

Data Processing Addendum

Last updated: March 21, 2023

This Data Processing Addendum ("DPA") between you, the user, together with any company or other business entity you are representing, if any (collectively, the "Customer") and the VistaPrint Contracting party as applicable under the Agreement ("VistaPrint") is incorporated by reference, and supplements, and forms part of, the terms governing the use of the different VistaPrint Services, as amended from time to time (collectively, the "Agreement"). This DPA applies where and to the extent VistaPrint is acting as a Processor or Service Provider (as applicable) of Personal Data on behalf of the Customer under the Agreement. This DPA will be effective and will replace and supersede any previously applicable terms relating to their subject matter as of the Effective Date of the Agreement and shall remain in force until such time as the Agreement is terminated.

1. DEFINITIONS

"Adequate Country" means, as applicable (i) where the EU GDPR applies, the European Economic Area ("EEA") or a country or territory which is deemed to ensure an adequate level of protection by the European Commission; (ii) where the UK GDPR applies, the UK or a country or territory recognized as ensuring adequate data protection pursuant to Section 17A of the UK Data Protection Act 2018 as amended or replaced; and (iii) where the Swiss FADP as amended or replaced applies, Switzerland or a country or territory outside Switzerland which has been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

"Business Purpose" means the limited purpose specifically identified in Annex I for which VistaPrint receives or accesses Personal Data.

"Data Protection Laws" means all applicable data protection and privacy laws and regulations, as applicable to a party, including, but not limited to, where applicable, the EU Data Protection Laws, and the US Data Protection Laws, and any other state or national data protection, data privacy or data security laws applicable to the scope of the Services, in each case as amended, superseded, or replaced from time to time.

"End-Users Personal Data" means Personal Data pertaining to visitors and users of Customer's services and Processed by VistaPrint on behalf of Customer for the provision of the Services.

"EU Data Protection Laws" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "EU GDPR"), (ii) the GDPR as incorporated into United Kingdom domestic law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the Swiss Federal Act on Data Protection of 19 June 1992 and its corresponding ordinances ("FADP"); (iv) the EU Directive 2002/58/EC on Privacy and Electronic Communications; and (v) any EU Member State or UK law made under or pursuant to items (i) - (iii); in each case as amended, superseded or replaced from time to time.

"Personal Data", **"Data Subject"**, **"Process"** or **"Processing"**, **"Controller"**, and **"Processor"** shall have the meaning given in the applicable Data Protection Laws or, if not defined therein, the GDPR, and the terms **"Business"** and **"Service Provider"** have the meanings given to them in the CCPA.

"Services" means the different services provided by VistaPrint to Customer on its website, where and to the extent VistaPrint is acting as a Processor or Service Provider (as applicable) on behalf of the Customer under the relevant Agreement, including, but not limited to, the ProAdvantage Program Agreement and the ProShop Terms of Use.

"Standard Contractual Clauses" or **"SCCs"** means (i) where the EU GDPR and/or the Swiss FADP applies, the [EU standard contractual clauses](#) as approved by the European Commission's Decision

(EU) 2021/914 of 4 June 2021 (“EU SCCs”); and (ii) where the UK GDPR applies, the [EU SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses](#) as issued by the UK Information Commissioner’s Office (“UK Addendum”), in each case, as may be amended, superseded, or replaced from time to time. The EU SCCs and UK Addendum are incorporated by reference and form an integral part of this DPA.

“**Sub-Processor**” means any entity engaged by VistaPrint, including its Affiliates, to assist in fulfilling its obligations pursuant to the Agreement or this DPA.

“**Transfer Risk Assessment**” means the additional guarantees to supplement the guarantees provided by the SCCs and UK Addendum.

“**US Data Protection Laws**” means all applicable laws and regulations of any jurisdiction in the United States relating to privacy, data protection or data security (in each case, as amended, superseded or replaced from time to time), including, without limitation, as applicable, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, together with the regulations promulgated thereunder (collectively, the “CCPA”); the Virginia Consumer Data Protection Act; the Colorado Privacy Rights Act; the Connecticut Data Privacy Act; and the Utah Consumer Privacy Act.

Other capitalized terms used but not defined in this DPA shall have the meaning given in the Agreement.

2. ROLES AND SCOPE OF PROCESSING

2.1. Role of the Parties. The Parties agree that, with respect to Processing End-Users Personal Data under this DPA, Customer acts as the Data Controller or Business (as applicable) and VistaPrint acts as the Data Processor or Service Provider (as applicable).

Customer acknowledges that VistaPrint acts as an independent Data Controller with regards to Personal Data that it collects directly from customers or visitors through its consumer-facing applications and services.

2.2. Scope of Processing. Each party shall comply with all applicable Data Protection Laws and its respective obligations under the Agreement and this DPA in relation to its Processing of the End-Users Personal Data as described in Annex I. Without limiting the foregoing, VistaPrint shall provide the same level of privacy protection as is required of Businesses (as defined in the CCPA) by the CCPA.

3. OBLIGATIONS OF THE PARTIES

3.1. Customer’s Obligations. In using the Services provided by VistaPrint:

- (i) Customer warrants and represents it has provided notice to the Data Subjects and has established all legal basis and obtained all consents necessary under applicable Data Protection Laws for VistaPrint, and its Sub-Processors, to Process End-Users Personal Data on its behalf and provide the Services pursuant to the Agreement, including this DPA.
- (ii) Customer is solely responsible for the accuracy and quality of the End-Users Personal Data provided and the legality of the means by which Customer acquires, discloses, and processes End-Users Personal Data. Customer remains exclusively liable for its own compliance with applicable Data Protection Laws with respect to any independent collection and processing of Personal Data unrelated to the Services.
- (iii) Customer instructs VistaPrint to process End-Users Personal Data on its behalf pursuant to this DPA and shall ensure its instructions comply with applicable Data Protection Laws. This DPA and the Agreement are Customer’s complete and final instructions to VistaPrint. Additional instructions outside the scope of the Agreement or this DPA must be agreed upon

separately in writing, including any additional fees that may be payable by Customer to VistaPrint for carrying out such additional instructions.

3.2. VistaPrint's Obligations. VistaPrint shall, in respect of the Processing of the End-Users Personal Data:

- (i) only Process End-Users Personal Data for the Business Purpose and in accordance with Customer's instructions, to the extent that the instructions are compatible with the Agreement and this DPA;
- (ii) treat End-Users Personal Data as confidential information and Process it only to the extent, and in such manner, as is necessary to perform the obligations under the Agreement and for the purposes further specified in Annex I below. VistaPrint may not Process End-Users Personal Data for any other purpose, unless VistaPrint is required to do so by law. In such case, VistaPrint will inform Customer in writing of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;
- (iii) assist Customer in ensuring compliance with its obligations under applicable Data Protection Laws, which could include, but is not limited to, in conducting any required privacy impact assessment or prior consultation with the relevant data protection authorities upon reasonable request from Customer;
- (iv) inform Customer if it believes that Customer's Processing instructions infringe applicable Data Protection Laws. In such case, VistaPrint reserves the right to stop Processing End-Users Personal Data until Customer issues new instructions, and VistaPrint shall not be liable to Customer for any failure to provide the Services under the Agreement during such period;
- (v) ensure that its employees and Sub-Processors who have access to End-Users Personal Data are subject to appropriate confidentiality obligations;
- (vi) notify Customer of any determination made that it can no longer meet its obligations under this DPA or Data Protection Laws;
- (vii) promptly notify Customer of any requests made by any Data Subject or enforcement agency in relation to the Processing of End-Users Personal Data so that Customer can respond to any such request; and
- (viii) promptly provide such cooperation and assistance as reasonably required by Customer to fulfil its obligations under Data Protection Laws in relation to Data Subject requests or any request from applicable government regulator or supervisory authority.

To the extent permitted by applicable Data Protection Laws, VistaPrint may use aggregated and anonymized data derived from the End-Users Personal Data ("Anonymized Data") internally to build and improve the quality of the Services, provided that such Anonymized Data does not constitute Personal Data under the applicable Data Protection Laws.

3.3. VistaPrint's Prohibited Processing Activities. VistaPrint shall not:

- (i) Sell or Share (as defined in the CCPA) End-Users Personal Data or retain, use, or disclose the End-Users Personal Data for any Commercial Purposes (as defined by the CCPA) or outside of its direct business relationship with Customer and under Customer's prior written authorization only; and
- (ii) co-mingle or combine End-Users Personal Data with its own data or the data of any third party, other than as strictly required to perform the Services.

VistaPrint certifies that it understands and will comply with the restrictions on the use of End-Users Personal Data in connection with the Services set forth in this DPA.

4. RIGHTS OF DATA SUBJECT

To the extent VistaPrint is able, and in line with applicable law, VistaPrint shall, taking into account the nature of the Processing, provide reasonable assistance to enable Customer to respond to any requests received from Data Subjects to exercise their rights under applicable Data Protection Laws. Customer shall cover all costs incurred by VistaPrint in connection with its provision of such assistance. If any such request is made directly to VistaPrint, VistaPrint will inform Customer, unless VistaPrint is legally prohibited from doing so, and Customer shall be solely responsible for responding to such a request. VistaPrint bears no responsibility for information provided in good faith to Customer in reliance on this Section.

5. SUB-PROCESSORS

5.1. General Authorization. Customer hereby grants VistaPrint a general authorization to engage Sub-Processors (including its Affiliates) to process End-Users Personal Data in order to provide the Services and fulfill its obligations under the Agreement and this DPA. VistaPrint will, subject to the confidentiality provisions of the Agreement and upon previous request by Customer, make available to Customer a list of the Sub-Processors it engages.

5.2. Responsibilities. VistaPrint shall impose substantially the same contractual obligations on its Sub-Processors as those imposed on VistaPrint under this DPA, to the extent applicable to the nature of the services provided by each Sub-Processor.

5.3. Objection Right for New Sub-Processors. When engaging new Sub-Processors, VistaPrint will provide Customer with prior notice, as soon as reasonably practicable, when and to the extent that such engagement is in connection with the provision of the applicable Services.

5.3.1. Customer may object to VistaPrint's appointment or replacement of a Sub-Processor in writing within a period of ten (10) business days from receipt of the notice based on reasonable grounds relating to applicable Data Protection Laws. In such event, VistaPrint may, in its sole discretion, choose to use commercial reasonable efforts (but is not required to) to make available to you an alternative solution to avoid the Processing of End-Users Personal Data by the new or replacement Sub-Processor. Until VistaPrint makes a decision concerning Customer's objection, VistaPrint may be required to temporarily suspend the Processing of the related End-Users Personal Data, including, if required for this matter, suspend or limit access to Customer's Account or suspend or limit certain features of the Services offered to Customer. If VistaPrint is reasonably able to provide the Services to the Customer in accordance with the Agreement without using the Sub-Processor and decides in its discretion to do so, then Customer will have no further rights under this Section in respect of the proposed use of the Sub-Processor.

5.3.2. If VistaPrint, in its discretion, requires use of the Sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement Sub-Processor within thirty (30) days from receipt of your valid reasoned objection, then Customer may terminate the applicable Agreement effective upon the date VistaPrint begins use of such new or replacement Sub-Processor solely with respect to the Services that will use the proposed new sub-Processor for the Processing of Personal Data by providing written notice to VistaPrint. Such termination will be without prejudice to any fees incurred by Customer prior to the termination of the affected Services and Customer will have no further claims against VistaPrint in connection with the termination of the affected Services.

5.3.3. If Customer does not object in writing to VistaPrint's appointment of a new Sub-Processor within ten (10) business days from receipt of the notice, Customer agrees that it will be deemed to have consented to that new Sub-Processor.

5.4. Liability. VistaPrint remains liable for any breach of this DPA caused by an act or omission of its Sub-Processors, to the same extent VistaPrint is liable for its own, except as otherwise set forth in the Agreement.

6. INTERNATIONAL DATA TRANSFERS

6.1. In General. As part of providing the Services, Customer authorizes VistaPrint, its Affiliates and its Sub-Processors to store, Process and transfer End-Users Personal Data anywhere in the world where VistaPrint, its Affiliates or Sub-Processors maintain data processing operations. Where EU, UK or Swiss Personal Data is transferred outside the EEA, the UK or Switzerland, VistaPrint shall only Process or permit the Processing of EU, UK or Swiss Personal Data outside of the EEA, the UK or Switzerland if one of the following conditions is met:

- a) the EU, UK or Swiss End-Users Personal Data are transferred to an Adequate Country; or
- b) the Standard Contractual Clauses and the Transfer Risk Assessment are in place between VistaPrint and Customer and/or between VistaPrint and the Sub-Processor, as appropriate.

6.2. EU Personal Data Transfers. To the extent that Personal Data is transferred from any EEA jurisdiction for which the GDPR governs the international nature of the transfer, the EU SCCs form part of this DPA, and they will be deemed completed as follows:

- (i) Module two (Controller to Processor) terms shall apply where Customer is a Controller and a data exporter of Personal Data and VistaPrint is a Processor and data importer in respect of that Personal Data.
- (ii) Module three (Processor to Processor) terms shall apply where VistaPrint is a Processor acting on behalf of a Controller and a data exporter of Personal Data, and the Sub-Processor is a Processor and data importer in respect to that Personal Data.
- (iii) Clause 7 (a)-(c) shall apply;
- (iv) Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes will be in accordance with the notification process set out on the Sub-Processor provisions of this DPA.
- (v) Clause 11 will not apply;
- (vi) Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law specified in the Agreement, provided that law is an EU Member State law recognizing third party beneficiary rights, otherwise, the laws of the Netherlands shall apply;
- (vii) Clause 18 (b), disputes shall be resolved before the courts specified in the Agreement, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of the Netherlands. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;
- (viii) The Annexes of the EU SCCs shall be populated with the relevant information set out in Annex I, Annex II and Annex III of this DPA; and
- (ix) If and to the extent the EU SCCs conflict with any provision of this DPA, the EU SCCs will prevail to the extent of such conflict.

6.3. UK Personal Data Transfers. To the extent that UK Personal Data is transferred for which the UK GDPR governs the international nature of the transfer, the EU SCCs referenced in Section 6.2 above shall apply together with the UK Addendum, and will be deemed completed as follows:

- (i) Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA;
- (ii) Table 4 in Part 2 of the UK Addendum shall be deemed completed by selecting “importer”; and
- (iii) Any conflict between the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

6.4. Swiss Personal Data Transfers. To the extent that Personal Data is transferred from Switzerland in a manner that would trigger obligations under the Federal Act on Data Protection of Switzerland (“FADP”), the EU SCCs shall apply to such transfers and shall be deemed to be modified in a manner to incorporate relevant references and definitions that would render such EU SCCs an adequate tool for such transfers under the FADP, including but not limited to the following:

- (i) The competent supervisory authority in Annex I.C of the EU SCCs under Clause 13 is the Federal Data Protection and Information Commissioner of Switzerland;
- (ii) The applicable law for contractual claims under Clause 17 of the EU SCCs is Swiss law or the law of a country that allows and grants rights as a third party beneficiary;
- (iii) The term “member state” used in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c); and
- (iv) The EU SCCs also protect the data of legal entities until the entry into force of the revised FADP.

6.5. Additional Safeguards. To the extent that VistaPrint processes Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the EEA, UK or Switzerland, VistaPrint has implemented a variety of additional safeguards regarding the transfer of such Personal Data from these jurisdictions. VistaPrint has conducted a Transfer Risk Assessment, which will be provided to Customer upon written request to the email dataprotection@vista.com.

7. DATA SECURITY AND DATA BREACH NOTIFICATION

7.1. Security Measures. VistaPrint has implemented and will maintain appropriate technical and organizational security measures to protect End-Users Personal Data against unauthorized or unlawful Processing and accidental loss or alteration (“Security Incident”). In particular, VistaPrint has implemented the technical and organizational measures as listed in Annex II.

7.2. Data Breach Notification. In the event VistaPrint becomes aware of a Security Incident impacting End-Users Personal Data, VistaPrint will take reasonable steps to notify Customer without undue delay and shall:

- (i) provide Customer with such information about the Security Incident as it is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to VistaPrint, and any restrictions on disclosing the information such as for confidentiality.
- (ii) At Customer’s request, provide reasonable assistance to enable Customer to notify appropriate authorities or impacted Data Subjects as required under applicable Data Protection Laws.

A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of End-Users Personal Data. VistaPrint’s notification of or response to a Security Incident will not constitute an acknowledgment of fault or liability with respect to said Security Incident.

8. AUDITS

8.1. Audit Reports. Upon Customer’s written request at reasonable intervals (no more than once per year) and subject to confidentiality obligations, VistaPrint will provide a copy of VistaPrint’s then most recent summaries of third-party audits, certifications or reports, as applicable. The parties agree that the Customer’s audit rights described in applicable Data Protection Laws will be satisfied by VistaPrint’s provision of such summaries and/or reports.

8.2. Supervisory Authority Audit. VistaPrint shall provide Customer with reasonable access to its documentation and systems in the event of an audit required by a government regulator or supervisory authority for compliance with applicable Data Protection Laws.

8.3. Confidential Information. Any information provided by VistaPrint under this Section 8 constitutes confidential information. VistaPrint will not be required to disclose any commercial secrets, including algorithms, source code, trade secrets and similar information.

9. DATA DELETION

The parties agree that upon termination of the DPA or Customer's written request, VistaPrint shall, and shall cause any Sub-Processors to securely destroy all End-Users Personal Data and any copies thereof as soon as reasonably practicable in accordance with the terms of the Agreement and applicable laws. Notwithstanding the foregoing, VistaPrint may retain all or part of the End-Users Personal Data disclosed if required under the Agreement or by applicable law or regulation (including applicable Data Protection Laws), provided such End-Users Personal Data remains protected in accordance with the terms of this DPA and applicable Data Protection Laws.

10. MISCELANEOUS

10.1. **Hierarchy.** In the event of any inconsistencies or conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail to the extent of that conflict in connection with the Processing of End- Users Personal Data. To the extent that there is any conflict between the Standard Contractual Clauses (where applicable), this DPA or the Agreement, the Standard Contractual Clauses shall prevail.

10.2. **Updates to the DPA.** VistaPrint may modify this DPA as required from time to time and will post the most current version on the site. Any such changes or modifications shall be effective upon posting. By continuing to use or access the Services after any modifications come into effect, Customer agrees to be bound by the modified DPA.

10.3. **Governing Law.** This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.4. **Limitation of Liability.** All activities under this DPA (including without limitation Processing of End-Users Personal Data) remain subject to the applicable limitations of liability set forth in the Agreement.

10.5 **Contact.** Any questions regarding this DPA should be addressed to the Data Protection Officer at dataprotection@vista.com. VistaPrint will attempt to resolve any complaints regarding the use of End-Users Personal Data in accordance with this DPA and the Agreement.

ANNEX I - DESCRIPTION OF PROCESSING/TRANSFER

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as the "Customer" or the name specified in Customer's account.

Address: The Customer's Billing Address specified in Customer's account.

Contact person's name, position and contact details: The contact information specified in Customer's account.

Activities relevant to the data transferred under these Clauses: Any activities relevant for the purposes of receiving the Services provided by VistaPrint in connection with the Agreement.

Signature and date: By entering into the DPA, data exporter is deemed to have signed the Standard Contractual Clauses and Annexes incorporated herein as of the DPA Effective Date.

Role (controller/processor): Controller

Data importer(s):

Name: Vistaprint's Contracting Party as applicable under the Agreement.

Address: Vistaprint's Contracting Party address as applicable under the Agreement.

Contact person's name, position and contact details: dataprotection@vista.com.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of VistaPrint Services.

Signature and date: By entering into the DPA, data importer is deemed to have signed the Standard Contractual Clauses and Annexes incorporated herein as of the DPA Effective Date.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects: Data subjects may include, but are not limited to:

- End-users (who are natural persons), such as existing and prospective customers, clients, or visitors, that are users of Customer's service.
- Current, former or prospective Customer's representatives, employees, candidates, agents, consultants, freelancers, business partners, sub-contractors and/or collaborators (who are natural persons).
- Third party individuals with whom Customer decides to engage through the Service.

Categories of personal data: Personal Data submitted within the scope and nature determined by Controller in its sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards: The parties do not anticipate the transfer of sensitive data.

Frequency of the transfer: Continuous basis depending on the use of the Services by Customer.

Nature of the processing: Performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing: We may use your Personal Data for the following purposes (and tasks related to such purposes), all in accordance with the Agreement and in a way that is proportionate and that respects your End-Users Personal Data:

- Providing you with the Services;
- Acting upon your instructions;
- Performing and enforcing the Agreement and this DPA;
- Defending our rights;
- Preventing, investigating and mitigating data security risks and incidents, fraud, errors and/or illegal or prohibited activities;
- Complying with applicable laws and regulations

Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: VistaPrint will retain the Personal Data until termination of the Agreement and in accordance with Section 9 of the DPA, unless otherwise established under the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Sub-Processors will Process Personal Data as necessary to perform the Services pursuant to the Agreement and for the duration of the Agreement, unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: The Dutch Data Protection Authority, unless required otherwise by Section 6 of the DPA.

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

VistaPrint currently maintains the following technical and organizational security measures for the protection, confidentiality and integrity of Personal Data. Please note that VistaPrint may modify these practices at its discretion. Any modifications made will not materially decrease the overall security and protection of Personal Data.

1. Preventing unauthorised persons from gaining access to systems with which Personal Data are processed or used (physical access control); in particular, by taking the following measures:
 - Controlled access for critical or sensitive areas
 - Incident logs
 - Automated systems of access control
 - ID or chip card readers
 - Security awareness training
2. Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:
 - Network devices such as intrusion detection systems, routers and firewalls.
 - Secure log-in with unique user-ID/password including password complexity requirements and multi-factor authentication where appropriate.
 - Policy mandates locking of unattended workstations. Screensaver password is implemented such that if user forgets to lock the workstation, automatic locking is ensured.
 - Logging and analysis of system usage.
 - Role-based access for critical systems containing Personal Data.
 - Process for routine system updates for known vulnerabilities.
 - Encryption of laptop hard drives.
 - Monitoring for security vulnerabilities on critical systems.
 - Deployment and updating of antivirus software.
 - Network devices such as intrusion detection systems, routers and firewalls.
 - Compliance with Payment Card Industry Data Security Standard.
3. Ensuring that persons entitled to use a system can gain access only to the data to which they have a right of access, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (access control to data); in particular, by taking the following measures:
 - Network devices such as intrusion detection systems, routers and firewalls.
 - Secure log-in with unique user-ID/password including password complexity requirements and multi-factor authentication where appropriate.
 - Logging and analysis of system usage.
 - Role based access for critical systems containing Personal Data.
 - Encryption of laptop hard drives.
 - Deployment and updating of antivirus software.
 - Compliance with Payment Card Industry Data Security Standard.
4. Ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage by taking the following measures:
 - Secure log-in with unique user-ID/password including password complexity requirements and multi-factor authentication where appropriate.

- Secure transmission protocols.
 - Logging and analysis of system usage.
 - Role based access for critical systems containing Personal Data.
 - Network devices such as intrusion detection systems, routers and firewalls.
 - Deployment of a VPN.
5. Ensuring that Personal Data is processed solely in accordance with company policy, by taking the following measures:
- Mandatory security and privacy awareness training for all employees.
 - Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant personal data and, where allowed by local law.
 - Diligently selecting appropriate personnel and service providers.
 - Entering into appropriate data processing agreements with sub-processors, which include appropriate technical and organizational security measures.
6. Ensuring that Personal Data is protected against accidental destruction or loss (availability control); in particular, by taking the following measures:
- Regular testing of the effectiveness of security measures.
 - Backup procedures and recovery systems.
 - Redundant servers in separate location.
 - Uninterruptible power supply and auxiliary power unit.
 - Remote storage.
 - Climate monitoring and control for servers.
 - Deployment and updating of antivirus software.
 - Disaster recovery and emergency plan.
7. Ensuring that data collected for different purposes or different principals can be processed separately (separation control); in particular, by taking the following measures:
- Role based access for critical systems containing Personal Data.
 - Separation of test and live data.
 - Compliance with Payment Card Industry Data Security Standard.

ANNEX III - LIST OF SUB-PROCESSORS

A list of the Sub-Processors we engage and our purpose for engaging them is accessible upon request by the Customer.