DATA PROTECTION AGREEMENT

Boomi and Provider have entered into a Provider Agreement under which Provider may process Boomi Data in connection with the provision of Solutions. This Data Protection Agreement, including its annexes and the Standard Contractual Clauses, ("**DPA**") governs Provider's processing of Boomi Data and shall form part of and be incorporated by reference into the Provider Agreement. At all times during the term of the Provider Agreement, or after the term if Provider retains access to Boomi Data, Provider shall, and shall cause its Representatives to, comply with this DPA. In the event of a conflict between the DPA, the NDA and/or the Provider Agreement, this DPA shall prevail.

1. **DEFINITIONS.** Terms not defined herein have the meanings set forth in the Provider Agreement.

1.1. **"Affiliate"** means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. **"**Control**"** means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully diluted basis) then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

1.2. **"Applicable Law"** means any and all applicable laws, statutes, and ordinances, rules, regulations, directives, edicts and similar governmental requirements of all international, federal, provincial, state, county, city, and borough departments, bureaus, boards, agencies, offices, commissions and other subdivisions thereof, or any other governmental, public, or quasi- public authority.

1.3. **"Boomi Group"** means Boomi, LP and Boomi, LP's and Brooklyn UK BidCo, Ltd's direct and indirect subsidiaries, and Boomi Group Company means any such entity.

1.4. **"Controller"** means an entity which, alone or jointly with others, determines the purposes and means of the processing of the Personal Data.

1.5. **"Data Breach"** means any accidental, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, use, modification, disposal, compromise, or access to Boomi Data or any act or omission that compromises or undermines the physical, technical, or organizational safeguards put in place by Provider in processing Boomi Data or otherwise providing Solutions.

1.6. **"Boomi Data"** means any and all data provided by a Boomi Group Company, its customers, authorized agents and/or subcontractors to Provider, or otherwise processed by Provider in connection with the provision of Solutions, including (a) all non-public information and data provided to or accessed by Provider through Boomi's network, or provided to or accessed by Provider for hosting or outsourcing services, (b) Highly Restricted Data, (c) Personal Data and/or (d) User Tracking Data.

1.7. **"EEA"** mean the Member States of the European Union plus Norway, Iceland and Liechtenstein.

1.8. **"Europe"** means for the purposes of this DPA the EEA, United Kingdom (**"UK"**) and Switzerland.

1.9. **"GDPR"** means the General Data Protection Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as amended or superseded from time to time.

1.10. **"Highly Restricted Data"** means Social Security or other government-issued identification numbers, medical or health information, account security information, individual financial account information, credit/debit/gift or other payment card information, account passwords, individual credit and income information, intellectual property, proprietary business models, pricing, customer infrastructure/system information or data flows and sensitive personal data as defined under Privacy Laws (including the GDPR).

1.11. **"Including"** means including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and "include" and its derivatives shall be construed accordingly.

1.12. **"Personal Data"** means any information or data that alone or together with any other information relates to an identified or identifiable natural person ("data subject"), or as otherwise defined as "personal data" or "personal information" under Privacy Laws. An identifiable natural person is one 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.

1.13. **"Privacy Laws"** means any law, statute, directive, or regulation, including any and all legislative and/or regulatory amendments or successors thereto, regarding privacy, data protection, information security obligations and/or the processing of Personal Data (including where applicable: (a) the GDPR; (b) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("UK GDPR") and the Data Protection Act 2018 (together, "UK Data Protection Laws"); (c) the Swiss Federal Data Protection Act and its implementing regulations ("Swiss DPA"); and (d) the California Consumer Privacy Act ("CCPA") and similar US state and federal laws to which a party to this DPA is subject and which are applicable to the Solutions provided, in each case, as may be amended, superseded or replaced.

1.14. "**Provider"** means the party from which Boomi is purchasing Solutions under the Provider Agreement and its Representatives.

1.15. **“Provider Agreement”** means the agreement or agreements between Boomi and Provider pursuant to which Boomi is purchasing Solutions from Provider, including a Master Purchase Agreement.

1.16. **“Processing”**, **“processed”** or **“process”** means any operation or set of operations performed upon Boomi Data whether or not by automated means, including access, receipt, collection, recording, organization, structuring, adaptation, alteration, retrieval, consultation, retention, storage, transfer, disclosure (including disclosure by transmission), dissemination or otherwise making available, restriction, alignment, combination, use, blocking, erasure and destruction.

1.17. **“Processor”** means an entity which processes the Personal Data on behalf of the Controller in order to perform Solutions purchased by Boomi under the Provider Agreement, or as otherwise defined as “Service Provider” under the Privacy Laws.

1.18. **“Representatives”** means any employee, officer, agent, consultant, auditor, Subcontractor, Subprocessor, outsourcer or other third party acting on behalf of Provider or under the apparent authority of Provider in connection with providing Solutions.

1.19. "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA 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 UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

1.20. **“Sell”** or **“sale”** or means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or any other non-monetary valuable consideration. Sale does not include Personal Data shared or transferred by Boomi to Provider for the provision of Solutions on behalf of Boomi under the Provider Agreement.

1.21. **“Standard Contractual Clauses”** means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (**"EU Standard Contractual Clauses"** or **"EU SCCs"**); and (ii) where the UK GDPR applies, the EU SCCs as amended by Part 2 of the International Data Transfer Agreement issued by ICO under s119A(1) of the Data Protection Act 2018, version B1.0, in force 21 March 2022, and any updates or replacements as may be issued by the ICO from time to time in accordance with s119A(1) (**"UK SCCs"**).

1.22. “**Subprocessors**” or “**Subcontractors:”** (i) means any Processor, including all subcontractors, acting for or on behalf of Provider (including any Provider Affiliate), providing Solutions to Boomi, or to whom Provider has assigned or delegated its contractual obligations to Boomi; (ii) includes any third party appointed by a Subcontractor which processes any Personal Data subject to this DPA; and (iii) does not include employees of Provider.

1.23. **“Solutions”** means any hardware, software (including third party components), software-as-a-service, services, or hosting services provided to Boomi or a Boomi customer pursuant to the Provider Agreement.

1.24. **“User Tracking Data”** means data associated with online or mobile users that records user information, interactions or behavior, user clicks or reaction to or interaction with content, advertising or any other activity, or in connection with tracking activities related to behavioral advertising.

2. **CONFIDENTIAL INFORMATION.** All Boomi Data is “Confidential Information” as defined in (a) the NDA; or (b) if Provider and Boomi have not entered into an NDA, the Provider Agreement. Any exclusions to the definition of “Confidential Information” in the NDA or the Provider Agreement shall not apply to the definition of Boomi Data. Provider shall treat Boomi Data as Confidential Information for as long as such Boomi Data is in Provider’s possession or control, including when the Boomi Data is held in archive, back up or business continuity/disaster recovery systems and shall ensure that all Representatives are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3. **PROVIDER OBLIGATIONS**

3.1. Role of Parties. The parties agree that Boomi is the Controller of Personal Data and Provider is the Processor of such data, except where Boomi acts as a Processor of Personal Data, in which case Provider is a subprocessor.

3.2. Processing. Provider shall (and shall ensure that its Representatives shall) only process Boomi Data in accordance with Boomi’s documented instructions, including with regard to international transfers of Boomi Data. Provider shall immediately inform Boomi in writing if, in its opinion, an instruction from Boomi infringes applicable Privacy Laws. Provider shall not knowingly process any Boomi Data in a way that results in Boomi being in breach of its obligations under Privacy Laws. Boomi hereby instructs and authorizes Provider to process Boomi Data for the sole and exclusive purpose of performing Provider’s obligations to Boomi under and in accordance with (a) the Provider Agreement; (b) Boomi’s and its agents’ written instructions; (c) Privacy Laws; and (d) this DPA (collectively, the “**Applicable Agreements**”). Where Provider tracks users’ online or mobile activities, the obligations and requirements set out in this DPA in relation to Personal Data extend to User Tracking Data.

3.3. Personal Data Processing. Provider shall process Personal Data as part of the provision of the Solutions as described below. Boomi may make reasonable amendments to this section by written notice to Provider from time to time as Boomi reasonably considers necessary:

(a) Subject Matter, Purpose and Duration. Provider shall process the Personal Data (for the term of the Provider Agreement as extended or amended) for the purpose of providing the Solutions specified in the Provider Agreement.

(b) Data Subjects. Personal Data processing may relate to any of the following data subjects: past, present and prospective employees, customers, end users, web site visitors, partners, clients, advisors, consultants, suppliers, contractors, subcontractors and agents, beneficiaries and relatives.

(c) Types of Personal Data. Personal Data processing may involve any of the following Personal Data (including special categories of data if appropriate): (i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails), (v) details of goods or services provided to or for the benefit of data subjects, and (vi) financial details (e.g. credit, payment and bank details).

3.4. Prohibition and limitations on Disclosure and Use. Provider shall not process, sell, transfer or otherwise disclose Boomi Data to, or permit processing by its Representatives or any Third Party except (a) on a need-to-know-basis related to the provision of the Solutions where instructed by Boomi; (b) to the extent necessary to provide the Solutions; (c) as permitted under the Applicable Agreements; or (d) if required by Applicable Law. If Provider is required by Applicable Law to transfer, disclose or permit processing of Boomi Data by a third party, Provider will promptly notify Boomi in advance of such requirement and cooperate with Boomi to limit the extent and scope of such transfer, disclosure or processing. Provider represents and warrants, i.e., certifies, that it understands the prohibitions and limitations regarding its use and all other processing activities and related purposes as outlined in the Provider Agreement (including this DPA) regarding Boomi Data, particularly in this Section. 3.4, and will comply with them.

3.5. Compliance with Privacy Laws. Provider agrees to comply with any and all Privacy Laws applicable to the provision of the Solutions and its processing of Personal Data.

3.6. Return and Destruction. Upon termination of the Provider Agreement or upon written request from Boomi, whichever comes first, Provider shall, and shall ensure that its Representatives and Subcontractors shall, immediately cease all processing of Boomi Data and return any Boomi Data to Boomi (by secure file transfer in such format as reasonably notified by Boomi to Provider) or, at the direction of Boomi, dispose of, destroy, or render permanently anonymous all Boomi Data, in each case using the security measures set out herein and certifying in writing to Boomi once the disposition, destruction or anonymisation has been fully completed. If Applicable Law does not permit Provider to destroy the Boomi Data, Provider shall not use the Boomi Data for any purpose other than as required by such Applicable Law and shall remain bound at all times with the provisions of the Applicable Agreements for as long as the Boomi Data is in Provider’s possession or control.

3.7. Notifications and Assistance. Taking into account the nature of the processing, Provider shall (and shall ensure its Subcontractors shall) assist Boomi by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Boomi’s obligations (as reasonably understood by Boomi) to respond to requests to exercise data subject rights under Privacy Laws in respect of the Personal Data. If Provider is contacted by a person with a request, inquiry or complaint regarding their Personal Data in connection with the Solutions, Provider shall (a) promptly and in any event within two calendar days provide Boomi with written notice of such request, inquiry or complaint; and (b) provide to Boomi all reasonable cooperation, assistance, information and access to Personal Data in its possession, custody or control as is necessary for Boomi to respond to such request, inquiry or complaint promptly and within any timeframe required by Privacy Laws. Provider shall not respond to such request, inquiry or complaint unless so instructed in writing by Boomi.

3.8 Privacy Impact Assessments. Provider shall provide cooperation and assistance to Boomi in connection with any privacy impact assessment(s) which Boomi may carry out in relation to the processing of Personal Data undertaken by the Provider, including any prior consultation(s) with supervisory authorities or other competent data privacy authorities which Boomi reasonably considers to be required by applicable Privacy Laws.

3.9 Controller status. Provider shall not determine the purposes and means of the processing of the Personal Data without Boomi’s prior explicit agreement in writing, in which case Provider shall be deemed a controller and shall only process the Personal Data as agreed in writing with Boomi and in full compliance with all applicable Privacy Laws.

4. **INTERNATIONAL TRANSFERS.**

4.1. Restricted Transfers outside of Europe. Provider may only conduct an onward Restricted Transfer with the prior written consent of Boomi, provided that such transfer is strictly necessary for the provision of the Solutions, is subject to the terms set out in the Standard Contractual Clauses and Provider complies with all Privacy Laws and this DPA. Provider shall ensure the same level of data protection as under this DPA and provide a copy of the safeguards to Boomi without undue delay. Notwithstanding the foregoing, the terms of the Standard Contractual Clauses shall not apply where and to the extent that Boomi adopts an alternative data export mechanism that is recognized by the relevant authorities or courts as providing an adequate level of protection or appropriate safeguards for Personal Data (**"Alternative Transfer Mechanism"**). The

Alternative Transfer Mechanism shall upon notice to Provider apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Privacy Laws applicable to Europe and extends to territories to which Personal Data is transferred) and Provider agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism (as applicable).

4.2. Transfers out of Asia Pacific. For countries located within the Asia Pacific region, Provider shall obtain Boomi's prior written consent where Personal Data will be transmitted by the Provider outside the country from which it was originally collected unless otherwise required by the Applicable Agreements.

4.3. Transfers out of countries with data export requirements. If any Privacy Laws require that further steps be taken in relation to any applicable data export restrictions to permit the transfer of Personal Data under the Agreement to Provider (including its Subcontractors), Provider will comply with such data protection requirements including executing any applicable data transfer agreements (e.g. standard contractual clauses) or an alternative solution to ensure that appropriate safeguards are in place for such transfer.

5. **APPROPRIATE SECURITY SAFEGUARDS.** Provider shall process the Boomi Data in a manner that ensures appropriate security of the Boomi Data (including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage) using appropriate technical and/or organisational measures which ensure a level of security commensurate to the risk, including as appropriate: (a) the encryption of the Boomi Data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) the ability to restore the availability and access to the Boomi Data in a timely manner in the event of a physical or technical incident, and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Boomi Data. In assessing the appropriate level of security, Provider shall take account in particular of the risks that may be presented by the processing of the Boomi Data, in particular from a Data Breach. Provider agrees to have in place and maintain as a minimum those information security measures set out in this DPA in Annex 3. As part of its compliance with this clause, Provider shall have and maintain appropriate and industry-standard physical, organizational and technical processes, security standards, guidelines, controls and procedures ("**Policies**") to protect against any Data Breach ("**Appropriate Safeguards**"). Provider shall regularly, but in no event less than annually, evaluate, test and monitor the effectiveness of its Appropriate Safeguards and shall promptly adjust and update Appropriate Safeguards as reasonably warranted by such results. Provider shall, upon request, provide Boomi with a written description of the Appropriate Safeguards. Provider shall provide Boomi with access to relevant documentation and reporting on the implementation, certification, effectiveness and remediation of the Appropriate Safeguards. Provider represents, warrants and covenants that Provider and its Subcontractors do and shall implement and maintain Policies which:

5.1. Risk Management. Evaluate organizational and administrative risks no less than annually, and system and technical risks no less than quarterly.

5.2. Asset Management. (a) Identify all equipment and media used in the processing of Boomi Data; (b) assign responsibility for all equipment and media to one or more custodians; and (c) require regular reviews of the asset inventory for accuracy and to identify missing equipment and media.

5.3. Access Control and Identity Management Policies. Prior to access to Boomi Data, (a) all data and system access rights are assigned to individuals according to their documented responsibilities and the principle of least privilege; (b) all user and administrator accounts are assigned to individuals and required to have strong passwords, password rotation, failed authentication locks and session timeouts; and (c) issuance of privileged access accounts require management approval and are held to strict security standards.

5.4. Awareness and Training Policies. Address (a) information security threats and best practices; (b) information security policies, procedures, and controls in place to protect Boomi Data; and (c) each Representative's roles and responsibilities in the protection of Boomi Data.

5.5. Accountability Policies. Ensure that (a) all account actions can be traced to the individual using the account, (b) the time, date and type of action is recorded for all privileged account actions and all account actions affecting Boomi Data, (c) all recorded account actions are actively monitored and can be easily retrieved for analysis, and (d) consequences for policy violations are established, communicated and acted upon.

5.6. Contingency Planning Policies. Define roles and responsibilities and provide clear guidance and training on the proper handling of contingency events including (a) natural threat events such as floods, tornadoes, earthquakes, hurricanes and ice storms; (ii) accidental threat events such as chemical spills and mechanical or electrical failures; and (iii) intentional acts such as privacy and security breaches, bomb threats, assaults and theft.

5.7. System Maintenance Policies. Are related to (a) structured vulnerability management, including regular scanning, penetration testing, risk analysis and timely patching; (b) change management, including documentation of the purpose, security impact analysis, testing plan and results, and authorization for all changes; (c) configuration management, including secure baseline configurations; and (d) monitoring to detect and generate alerts for unauthorized changes.

5.8. System and Communications Protection Policies. Preserve the confidentiality, integrity and availability of Boomi Data, including: (a) physical controls that restrict and monitor access to systems that process Boomi Data; (b) technical and administrative controls that protect against malicious software and malicious actors; (c) strong encryption of data in transit across untrusted and public networks and, in the case of Highly Restricted Data, at rest in all locations where it is stored; (d) periodic encryption key rotation and management; (e) prohibition of Highly Restricted Data and Personal Data being processed in non-production environments; (f) regular security control reviews and effectiveness testing; and (g) strong technical and administrative controls regarding remote access and mobile devices.

5.9. Media Protection Policies. Ensure that media containing Boomi Data is securely handled, including (a) strong encryption of Boomi Data on all mobile devices and removable storage; (b) requirement for secure sanitization and destruction methods for media that at any time held Boomi Data; and (c) requirement that all media, including paper, containing unencrypted Boomi Data be stored in a secure location.

6. **PAYMENT CARD INFORMATION.** If Provider processes, or is obligated to process, any cardholder data in connection with the Provider Agreement, then Provider, at its own expense, shall:

(a) prior to, and for the entire duration of, any such processing or processing obligation, be in full compliance with the Payment Card Industry Data Security Standard ("PCI DSS"); and

(b) prior to any such processing or processing obligation, and annually thereafter, provide Boomi with a written attestation, as well as any evidence in support thereof which Boomi reasonably requests, that Provider satisfies such PCI DSS compliance requirements and remains current with respect to its filings of the PCI Report on Compliance/Self Assessment Questionnaire and the PCI Quarterly Network Scan filings.

Any failure by Provider to comply with the above obligations of this Section will constitute a breach of the Provider Agreement and trigger Boomi's right to immediately terminate the Provider Agreement without liability to Boomi.

7. **INFRASTRUCTURE SECURITY & CONNECTIVITY.** If (a) the Solutions include application, website, data or system hosting; (b) network connectivity is required to provide the Solutions; or (c) the Solutions are dependent on the integrity of Provider's environment, the following requirements shall apply:

7.1. Network Access. The connection and mechanism to transmit Boomi Data between Provider and Boomi shall be through a Boomi I/T-approved secure solution. Duration of access shall be restricted to only when access is required. Provider shall use Appropriate Safeguards to protect against any compromise, unauthorized access or other damage to Boomi's network and to secure the Provider's networks and I/T environments associated with the Solutions. Upon request, Provider shall provide Boomi with a high level network diagram that outlines Provider's I/T network supporting the Solutions.

7.2. Audit. Upon request, Provider shall provide a controls audit report and remediation effort, such as a SSAE 16 or information security audit performed within the past year, as applicable to the Solutions. The audit shall include an assessment of Provider's applicable general controls and security processes and procedures to ensure compliance with Privacy Laws and industry standards. The audit shall be at Provider's expense as part of Provider's ongoing information security program to evaluate Provider's general security controls.

7.3. Testing. In addition to Provider's internal control programs, Provider will have independent penetration tests performed on its environment as relevant to this DPA not less than once year, and will perform security vulnerability scans not less frequently than quarterly. Provider commits to remediate all vulnerabilities identified in a timeframe commensurate with the risk, or as agreed upon with Boomi.

8. **SOLUTION SECURITY**

8.1. Vulnerabilities. Provider shall have controls in place to identify any security vulnerabilities in the Solutions during development and after release. Provider shall provide Boomi written notice of (a) publicly-acknowledged vulnerabilities/zero day exploits within five business days of the public acknowledgement; and (b) internally-known yet publicly-undisclosed vulnerabilities/zero day exploits within ten business days of their discovery. Provider commits to remediate all vulnerabilities identified in the Solutions at Provider's expense, and to remediate vulnerabilities with a base score above 4 as defined by Common Vulnerability Scoring System in a timeframe commensurate with the risk or as agreed upon with Boomi. Provider's use of open source code shall not alter Provider's responsibility to identify and remediate vulnerabilities as described here.

8.2. Coding Practices. Provider agrees (a) to use industry secure-coding practices (for example, Microsoft's Software Development Lifecycle, Cigital Software Security Touchpoints, OWASP standards or Sans Top 25); (b) the Solutions are designed based on industry secure-coding practices; and (c) information security is addressed throughout the development life-cycle. The Solutions' processes, direct capabilities, and other necessary actions shall comply with all PCI standards and Privacy Laws.

8.3. Security Assessments. Provider shall submit the results and remediation efforts of an independent security assessment for all Solutions that (a) are customer facing, including websites, shipped with or installed on customer systems; or (b) process Highly Restricted Data. The assessment scope and remediation efforts must be agreed upon by Boomi and addressed to Boomi's satisfaction prior to acceptance of such Solutions.

9. **DATA BREACH.** Provider shall notify Boomi not later than 24 hours after becoming aware of an actual or reasonably suspected Data Breach. Such notification must be provided, at a minimum, by email with a read receipt to privacy@boomi.com and with a copy to Provider's primary business contact within Boomi. In facilitating investigation and remediation of a Data Breach, Provider shall cooperate fully with Boomi. Provider shall not inform any third party of any Data Breach without first obtaining Boomi's

written consent except as may be strictly required by Privacy Laws in which case Provider will, unless prohibited by law, notify Boomi in advance of informing any such third party and cooperate with Boomi to limit the scope of the information disclosed to what is required by Privacy Laws. Details of any complaint received by Provider related to processing of Highly Restricted, Personal Data or User Tracking Data shall be promptly sent to Provider's Boomi business contact. Provider shall reimburse Boomi for costs Boomi incurs in responding to, remediating, and/or mitigating damages caused by a Data Breach or in following up a complaint by an individual data subject or a regulator. Provider shall take all necessary and appropriate corrective actions, including as may be instructed by Boomi or Privacy Laws, to remedy or mitigate any Data Breach. Provider shall, to the extent such information is known or available to Provider at the time, notify Boomi of the following: (a) the nature of the Data Breach including, where possible, the categories and approximate number of data subjects affected and number of Personal Data records concerned; (b) the name and contact details of Provider's data protection officer or other contact point where more information can be obtained; (c) a description of the likely consequences of the Data Breach; and (d) a description of the measures taken or proposed to be taken by Provider to address the Data Breach, including (where appropriate) measures to mitigate its possible adverse effects. Where it is not possible for Provider to provide the above information at the same time, Provider shall provide the information in phases without undue further delay. The information must be provided, at a minimum, by email with a read receipt to privacy@Boomi.com and with a copy to Provider's primary Boomi business contact.

10. REPRESENTATIVES AND SUBCONTRACTORS

10.1. Restrictions. Unless expressly permitted by the Provider Agreement Provider shall not (a) transfer; (b) sell or disclose; (c) subcontract the processing of; or (d) permit the processing of, Boomi Data by or to any Subcontractors without the prior written authorisation of Boomi. Notwithstanding the foregoing, Boomi consents to Provider engaging Subcontractors provided that: Provider provides at least 60 days prior written notice to Boomi (such notice to be provided to procurement@boomi.com) of the engagement of any new Subcontractor (including details of the processing and location of the processing) and Provider shall update the list of all Subcontractors engaged to process the Personal Data under this DPA at Annex 4 and send such updated version to Boomi prior to the engagement of the Subcontractor in the terms indicated above. If Boomi objects to the engagement of any Subcontractor, then either Provider will not engage or permit the Subcontractor to process the Personal Data or Boomi may elect to suspend or terminate the processing of Personal Data under the Provider Agreement and/or terminate the Provider Agreement without any further liability or obligation to Provider, and Provider shall refund to Boomi any amounts which were paid for work not yet performed under the Provider Agreement.

10.2. Requirements for Subcontractors and Representatives. Provider shall take all reasonable steps to ensure the reliability of Representatives and Subcontractors that may have access to the Boomi Data, including carrying out appropriate background checks (where permitted by Applicable Law) and carrying out adequate due diligence to ensure that any Representatives and Subcontractors are capable of providing the level of protection for Boomi Data required by this DPA. Provider shall ensure Representatives and Subcontractors are appropriately trained in the handling and secure processing of Boomi Data under Privacy Laws. Provider shall only retain Subcontractors that Provider can reasonably expect to appropriately protect the privacy, confidentiality and security of the Personal Data. If Provider is permitted by Boomi to transfer Boomi Data to a Subcontractor, Subcontractor shall comply with Section 4 "International Transfers" of this DPA. Provider remains fully liable for any breach of this DPA or the Provider Agreement that is caused by an act, error, or omission of such Subcontractor.

10.3. Subcontractor Agreement. Agreements by and between Provider and the Representatives and Subcontractors authorized to Process Boomi Data ("**Subcontractor Contracts**") shall include substantially equivalent restrictions and conditions as this DPA and shall be in writing. Provider shall have sole liability for all acts or omissions of Representatives and Subcontractors. Provider shall provide Boomi with a copy of Subcontractor Contracts upon request.

10.4. Subcontractor Audits. Provider shall audit each of its Subcontractors that process Boomi Data at least once every twelve months and more frequently in the event of a Data Breach. If the audit reveals any compliance deficiencies, breaches and/or failures by the Subcontractor, Provider shall promptly notify Boomi and use all reasonable efforts to work with the Subcontractor to remedy the same promptly. If, within Boomi's reasonable discretion, a satisfactory remedy cannot be implemented within a reasonable time, Boomi may instruct Provider not to continue using the Subcontractor to provide Solutions to Boomi, in which case Provider shall be required, as instructed by Boomi, to promptly return or delete any Boomi Data in the Subcontractor's possession or control. To the extent not restricted by confidentiality, Provider shall share the results of such audits with Boomi upon prior written request. Boomi agrees that it will comply with the confidentiality obligations in this DPA in relation to any disclosed audit results.

11. **CANADIAN DATA**. If Provider processes Personal Data concerning persons located in Canada in the course of providing Solutions, Provider and Boomi agree to the additional obligations and requirements in this Section 12. Provider shall not take any actions or make any omissions that will cause Boomi to be in contravention of the Personal Information Protection and Electronic Documents Act (Canada), as amended or supplemented from time to time, and any other Canadian federal or provincial legislation governing the processing of Personal Data. Provider shall keep all data, databases or other records containing Personal Data processed in connection with the Solutions logically isolated and separate from any information, data, databases or other records processed by Provider for itself or for third parties. Provider shall designate and identify to Boomi an individual responsible for the oversight of the Personal Data. Boomi may be required to disclose, without advance notice or consent, Confidential Information of Provider to authorities in connection with any investigation, audit or inquiry in connection with the Solutions. Provider shall not move, remove, or transmit any Personal Data from Provider's facilities without the express consent of Boomi and without using appropriately secure technology to protect such information while in transit. If Provider is contacted by a person with a request, inquiry or complaint regarding their Personal Data in connection with the Solutions, Provider shall promptly refer such person to Boomi.

12. **SUPPLEMENTAL AGREEMENTS TO THE DPA.**

12.1. EU Standard Contractual Clauses. If Provider processes Personal Data that is subject to the GDPR, in the course of providing Solutions, Provider and Boomi hereby agree that, when the transfer of Personal Data from Boomi (as "data exporter") to Provider (as "data importer") is a Restricted Transfer and Privacy Laws require that appropriate safeguards are put in place, such transfer shall be subject to the EU Standard Contractual Clauses, which shall be deemed incorporated into, and form part of, this DPA, as further specified in Annex 1 of this DPA. Should the EU Commission issue and require use of amended or updated EU Standard Contractual Clauses, such clauses shall be incorporated herein by this reference automatically and supersede prior versions of the Standard Contractual Clauses as of the date such amended or updated EU Standard Contractual Clauses become effective as set by the EU Commission.

12.2. UK Transfer Mechanism. In relation to transfers of Personal Data subject to the UK GDPR from the UK to countries outside the UK (which are not subject to an adequacy decision under UK GDPR), Provider agrees to comply with the UK SCCs. The UK SCCs are incorporated herein by reference, form an integral part of this DPA, and shall be interpreted in accordance with the following:

(a) the UK SCCs' Tables 1 (Parties) and 2 (Selected SCCs, Modules, and Selected Clauses) shall be deemed populated with the corresponding information set forth in Annex 1, Section 2 of this DPA;

(b) the UK SCCs' Table 3 (Appendix Information) shall be deemed populated as follows:

(i) the list of Parties is set out in Section 1;

(ii) the description of the transfer is set out in Annex 1;

(iii) the relevant information is set out in Annex 3 (Technical and Organisational Measures); and

(iv) the list of subprocessors is set out in Annex 4;

(c) the UK SCCs' Table 4 (Ending the Addendum) shall be deemed completed with the selection of "neither Party."

12.3. Switzerland Transfer Mechanism. In relation to transfers of Personal Data subject to the Swiss DPA, Provider agrees to process such Personal Data in compliance with the EU SCCS, as implemented under the above Section 13.1 and modified as follows:

(a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA (as applicable);

(c) references to "EU," "Union" and "Member State law" shall be replaced with references to Switzerland;

(d) Clause 13(a) and Part C of Annex II shall not be used and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner (as applicable);

(e) 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" (as applicable);

(f) in Clause 17, the SCCs shall be governed by the laws of Switzerland; and

(g) in Clause 18(b), disputes shall be resolved before the courts of Switzerland.

12.4. Conflict. If and to the extent there is a conflict between the Standard Contractual Clauses, including those versions set forth pursuant to Sections 13.1, 13.2 and 13.3 above, and any provision of the Provider Agreement (including this DPA), the terms of the Standard Contractual Clauses shall prevail.

12.5. Alternative Transfer Mechanism. The Standard Contractual Clauses shall not apply where and to the extent that Boomi adopts an alternative data export mechanism recognized by the relevant authorities or courts as providing an adequate level of protection or appropriate safeguards for Personal Data ("Alternative Transfer Mechanism"). Upon notice to Provider, the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Privacy Laws applicable to Europe and extends to territories to which Personal Data is transferred). Should such Alternative Transfer Mechanism apply, Provider agrees to execute any documents and take any other actions that Boomi reasonably deems necessary for such Alternative Transfer Mechanism to have proper legal effect.

12.6. HIPAA Compliance. If Provider creates, receives, transmits, accesses, maintains, is exposed to, or becomes aware of "Protected Health Information" as defined in 45 C.F.R. § 160.103 in the course of providing Solutions, Provider and Boomi hereby agree to and Provider shall comply with, as applicable, the US HIPAA Subcontractor Agreement and the Business Associate Agreement set out at www.boomi.com/supplierBAA (respectively, the "HIPAA Subcontractor Agreement" and the "Business Associate Agreement"). To the extent applicable, the HIPAA Subcontractor Agreement and the Business Associate Agreement are incorporated herein in full by reference.

12.7. Authority. PROVIDER REPRESENTS AND COVENANTS TO BOOMI THAT PROVIDER IS AUTHORIZED TO BIND PROVIDER TO ALL PROMISES AND COMMITMENTS, IN THIS AGREEMENT AND ITS ATTACHMENTS.

13. **BOOMI GROUP RIGHTS**. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA. Where the Solutions include the processing by Provider Representatives of Boomi Data on behalf of Boomi Group Company, each such Boomi Group Company is intended to be a third party beneficiary and may enforce the terms of this DPA as a third party beneficiary against Provider in respect of that Boomi Group Company's own Boomi Data, as if such Boomi Group Company were a party to this DPA and/or any Provider Agreements.

14. **AUDITS**. Provider shall make available to Boomi upon request all information necessary to demonstrate compliance with its obligations under this DPA and shall permit Boomi or its designee to (a) audit Provider's compliance with this DPA; and (b) inspect any Personal Data in the custody or possession of Provider. Provider shall promptly respond to all inquiries from Boomi with respect to Provider's handling of Personal Data.

15. **RECORD KEEPING**. Provider shall maintain a written or electronic record of processing activities carried out on behalf of Boomi containing the following minimum information: (a) name and contact details of Provider and its Subcontractors, (b) name and contact details of its data protection officer (if any), (c) the categories of processing carried out on behalf of each controller, (d) any transfers of personal data to countries outside the EEA and documentation showing Model Clauses are in place, (e) a general description of the technical and organisational security measures in place to safeguard the Personal Data including the measures in this DPA.

16. **INDEMNIFICATION.** Provider shall defend, indemnify and hold harmless Boomi and Boomi's directors, officers, employees, representatives, and agents from and against any and all claims, actions, demands, and legal proceedings and all liabilities, damages, losses, judgments, authorized settlements, costs, fines, penalties and expenses including reasonable attorneys' fees arising out of or in connection with (a) Provider's breach of this DPA; (b) Provider's failure to comply with the PCI DSS; or (c) violation by the Provider of any Privacy Laws.

17. **MISCELLANEOUS.**

17.1. Survival. Provider's obligations under this DPA shall survive the termination or expiration of the DPA, NDA, and the Provider Agreement and continue in effect for as long as Provider continues to process Boomi Data.

17.2. Notices. Legal notices shall be made in writing to the Notice Address set forth in the Provider Agreement. Written notice made by facsimile, overnight courier, registered mail or certified mail and sent to the Boomi Notice Address or Provider Notice Address (or to successor individuals and addresses that have been properly noticed to the other party) are deemed to be effective upon sending. All other written communications, deliveries or business notices between Provider and Boomi required by, permitted by or pertaining to this DPA shall be effective when received.

17.3. Assignment. Provider may not assign or transfer this DPA, in whole or in part, whether voluntarily, by contract or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Boomi. Any attempt to assign or transfer this DPA other than in accordance with this Section will be null and void. Boomi may assign the DPA without Provider consent.

17.4. Waiver/Amendment. No waiver of any term or condition is valid unless in writing and signed by authorized representatives of both parties, and shall be limited to the specific situation for which it is given. No amendment or modification to this DPA shall be valid unless set forth in writing specifically referencing this DPA and signed by authorized representatives of both parties. No other action or failure to act shall constitute a waiver of any rights.

17.5. Entire agreement. This DPA sets forth the entire agreement and understanding of the parties relating to the subject matter herein, and replaces all prior or contemporaneous discussions and agreements between the parties, both oral and written.

17.6. Independent contractor. In performing Provider's responsibilities pursuant to this DPA, it is understood and agreed that Provider is at all times acting as an independent contractor and that Provider is not a partner, joint venturer, or employee of Boomi. It is expressly agreed that Provider will not for any purpose be deemed to be an agent, ostensible or apparent agent, or servant of Boomi, and the parties agree to take any and all such action as may be reasonably requested by Boomi to inform the public and others utilizing the professional services of Provider of such fact.

17.7. Additional agreements. Each of the parties hereto agrees to execute any document or documents that may be requested from time to time by the other party to implement or complete such party's obligations pursuant to this DPA, Privacy Law or Applicable Law. The parties agree to take such reasonable actions as are necessary to amend this DPA from time to time as is necessary for Boomi to comply with Privacy Law and Applicable Law.

17.8. Interpretation. Any ambiguity in this DPA will be resolved in favor of a meaning that permits Boomi to comply with Privacy Law and Applicable Law. In addition, in no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

17.9. Governing Law; Venue. The DPA and any disputes between Provider and Boomi (and their Representatives) including without limitation, tort and statutory claims arising under or relating in any way to the DPA or any relationships contemplated herein shall be governed and construed in accordance with the laws of the State of Delaware, U.S., exclusive of any provisions of the United Nations Convention on the International Sale of Goods and without regard to its principles of conflicts of law, unless required otherwise by Privacy Laws or the Standard Contractual Clauses. Provider and Boomi irrevocably submit and consent to the exclusive jurisdiction and venue of the U.S. District Court for the District of Delaware or if there is no basis for Federal jurisdiction, then any claims must be brought in the Delaware State Court in Wilmington County, Delaware. The parties agree that such courts shall be the exclusive proper forum for the determination of any claim or dispute arising out of, or in connection with, the DPA and waive any objection to venue or convenience of forum.

ANNEX 1
EU STANDARD CONTRACTUAL CLAUSES

1. Transfer Mechanism

(a) In relation to transfers of Personal Data protected by the GDPR, to the extent that the Boomi is a Controller of the Personal Data processed by Provider, Module Two (Controller to Processor) of the EU SCCs will apply in accordance with Section 2 below.

(b) In relation to transfers of Personal Data protected by the GDPR, to the extent that the Boomi is a Processor of the Personal Data processed by Provider, Module Three (Processor to Processor) of the EU SCCs will apply in accordance with Section 2 below.

2. Optional Provisions and Annexes

(a) In Clause 7, the optional docking clause will apply;

(b) In Clause 9 , Option 2 will apply and the time period for prior notice of Subprocessor changes will be as set forth in Section 3.2 of this DPA;

(c) In Clause 11, the optional language will not apply;

(d) In Clause 17, Option 1 shall apply, and the EU SCCs will be governed by Irish law;

(e) Under Clause 18(b) of the Standard Contractual Clauses, disputes arising from the Standard Contractual Clauses will be resolved before the courts of Ireland;

(f) In Annex I, Part A shall be completed as follows:

A. Data Exporter

Name:	Boomi LP
Address:	1W Elm Street, Suite 200 Conshohocken, PA 19428 United States
Contact person’s name, position and contact details:	Conor Swaine, Global Privacy Lead Privacy@Boomi.com
Role	Controller or Processor

B. Data Importer

Name:	
Address:	
Contact person’s name, position and contact details:	
Role	Processor

(g) In Annex I, Part A shall be completed as follows:

A. *Categories of data subjects and Personal Data:* are as set out in Annex 2

B. *Frequency of transfer:* The transfers occur on a semi-continuous basis in order to provide the Solutions

C. Subject matter and nature of Processing: are as set out in Annex 2

D. Purpose of the transfer and further Processing: are as set out in Annex 2

E. *Period of retention:* Personal data, shall be retained for the duration of the provision of the Services as set out in the Documentation. Deletion shall be as set out in the DPA.

F. Duration of Processing: as set out in Annex 2

(h) In Annex I, Part C shall be completed as follows:

The competent supervisor authority shall be Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

(i) Subject to section 5 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 3 to the DPA.

ANNEX 2
DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

DATA EXPORTER. The data exporter is identified at the start of the Clauses and is a provider of IT products and services. The data exporter is the Controller and has appointed the data importer to provide certain products and/or services as specified in the Provider Agreement as its Processor. To facilitate the provision of these products and services, the data exporter may provide to the data importer access to the personal data described below.

DATA IMPORTER. The data importer is a signatory to the Clauses and a provider of products and/or services. The data importer will be the recipient of personal data which is exported by the data exporter to the data importer as described below.

B. DESCRIPTION OF TRANSFER

DATA SUBJECTS. The personal data transferred may concern the following categories of data subjects:

- Past, present and prospective employees and partners;
- Past, present and prospective clients, customers, end users, web site visitors;
- Past, present and prospective advisors, consultants, suppliers, contractors, subcontractors and agents;
- Beneficiaries and relatives.

CATEGORIES OF DATA. The data subjects' personal data transferred may concern the following categories of data:

1. Contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information);
2. Employment details (which may include company name, job title, grade, demographic and location data);
3. IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies);
4. Data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);
5. Details of goods or services provided to or for the benefit of data subjects;
6. Financial details (e.g. credit, payment and bank details).

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE). Personal data transferred may include information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union opinions, memberships or activities, social security files, and data concerning health (including physical or mental health or condition), sexual life and information regarding criminal offences or alleged offences and any related court proceedings and shall include special categories of data as defined in Article 8 of the Directive 95/46/EC.

PROCESSING OPERATIONS. The personal data transferred may be subject to the following processing activities: Any operation with regard to personal data irrespective of the means applied and procedures, in particular the obtaining, collecting, recording, organizing, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, archiving, transmission, blocking, erasing, or destruction of data, the operation and maintenance of systems, management and management reporting, financial reporting, risk management, compliance, legal and audit functions and shall include "processing" which shall have the meaning given to such term in the Directive.

TRANSFER DETAILS. The duration of the processing is until the termination of the Provider Agreement in accordance with its terms plus the period from the expiry of the Provider Agreement until deletion of the Personal Data by Boomi in accordance with the terms of the Provider Agreement, including this DPA. **T**he frequency of the transfer (e.g., whether the data will be transferred on a one-off or continuous basis), and purpose of the data transfer shall be for purpose of providing Services, as subscribed by the Boomi, as further specified in the Documentation, including the selected service levels and support options. The Agreement and the relevant service descriptions and statements of work shall apply for the specifics and possible additional services.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

ANNEX 3

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

SECURITY PRACTICES. Data importer has implemented corporate information security practices and standards that are designed to safeguard data importer's corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the data importer's executive management and are periodically reviewed and updated where necessary. Data importer shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

ORGANIZATIONAL SECURITY. It is the responsibility of the individuals across the data importer's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, data importer's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – the IS function drives data importer's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.

2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.

3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.

4. **Forensic investigations** – the IS function works with Security Operations, Legal, Global Privacy Office and Human Resources to carry out investigations, including eDiscovery and eForensics.

5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

ASSET CLASSIFICATION AND CONTROL. Data importer's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that data importer might track include:

1. information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information
2. software assets, such as identified applications and system software
3. physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. **Screening/background checks:** Where reasonably practicable and appropriate, as part of the employment/recruitment process, data importer shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to data importer's networks, systems or facilities.

2. **Identification:** Data importer shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other data importer entities or customers for whom the employee is providing services.

3. **Training:** Data importer's annual compliance training program includes a requirement for employees to complete a data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.

4. **Confidentiality:** Data importer shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. **Physical Security Program:** Data importer shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Data importer's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which personal data is processed and continually monitor any changes to the physical infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of data importer. Data importer balances its approach towards security by considering elements of control that include architecture, operations and systems.

2. **Physical Access controls:** Physical access controls/security measures at data importer's facilities/premises are designed to meet the following requirements:

   (a) access to data importer's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the data importer. Only personnel associated with data importer are provided access to data importer's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

   (b) relevant data importer facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

   (c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or keycard assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the data importer's facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary (up to 14 days) credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to data importer's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

   (d) employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

   (e) visitors who require access to data importer's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

   (f) select data importer facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

   (g) locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

   (h) for data importer's major data centres, security guards, UPS and generators, and change control standards are available;

   (i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. **Security incident response plan:** Data importer maintains a security incident response policy and related plan and procedures which address the measures that data importer will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the data importer's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

DATA TRANSMISSION CONTROL AND ENCRYPTION. Data importer shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, data importer shall:

1. implement industry-standard encryption practices in its transmission of personal data. Industry-standard encryption methods used by data importer includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by data importer. The data importer's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to

unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including data importer's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

SYSTEM ACCESS CONTROLS. Access to data importer's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. **Admission Controls** (i.e. measures to prevent unauthorized persons from using data processing systems):

    (a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;
    (b) access to IT systems will be granted only when a user is registered under a valid username and password;
    (c) data importer has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;
    (d) mandatory password changes on a regular basis;
    (e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;
    (f) data and user classification determines the type of authentication that must be used by each system;
    (g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **Access Controls** (i.e. measures to prevent unauthorised access to systems):

    (a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);
    (b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;
    (c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;
    (d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. Data importer applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve the data importer's relevant business purposes
2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;
3. third party use of personal data is governed through contractual terms and conditions between the third party and data importer which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

SEPARATION CONTROL. Where legally required, data importer will ensure that personal data collected for different purposes can be processed separately. Data importer shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. Data importer protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, data importer's record management policy and practices, as well as legal retention requirements;
2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;
3. electronic personal data is given to data importer's IT Asset Management team for proper disposal;
4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. Data importer has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

SYSTEM DEVELOPMENT AND MAINTENANCE. Publicly released third party vulnerabilities are reviewed for applicability in the data importer environment. Based on risk to data importer's business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

COMPLIANCE. The information security, legal, privacy and compliance departments work to identify regional laws and regulations that may be applicable to data importer. These requirements cover areas such as, intellectual property of the data importer and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

ANNEX 4
LIST OF SUBPROCESSORS

Provider uses a range of Subcontractors, including the following:

Name	Description of processing	Location