditor's opinion letter and test results; and

- End User Control Considerations for physical and environmental controls listed to determine that they are in place.

Descartes management also follows up on exceptions affecting the physical and environmental security (if any) identified, with the third party's management to develop a corrective action plan and to identify compensating controls if necessary to mitigate associated risks.

A restricted number of Descartes personnel and contractors have access to the data center based on a written justification / revalidation with approval from management. Employees must register with the data center by providing photo ID and submit to biometric measurement. Identification must match and is evaluated upon each visit to the data center. Terminated or transferred employee access to Descartes' controlled area within the data center is revoked in a timely manner. Descartes management validates access rights to Descartes' controlled area on an annual basis. Changes in authorization result in service requests in the Descartes ticketing system and access authorization changes with the data center provider.

To monitor ongoing annual service delivery by 'co-location' service providers, Descartes has monitoring controls over the following four service elements: physical access, environmental protection, tape management/handling and power supply. Descartes uses the following ongoing operational controls to assess and monitor the third party's service delivery:

- To monitor physical access controls at the data center, Descartes has personnel that regularly visits the data center and observe the physical access controls in effect.

- Environmental protection and power supply are monitored through Descartes incident management process. The servers in the data centres are configured to provide alerts into the Descartes incident and problem management process.

6.1 Security Incidents

In addition to the concepts described in Incident and Problem Management sections, Descartes has a formal Security Incident Management policy with defined security incident processes, communication methods, and roles. This policy is based on the NIST Computer Security Incident Handling Guide SP800-60r2 with the following defined phases to prepare for, handle and to resolve a security incident:

- Preparation;

- Detection and Analysis;

- Containment, Eradication & Recovery; and

- Post-Incident Activity.

In the event of a security incident, the dedicated Information Security team will organize the formation of a Computer Security Incident Response team and handle the security incident according to the policy and procedure in coordination with the rest of the organization.