Data Sharing & Processing Addendum
(UK & EU & Switzerland)

This Addendum applies to the sharing and processing of Personal Data by the Parties in connection with the Services and the Vendor-Requested Services form part of the Agreement.
The Parties agree that this Addendum sets forth the terms and conditions of sharing and processing Personal Data for the following purposes:

(i) Providing and/or using the Services, where both Parties act as the Data Controllers,
(ii) Performing the Vendor-Requested Services, where the Vendor acts as the Data Controller and 2Checkout acts as the Data Processor; and, where applicable,
(iii) Transferring of Personal Data to Third Countries, in accordance with applicable Data Protection Laws.

THEREFORE, THE PARTIES AGREE TO THE FOLLOWING:

1. DEFINITIONS

"Additional Safeguards"	means any legal instrument, safeguards, or measures to be entered into by the Parties of this Addendum as may be required under the applicable Data Protection Laws to Transfer the Personal Data from the territory outside the EEA or the United Kingdom or Switzerland, including but not limited to the EU SCCs.
"Agreement"	means the master services agreement, merchant agreement, payment services agreement, terms and conditions, framework agreement or any other agreement governing the provision of the Services by 2Checkout to the Vendor, together with any applicable Order Form, Statement of Work, service order, implementation plan, Applicable Documentation, amendment, addendum or other contractual document executed or otherwise agreed by the Parties from time to time.
"Data Controller"	means the controller of the Personal Data under the applicable Data Protection Laws, as identified in Clause 3 of this Addendum.
"Data Processor"	means the processor of the Personal Data under the applicable Data Protection Laws, as identified in Clause 3 of this Addendum.
"Data Exporter"	means the Data Controller or the Data Processor transferring the Personal Data to the Data Importer.
"Data Importer"	means the Data Controller or the Data Processor receiving the Personal Data from the Data Exporter.
"Data subject"	means any identified or identifiable natural person whose personal data, is shared under this Addendum.
"Data Breach"	means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data.
"Data Protection Laws"	means all privacy and data protection laws applicable to Vendor and/or 2Checkout in respect of the processing of Personal Data under this Addendum, including all binding regulatory requirements, guidance and codes of practice issued by a relevant regulatory authority and, as applicable, the European Data Protection Law.
"EEA"	all member states of the European Union, Norway, Iceland, and Liechtenstein.
"EU Adequacy Decisions"	means the decisions issued by the European Commission that a non-EU country, territory, or organization provides an adequate level of data protection that is essentially equivalent to the protections under the EU GDPR. The list of countries recognized as providing an adequate level of data protection is determined by the European Commission and may be changed. A current list of the countries recognized by the European Commission may be accessed here.
"European Data Protection Law"	means, as applicable: (a) Regulation (EU) 2016/679 (the "EU GDPR") and the national data protection and privacy laws of the EEA member states implementing or supplementing it (including the e-Privacy Directive); (b) the retained EU GDPR as it forms part of the law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 (the "UK GDPR"), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations and the Data (Use and Access) Act

	2025; and (c) the Swiss Federal Act on Data Protection (the "Swiss FADP"); in each case as amended or superseded from time to time.
"EU-U.S. Data Privacy Framework", "EU-U.S. DPF"	means the decision of the EU Commission 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU-US Data Privacy Framework.
"EU Standard Contractual Clauses", "EU SCCs"	means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to Data Importers, as set out in the Annex to Commission Decision 2021/914, or such alternative clauses as may be approved by the European Commission from time to time.
"Shoppers' Personal Data"	means Personal Data of shoppers shared between the Parties for the purpose of performing the Agreement. Description of the Shoppers' Personal Data is provided in Schedule 1.A(i) and in Schedule 1.A. (ii) attached hereto.
"2Checkout's Personnel Data"	means Personal Data of 2Checkout's personnel shared between the Parties for the purpose of performing the Agreement and maintaining the relations between the Parties. Description of 2Checkout's Personnel Data is provided in Schedule 1.B attached hereto.
"Vendor's Personnel Data"	means Personal Data of Vendor's personnel shared between the Parties for the purpose of performing the Agreement and maintaining the relations between the Parties. Description of the Vendor's Personnel Data is provided in Schedule 1.C attached hereto.
"Payment information"	means only those limited payment-related references and subscription identifiers that 2Checkout, acting in its sole reasonable discretion and subject to applicable law, payment card scheme rules, acquiring bank requirements, PCI DSS, regulatory obligations and technical feasibility, determines may be disclosed to a New Provider solely for the purpose of facilitating an approved merchant migration. Such information may include, where available and legally, contractually and technically permissible, subscription identifiers, transaction reference numbers, Acquirer Reference Numbers (ARNs), card scheme transaction reference identifiers, recurring payment reference identifiers, transferable payment token references (where portability is supported by the applicable token service), and other limited payment-related references approved by 2Checkout in writing. For the avoidance of doubt, Payment Information does not include payment credentials, payment card data, Sensitive Authentication Data as defined by PCI DSS, PCI DSS security information, tokenization keys, fraud prevention information, anti-money laundering or customer due diligence information, sanctions screening information, underwriting information, internal risk assessments, regulatory reporting information, proprietary analytics, or any information that 2Checkout is prohibited from disclosing under applicable law, contractual obligations, payment card scheme rules or regulatory requirements.
"Personal Data"	has the meaning given under European Data Protection Law.
"Personnel Data"	means jointly: Vendor's Personnel Data, and 2Checkout's Personnel Data.
"Processing Activity"	means any operation or set of operations performed on Personal Data for a specific purpose in connection with the Services, regardless of whether such activity is performed as part of a standard service offering, an optional service, a customization, an implementation, a configuration, an integration or any other engagement under the Agreement.
"Onward Transfer"	means transfer of the Personal Data by the Data Importer to either a Third-Party Controller or a Third-Party Processor.
"Security Measures"	means a minimum set of security measures specified in Schedule 2.A, as may be updated or reissued from time to time.
"Services"	means any products, platforms, dashboards, software, applications, features, functionalities, APIs, connectors, integrations, tools, modules, implementations, support services, managed services, professional services, Vendor-Requested Services, optional services, or any other products, services or functionality provided by 2Checkout under or in connection with the Agreement, including the provision of, or access to, any platform, dashboard, portal, interface, API, connector

	or other technical environment made available to the Vendor or its authorized users, as further described in the Agreement, any Order Form, Statement of Work, Applicable Documentation or other contractual documentation executed by the Parties.
"Sub-processor(s)"	means any party entrusted by the data processor to process Personal Data on its behalf. For the avoidance of doubt, if a subcontractor has access to or otherwise processes Personal Data, this subcontractor qualifies as a Sub-processor.
"Sub-processor(s) of 2Checkout"	means any party, including 2Checkout's affiliates and non-affiliated Third-Party, entrusted by 2Checkout to process Personal Data on its behalf. A list of the authorized Sub-processors of 2Checkout is provided in Schedule 3.A, and may be updated from time to time.
"Supplementary Security Measures"	means supplementary measures referred to in the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", adopted by the European Data Protection Board on 18 June 2021, which may be implemented to ensure the compliance of the Transfer with the relevant data transfer mechanisms as specified in Schedule 2.B attached hereto.
"Swiss Adequacy Decisions"	means decisions adopted by the Swiss Federal Council that the destination country guarantees an appropriate level of data protection, published in the annex to the Ordinance to the Federal Act on Data Protection (Annex 1 DPO), as amended from time to time.
"Swiss-U.S. Data Privacy Framework", "Swiss-U.S. DPF"	means a reliable mechanism for personal data transfers to the United States from Switzerland consistent with the Swiss FADP.
"Transfer", "Transferring", "Transferred" and any other variations of this term	means sending to and storage of the Personal Data within a Third Country, or making Personal Data accessible to the Data Importer established in the Third Country.
"Third country", "Third countries"	means any country, territory or specific sector that does not ensure an adequate level of data protection as required under the applicable Data Protection Laws, including: (i) where the EU GDPR applies, any country, territory or sector outside the EEA not covered by the relevant EU Adequacy Decision; (ii) where the UK GDPR applies, any country, territory or sector outside the UK not covered by the relevant UK Adequacy Regulations; and (iii) where the Swiss FADP applies, any country, territory or sector outside Switzerland not covered by the relevant Swiss Adequacy Decision.
"Third-Party Controller"	means any Third-Party, acting as the Controller, to whom the Data Importer, transfers Personal Data either under a contract or other legal act between the Importer and the Third-Party Controller.
"Third-Party Processor"	means any Third-Party acting as a Processor to whom either Party entrusts the processing of Personal Data.
"UK Adequacy Regulations"	means regulations under the UK GDPR under which the legal framework in the Data Importer's country, territory, international organization or particular sector has been assessed as providing 'adequate' protection for people's rights and freedoms regarding their personal data, as updated from time to time.
"UK Extension to the EU-U.S. Data Privacy Framework", "UK Extension to the EU-U.S. DPF"	means a reliable mechanism for personal data transfers to the United States from the United Kingdom (and Gibraltar) consistent with UK law, in force from October 12, 2023.
"Vendor-Requested Services"	means any Services, including any Service Customizations, implementation services, professional services, managed services, support services, integrations, configurations, migrations, bespoke developments, marketing services, analytics services, reporting services, customer communication services, campaign management services, cookie or other tracking technology implementations, promotional campaigns, abandoned cart campaigns, or any other functionality, feature or Processing Activity requested, purchased, activated, configured or otherwise instructed by the Vendor and performed by 2Checkout on behalf of the Vendor in accordance with the Vendor's documented instructions. For the

	avoidance of doubt, Vendor-Requested Services include, without limitation, services previously described or marketed as Professional Services, Marketing Services or similar service offerings, irrespective of how such services are designated, renamed, grouped or otherwise described in the Agreement, the Applicable Documentation or any other contractual documentation.
"Personal data/data", "Special categories of personal data", "Processing", "controller". "processor"	have the meaning given to the relevant terms in the applicable Data Protection Laws.

2. INTERPRETATIONS

2.1. In the event of any conflict or ambiguity between:

the provisions of this Addendum and the provisions of the Agreement, the provisions of this Addendum shall prevail;

(i) the provisions of this Addendum and the provisions of the Appendices, the provisions of the Appendices shall prevail;

(ii) the provisions of this Addendum and the provisions of any Additional Safeguards executed, the provisions of the Additional Safeguards shall prevail with respect to Personal Data subject to the Transfer covered by such Additional Safeguards;

(iii) the provisions of this Addendum and the provisions of the Data Processing Agreement (Attachment 1), the provisions of the Data Processing Agreement shall prevail with respect to Personal Data entrusted under the Data Processing Agreement to be processed by the Data Processor;

(iv) the provisions of the Data Processing Agreement (Attachment 1) and the provisions of any executed Additional Safeguards, the provisions of the executed Additional Safeguards shall prevail with respect to Personal Data subject to the Transfer covered by such Additional Safeguards; and

(v) the provisions of the Supplementary Measures and the provisions of any executed Additional Safeguards, the provisions of the Supplementary Measures shall prevail with respect to Personal Data subject to the Transfer covered by such Supplementary Measures.

2.2. Where the UK GDPR applies, references in this Addendum to the EU GDPR, to EU or EEA Member State law and to competent supervisory authorities shall be read to include, as applicable, the UK GDPR, the law of the United Kingdom and the UK Information Commissioner's Office. Where the Swiss FADP applies, those references shall be read to include, as applicable, the Swiss FADP, Swiss law and the Swiss Federal Data Protection and Information Commissioner, so that data subjects in Switzerland retain equivalent rights and remedies under Swiss law.

3. RELATIONSHIP OF THE PARTIES

3.1. Where 2Checkout processes Personal Data for Vendor-Requested Services solely on the Vendor's behalf and under its documented instructions, the Vendor shall act as the Data Controller (or Processor, where applicable) and 2Checkout shall act as the Data Processor (or Sub-processor, where applicable) for those specific Processing Activities only.

3.2. Any Processor or Sub-processor relationship under this Section applies exclusively to the specific Processing Activities performed in connection with the relevant Vendor-Requested Services and does not affect 2Checkout's role as an independent Data Controller for any other Processing Activities under the Services, including payment processing, merchant onboarding, underwriting, fraud prevention, sanctions screening, anti-money laundering compliance, tax determination and remittance, invoicing, settlement, refunds, chargeback management, shopper support, subscription management, platform security, operational resilience, record retention, regulatory reporting or compliance with applicable contractual, legal and regulatory obligations.

3.3. For each category of Personal Data, the Parties act as follows:

(i) Shoppers' Personal Data - for providing the Services by 2Checkout, including processing orders and payments, fraud prevention and refunds: 2Checkout acts as Data Controller and Data Exporter; the Vendor acts as Data Controller and Data Importer.

(ii) Shoppers' Personal Data - for providing the warranty, license conditions, specific instructions and technical support by the Vendor: 2Checkout acts as Data Controller and Data Exporter; the Vendor acts as Data Controller and Data Importer.

(iii) Shoppers' Personal Data - for providing Vendor-Requested Services: 2Checkout acts as Data Processor and Data Exporter; the Vendor acts as Data Controller and Data Importer.

(iv) 2Checkout's Personnel Data - for managing the business and contractual relationship between the Parties (including providing the Vendor with access to the Dashboard, the ability to monitor sales performance, and technical support), ensuring compliance with the Vendor's security and legal obligations, and pursuing a legitimate interest of the Data Controller or third parties: 2Checkout acts as Data Controller and Data Exporter; the Vendor acts as Data Controller and Data Importer.

(v) Vendor's Personnel Data - for managing the business and contractual relationship between the Parties (including using the Services), ensuring compliance with 2Checkout's security and legal obligations (including regulatory compliance, risk assessment and account verification), and pursuing a legitimate interest of the Data Controller or third parties: 2Checkout acts as Data Controller and Data Importer; the Vendor acts as Data Controller and Data Exporter.

4. SUBJECT MATTER OF THIS ADDENDUM

4.1. Data Controller – to – Data Controller Processing and Personal Data Sharing

4.2. When performing the Services, the Parties may share the following categories of the Personal Data:

(i) Shoppers' Personal Data - described in Schedule 1.A.(i);

(ii) Vendor's Personnel Data - described in Schedule 1.C.; and

(iii) 2Checkout's Personnel Data - described in Schedule 1.B.

4.2.1. Both 2Checkout and the Vendor are independent Data Controllers in respect of the Shoppers' Personal Data processed by either Party in a course of performance of the Agreement for the purpose of providing the Services (namely e-commerce related operations that facilitates the online payments and invoice) by 2Checkout and for the purpose for providing warranty and technical support to the shoppers by the Vendor (namely to active/de-activate subscription, providing activation codes and any other support that is related to the services/products provided by the Vendor to the shoppers).

4.2.2. Both 2 Checkout and the Vendor are independent Data Controller of the other Party's Personnel Data and hereby confirm that they collect, access, and process the other Party's Personnel Data as reasonably necessary, mainly for the management of the Agreement, including the use of the Platform and Dashboard functionalities made available under the Agreement.

4.2.3. The Parties hereby agree to share Personal Data in accordance with the terms and obligations set forth in this Addendum.

4.2.4. If Personal Data shared in accordance with this Clause 4.1., is Transferred to the other Party, the Parties agree that the Transfer of the Personal Data shall be carried out in compliance with the Additional Safeguards, as determined in accordance with the applicable Data Protection Laws and subject to Clause 8.2. of this Addendum.

4.2.5. For the avoidance of any doubts, the Parties acknowledge and agree that 2Checkout shall retain sole responsibility for the processing of certain categories of personal data that are subject to heightened confidentiality and regulatory obligations. Accordingly, unless the Parties agree otherwise, and provided that the Vendor meets all requirements to receive such data (e.g. PCI DSS certification, SOC certification etc.), 2Checkout shall not, disclose or grant access to the Vendor to the following categories of personal data:

(i) Know our customer data as part of the customer due diligence: data pertaining to the Vendor, such as business information, ownership, and control information, identity information, including ID, financial data, information required for Know Your Customer (KYC) obligations, utility bills, credit, litigations and financial history, to prevent fraudulent conduct or behavior that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud.

(ii) Underwriting data: data pertaining to the Vendor, such as business information, ownership, and control information, identity information, including ID, financial data, information required for Know Your Customer (KYC) obligations, utility bills, credit, litigations and financial history, full name of the business owner, date of birth of the Vendor/business owner, physical address, e-mail address, phone number, SSN (social security number) or TIN (taxpayer identification number), bank information (bank name, account number, routing number), business registration details (legal name, commercial name, registration number, date and place of registration), website URL, information on criminal convictions and offenses and politically-exposed persons.

(iii) Anti-fraud data: data pertaining to the shoppers, such as transaction data (details of financial transactions including date, time, amount, location, and parties involved), user information (personal and account information such as name, address, contact details, account numbers), device and location information (data related to the device used for transactions and the geographic location to assess the legitimacy of transactions), authentication and authorization data (information about authentication methods, login attempts, and authorization processes to ensure secure access to accounts and services).

(iv) PCI DSS and payment security data: payment card data, authentication data, payment security information and any other data processed or generated to comply with the Payment Card Industry Data Security Standard ("PCI DSS"), applicable card scheme rules, payment security requirements or equivalent regulatory or contractual obligations. This includes, where applicable, primary account numbers (PAN), payment tokens, payment credentials, authentication data, cryptographic information, encryption keys, tokenization data, security logs, access logs, audit records, vulnerability assessment results, penetration testing records, fraud detection indicators, card scheme compliance information and other payment security records.

(v) The above categories of data are processed by 2Checkout solely for the purposes of transaction authorization, fraud prevention, financial risk mitigation, and compliance with applicable laws and regulatory frameworks, including but not

limited to the Data Protection Laws, Payment Card Industry Data Security Standard (PCI DSS), AML/CTF laws, and equivalent international obligations.

4.2.6. The Vendor acknowledges and agrees that it has no right to request, access, or receive from 2Checkout the personal data referred to in Clause 4.1.7 unless:

(i) a specific legal obligation imposed on the Vendor requires such disclosure, e.g. if the Vendor is an individual and submits the request for access to its personal data in accordance with the applicable Data Protection Laws, or

(ii) such disclosure is governed by a separate written agreement between the Parties or other legally required documentation.

4.2.7. For further information regarding the purposes of processing and the categories of personal data processed by Verifone in its capacity as a Data Controller and a Data Exporter, please refer to the Privacy Informing Notice, which may be updated from time to time at Verifone's sole discretion. In the event of any inconsistency, the Privacy Notice shall be read as a complementary document, providing additional context regarding the processing of personal data by 2Checkout under applicable Data Protection Laws.

4.3. Data Controller – to – Data Processor Processing and Personal Data Sharing

4.3.1. If any Service provided by 2Checkout to the Vendor, in particular, the Vendor-Requested Services , involves 2Checkout processing any personal data, including but not limited to the Shoppers' Personal Data, as described in the Schedule 1.A.(ii), on behalf of the Vendor, then the Parties hereby record their intention that the Vendor shall be, respectively, the Data Controller or the Data Processor, and 2Checkout shall be, respectively, the Data Processor or the Sub-processor of the personal data processed in the course of providing the Vendor-Requested Services under the Agreement. In any such case, the Vendor entrusts those personal data, including the Shoppers' Personal Data, as described in the Schedule 1.A.(ii) to 2Checkout for processing under the terms and obligations set forth in the Data Processing Agreement, attached hereto as Attachment 1, as agreed upon by the Parties.

4.3.2. If personal data shared in accordance with this Clause 4.2. is Transferred to the other Party, the Parties agree that the Transfer of the Personal Data shall be carried out in compliance with the Additional Safeguards, as determined in accordance with the applicable Data Protection Laws and subject to Clause 8.3. of this Addendum.

4.3.3. The Vendor shall cooperate with 2Checkout in good faith to facilitate data protection compliance and risk mitigation throughout the engagement.

5. DATA PROTECTION OBLIGATIONS

5.1. Each Party shall comply with its obligations as Data Controller under applicable laws and is individually responsible for its own compliance, including fair and lawful processing of the Personal Data and safeguarding data subjects' rights.

5.2. Each Party warrants and undertakes that:

(i) it has collected and shall continue to collect and share the Personal Data in accordance with the applicable Data Protection Laws and any other legislation and regulatory requirements which apply to the respective Party relating to the use and sharing of the Personal Data;

(ii) where the legal basis for collection, use or sharing Personal Data is consent, it has obtained valid, informed, and freely given consent from the relevant data subjects, including the consent for further processing of their Personal Data by the other Party as stipulated in this Addendum;

(iii) where another legal basis applies to collection, use, or sharing and further processing of Personal Data, it has established and documented that basis in accordance with the applicable Data Protection Laws;

(iv) data subjects whose Personal Data is shared between the Parties have been provided with all required information under applicable Data Protection Laws, including information about the purposes of sharing, any rights available to data subjects, and where and how to send the data access requests;

(v) the sharing of Personal Data under this Addendum does not and will not infringe the rights or freedoms of any data subject, nor violate any applicable contractual, statutory, or regulatory restrictions;

(vi) it shall grant access to its personnel or any Third-Party, and process the Personal Data only to the extent strictly necessary for the purposes of performance of the Agreement and for the purposes set out in Schedule 1.A.(i), Schedule 1.A.(ii), Schedule 1.B and Schedule 1.C to this Addendum, as applicable, as well as for the secondary purposes that are compatible with the purposes of the relevant Personal Data processing, or for the purpose of the Onward Transfers, provided that the Onward Transfers is compliant with this Addendum;

(vii) it shall not knowingly perform its obligations under the Agreement and this Addendum in such a way as to cause the other Party to breach any of its obligations under the applicable Data Protection Laws;

(viii) it shall provide reasonable and timely assistance to help the other Party comply with its obligations under applicable Data Protection Laws, including responding to requests from data subjects exercising their rights;

(ix) it shall respond promptly to requests or complaints made by the data subjects, courts, government agencies or the supervisory authorities and provide assistance to the other Party where permitted and required;

(x) it should ensure that all persons within its personnel (including employees, workers, agents, trainees, and Third-Party Processor personnel) who access the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(xi) it shall take all necessary steps to ensure the reliability of all persons within its personnel (including employees, workers, agents, trainees and Third-Party Processor personnel) who access the Personal Data and accountability of all processing on Personal Data carried out by the persons referred to in above;

(xii) it shall notify the other Party promptly if it has any reason to believe that the legislation applicable to the notifying Party is likely to have a substantial adverse effect on the warranties and obligations set out in this Addendum or otherwise prevents it from complying with its obligations under this Addendum;

(xiii) it shall retain the Personal Data for no longer than necessary for the purpose(s) for which it has been shared, transferred and processed.

5.3. Each Party shall ensure that the shoppers are properly directed to the appropriate support channel depending on the nature of their inquiry and that the Shoppers' Personal Data is accessed and processed by each Party only to the extent necessary to fulfill their respective purposes set out in the respective Schedule 1.A(i) and Schedule 1.A(ii) .

6. PARTIES' OBLIGATIONS REGARDING THE PERSONNEL DATA

6.1. The Parties confirm that processing of the other Party's Personnel Data shall be limited to what is strictly necessary and proportionate for the purposes set out in Schedule 1.B and Schedule 1.C. of this Addendum, including performance of the Agreement, and that each Party remains subject to its obligations as a Data Controller under applicable Data Protection Laws.

6.2. The Parties confirm that Personnel Data received from the disclosing Party may be disclosed to other recipients, such as companies or internal teams within the corporate group of the receiving Party, ITC services providers, consultants, business partners, counsels, and other third parties to which disclosure of the Personnel Data is necessary for the purposes set out, respectively, in Schedule 1.B and Schedule 1.C. of this Addendum.

6.3. In accordance with the applicable Data Protection Laws, the data subjects, including but not limited to representatives, employees, co-workers, delegated personnel of each Party, have the right to access, rectify, erase, restrict, object, request the portability of their personal data, and the right to lodge a complaint before the competent supervisory authority.

6.4. Insofar as the Party receiving the Personnel Data of the other Party does not have a direct relationship with the data subjects concerned, the disclosing Party undertakes to provide those data subjects (including, but not limited to, its representatives, employees, co-workers, and delegated personnel) with the information required under applicable Data Protection Laws regarding the processing of their personal data by the receiving Party for the purposes described above. This shall be done within 5 business days following the signing of the Agreement, by providing the data subjects with an access to the relevant privacy notice made available by the receiving Party, either via the link specified in Clause 6.5 below or as otherwise communicated to the disclosing Party via email.

6.5. Information regarding the processing of the Personnel Data is available:

(i) For 2Checkout: please refer to the following: Privacy Notice; and

(ii) For Vendor: please refer to the contact details mentioned in the order form, Terms & conditions of service, etc.

7. REPRESENTATIONS OF THE VENDOR

7.1. Vendor represents and warrants that collection, processing and sharing the Personal Data does not breach any applicable Data Protection Laws, and all other legislation and regulatory requirements in force from time to time which apply to the Vendor relating to the collection, processing and deletion of Personal Data (including, without limitation, the privacy of electronic communications).

7.1. Vendor represents and warrants that by sharing, Transferring or otherwise disclosing the Personal Data to 2Checkout and by allowing 2Checkout to process Personal Data for the purposes of the performance of the Agreement, Vendor will not be in breach, and will not cause 2Checkout to be in breach of the Data Protection Laws or any other applicable laws, so that 2Checkout may lawfully use, process, and Transfer the Personal Data in accordance with the applicable law, the Agreement and this Addendum.

7.1. Vendor represents and warrants that the Personal Data shared in accordance with this Addendum is accurate, up to date (where applicable), relevant, and limited to what is necessary in relation to the purposes for which it is shared.

7.1. Vendor undertakes to consider the Vendor Products, tools, products, applications or services provided under the Agreement, the principles of privacy by design and privacy by default for Personal Data processed by the Vendor Products, tools, products, applications or services.

7.1. Vendor warrants that the Vendor Products, tools, products, applications and services provided under the Agreement comply with the principles of proportionality, minimization and limitation of Personal Data set out in the applicable Data Protection Laws.

7.1. Notwithstanding anything contained in the Agreement, Vendor understands and acknowledges that it is solely responsible for implementing and maintaining appropriate security measures for all personal data processed in systems within its control.

7.1. While the Vendor is free to determine its own data protection and privacy policies applicable to the processing of personal data by the Vendor in the context of the Agreement, the Vendor acknowledges and agrees that such policies shall comply with applicable Data Protection Laws and shall be made available to 2Checkout.

8. CROSS-BORDER DATA TRANSFERS

8.1. The Parties agree that the Transfer of Personal Data shall be carried out in compliance with the Additional Safeguards determined in accordance with the applicable Data Protection Laws and this Addendum.

8.1. Data Controller – to – Data Controller Personal Data Transfers

8.2.1. Where the Shoppers' Personal Data and 2Checkout's Personal Data is Transferred by 2Checkout (acting as the Data Controller and the Data Exporter) to the Vendor (acting as the Data Controller and the Data Importer):

(i) located outside of the EEA in a territory or sector not at that time subject to the EU Adequacy Decisions, or

(ii) which does not participate in the EU-U.S. Data Privacy Framework,

the Parties are subject to Module One of the EU SCCs, incorporated by reference under Section 8.9.

8.2.2. Where the Vendor's Personal Data or any other personal data is Transferred by the Vendor (acting as the Data Controller and the Data Exporter) to 2Checkout (acting as the Data Controller and the Data Importer) from the territory outside the United Kingdom, the EEA or the Switzerland, the Parties may agree on the Additional Safeguards ensuring that Personal Data is adequately protected and that the data subjects are granted appropriate rights, including the right to obtain effective administrative or judicial redress and to claim compensation in the event of a breach of the Addendum or the applicable safeguards to which the Parties have agreed to be bound. In such instance, Vendor shall inform 2Checkout about any legal instruments, including the Additional Safeguards, that may be required under the applicable Data Protection Laws and shall cooperate fully with 2Checkout to ensure that its processing of the Transferred Data is compliant with such Data Protection Laws.

8.3. Data Processor – to – Data Controller Personal Data Transfers

Where the Shoppers' Personal Data or any other personal data is Transferred by 2Checkout (acting as the Data Processor and the Data Exporter) to the Vendor (acting as the Data Controller and the Data Importer) located outside of:

(i) the EEA in a territory or sector not at that time subject to the EU Adequacy Decisions, or

(ii) which does not participate in the EU-U.S. Data Privacy Framework,

the Parties are subject to Module Four of the EU SCCs, incorporated by reference under Section 8.9.

8.4. Data Processor – to – Data Sub-processor Personal Data Transfers

Where the Shoppers' Personal Data or any other personal data is Transferred by 2Checkout (acting as the Data Sub-processor and the Data Exporter) to the Vendor (acting as the Data Processor and the Data Importer):

(i) located outside of the EEA in a territory or sector not at that time subject to the EU Adequacy Decisions, or

(ii) which does not participate in the EU-U.S. Data Privacy Framework,

the Parties are subject to Module Three of the EU SCCs, incorporated by reference under Section 8.9.

8.5. Where the Personal Data or any other personal data is Transferred from the territory outside the EEA or the United Kingdom, or Switzerland, the Parties may agree on any other legal instrument, including the Additional Safeguards, ensuring that Personal Data is adequately protected and that the data subjects are granted appropriate rights, including the right to obtain effective administrative or judicial redress and to claim compensation in the event of a breach of the applicable safeguards to which the parties have agreed to be bound. In such an instance, the Data Exporter shall inform the Data Importer about any legal instruments that may be required under the applicable Data Protection Laws and shall cooperate fully with the Data Importer to ensure that its processing of the Transferred Data is compliant with such applicable Data Protection Laws.

8.6. Where required under the applicable Data Protection Laws, the Parties undertake to carry out a Transfer Impact Assessment prior to transferring Personal Data to the Data Importer. If the outcome of the Transfer Impact Assessment indicates that the Supplementary Measures shall be implemented, the Parties undertake to implement them and document their implementation before the relevant Personal Data is Transferred to the Data Importer.

8.7. To the extent possible under the applicable laws, each Party agrees that in the event that the competent authority issues new international data transfer instruments replacing any of the Additional Safeguards entered into by the Parties under this Addendum, such new international data transfer instruments shall automatically apply to the Transfer of the Personal Data from the Data Exporter to the Data Importer as from the date the currently agreed and relevant Additional Safeguards are no longer valid, and shall be deemed completed on a mutatis mutandis basis to the completion of the relevant Additional Safeguards as described above.

8.8. In any event, if any applicable Data Protection Laws conflict with the provisions of this Addendum, then to the extent of such conflict:

(i) where the standard of data protection required by applicable Data Protection Laws exceeds the standard required by this Addendum, the Data Importer shall process the Transferred Data to a standard consistent with applicable Data Protection Laws; and

(ii) where the standard of data protection required by this Addendum exceeds the standard required by applicable Data Protection Laws, the Data Importer shall process the Transferred Data to a standard consistent with this Addendum.

8.9. EU Standard Contractual Clauses. Where a Transfer under this Section 8 requires the EU Standard Contractual Clauses (the "EU SCCs"), the Parties incorporate the EU SCCs by reference as if set out in full, and their execution of this Addendum constitutes execution of the applicable Module. The applicable Module is: (a) Module One (controller to controller) for Transfers by 2Checkout (as Data Controller) to the Vendor (as Data Controller) of Shoppers' Personal Data (Schedule 1.A(i)), 2Checkout's Personnel Data (Schedule 1.B) and the Vendor's Personnel Data (Schedule 1.C); (b) Module Four (processor to controller) for Transfers by 2Checkout (as Data Processor) to the Vendor (as Data Controller) of Shoppers' Personal Data (Schedule 1.A(ii)); and (c) Module Three (processor to processor) for Transfers by 2Checkout (as Data Sub-processor) to the Vendor (as Data Processor) of Shoppers' Personal Data (Schedule 1.A(ii)). For each Module: Clause 7 (docking) is not used; Clause 9(a) Option 2 applies with 30 days' notice (Modules Three and Four); Clause 11 (independent dispute-resolution body) is not selected; the competent supervisory authority (Clause 13) is the Dutch Autoriteit Persoonsgegevens; and the governing law and forum (Clause 17) are those of the Netherlands. Annex I is populated by the Schedules referenced above, Annex II by Schedules 2.A and 2.B, and Annex III by Schedules 3.A and 3.B. The authoritative text is Commission Implementing Decision (EU) 2021/914, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914.

8.10. UK and Swiss Transfers. For Transfers of UK Personal Data, the EU SCCs incorporated under Section 8.9 are supplemented by the International Data Transfer Addendum issued by the UK Information Commissioner's Office, which the Parties incorporate by reference, and references in those EU SCCs are read as modified by that Addendum. For Transfers of Swiss Personal Data, those EU SCCs apply with the adjustments required by the Swiss Federal Act on Data Protection, so that references to the GDPR, to EU Member State law and to competent supervisory authorities are read to include, as applicable, the Swiss FADP, Swiss law and the Swiss Federal Data Protection and Information Commissioner, and data subjects in Switzerland may enforce their rights in Switzerland.

9. DATA SECURITY

9.1. Each Party will implement and maintain appropriate technical and organizational security measures to ensure the appropriate protection, confidentiality and security of the shared Personal Data, as described in Schedule 2.A. regarding the minimum technical and organizational security measures attached to this Addendum.

9.2. The Vendor expressly agrees to fully comply with all requirements defined and communicated by 2Checkout for the use of the Platform and Dashboard. This includes access control requirements, authentication protocols, system usage guidelines, and any additional data protection safeguards mandated by Verifone to ensure secure and compliant use of its systems. These requirements are reflected in: Verifone's Website Use Terms.

9.3. Both Parties undertake to implement and maintain appropriate technical and organizational security measures designed to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage to personal data or other confidential information exchanged or processed under this Agreement. The Parties acknowledge and agree that any security measures described or referenced in this Addendum represent a minimum baseline and shall not be construed as exhaustive or limiting. Each Party shall continuously monitor, maintain, and update its respective security measures in line with (i) technological developments, (ii) emerging threats, (iii) industry best practices and (iv) applicable regulatory standards (including, where applicable, ISO/IEC 27001, NIST, ENISA, or similar). Each Party shall carry out regular checks to ensure that these measures continue to provide an appropriate level of the Personal Data security.

10. DATA BREACH

In the event of a Data Breach, the Party experiencing the Data Breach will:

(i) notify the Data Breach to the other Party in the most expedient time possible under the circumstances and without undue delay but in no event later than within 48 hours after becoming aware of the Data Breach, by writing at the e-mail addresses provided in this Addendum or at any other address, as may be agreed between the Parties. The Vendor further agrees that 2Checkout shall be notified of all Data Breaches exclusively through the following online notification form available on www.verifone.com – Report Security Incident.

(ii) if required by the applicable Data Protection Laws, notify the relevant supervisory authority and/or the data subjects concerned about the Data Breach within the mandatory deadlines, in the form required by the applicable Data Protection Laws, and, if necessary, in cooperation with the other Party;

(iii) provide the other Party, in a timely manner and as soon as such information can be collected or otherwise becomes available, with a detailed description of the Data Breach, including (a) a description of the nature of the Data Breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), (b) a description of the likely consequences of the Data Breach, (c) the measures taken or proposed to address and mitigate the possible adverse effect of the Data Breach, and (d) the details of a contact point from whom more information can be obtained ;

(iv) provide commercially reasonable cooperation as the other Party may require for it to fulfill its reporting obligations under the applicable Data Protection Laws or any other applicable laws. Where, and insofar as it is not possible to provide all this information at the same time, the initial notification shall contain the information then available, and the notifying Party shall provide further or supplementary information as soon as it becomes available;

(v) act immediately to investigate the Data Breach and to identify, prevent and make reasonable efforts to mitigate the effects of the Data Breach; and

(vi) not release or publish any filing, communication, notice, press release, or report concerning any Data Breach without the other Party's prior approval, except where and to the extent required by the applicable Data Protection Laws.

11. CONFIDENTIALITY AND NOTIFICATIONS

11.1. Each Party will maintain the confidentiality of the shared Personal Data and will not disclose the Personal Data to third parties unless the other Party or the Addendum or any other agreement that may be executed between Vendor and 2Checkout authorizes the disclosure, or as required by domestic law, court or regulator (including the supervisory authority).

11.2. Unless strictly prohibited by applicable law, each Party shall promptly inform the other Party, and in any event within five (5) business days, of any inquiry, communication, request, or complaint received from (i) any governmental, regulatory, or supervisory authority, including any data protection authority; or (ii) any data subject, relating to data processing, any Personal Data, or any obligations under applicable Data Protection Laws.

11.3. Unless strictly prohibited by applicable law, each Party shall promptly inform the other Party, and in any event within five (5) business days, if it becomes aware of any direct access by public authorities to the Personal Data.

11.4. Notifications shall include all information available to the notifying Party and each Party shall provide reasonable assistance to the other Party to enable it to respond to or challenge such access to the relevant Personal Data

11.5. If the Party is prohibited from providing notifications pursuant to Clause 11.2. or Clause 11.3. of this Addendum under the applicable laws, the Party shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Party agrees to document its best efforts in order to be able to demonstrate them on request of the other Party.

11.6. If a domestic law, court, or regulator (including the supervisory authority) requires the Party to process or disclose the Personal Data to a Third-Party, such Party must first inform the other Party of such legal or regulatory requirement and give that Party an opportunity to object or challenge the requirement, unless the applicable law prohibits the giving of such notice.

12. LIABILITY LIMITATIONS

To the extent permitted by applicable laws, limitations of remedies and damages liability set out in the Agreement apply to all claims related or made pursuant to any breach of the terms of this Addendum.

13. COMMENCEMENT AND TERMINATION

13.1 This Addendum will commence on the Effective Date indicated in the Agreement and will continue in full force and effect until the Agreement remains in effect or until either Party retains any of the Personal Data related to the Addendum in its possession or control.

13.2. Any Party may suspend the processing of the Personal Data, if it has reason to believe that the legislation applicable to it or to the other Party is likely to have a substantial adverse effect on the warranties and obligations set out in this Addendum or otherwise prevents the relevant Party from complying with its obligations under this Addendum. In such case, the Parties shall negotiate in good faith the measures, remedies and corrections necessary to restore the processing of Personal Data in compliance with this Addendum.

13.3. This Addendum shall automatically terminate with respect to the Personal Data processed for the purposes of the relevant Services upon the termination of the Agreement, any Work Order, Statement of Work (SOW), or any part thereof, to the extent such termination relates to the processing of that Personal Data for the specified Services.

13.4. Each Party shall have the right to terminate this Addendum or the part thereof if case of any of the following:

(i) the processing of Personal Data has been suspended, provided that the compliance with this Addendum is not restored within a reasonable time and in any event within one month following suspension;

(ii) the other Party is in substantial or persistent breach of this Addendum or its obligations under the applicable Data Protection Laws;

(iii) the other Party fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Addendum.

13.5. Termination of this Addendum or any of its Attachments shall result in the termination of the Agreement to the extent that its further performance is either impossible or would impose significantly higher costs on any of the Parties, and provided that the Parties have not, within a reasonable time, reached a mutually satisfactory agreement on measures, remedies, or corrections to the processing of the Personal Data necessary to ensure compliance with this Addendum or the applicable Data Protection Laws.

13.6. Any provision of this Addendum that expressly or by implication should come into or continue in force on or after termination of the Agreement to protect the Personal Data will remain in full force and effect.

14. TECHNOLOGY EVOLUTION

The Vendor agrees that 2Checkout may introduce, modify, replace or discontinue technologies, tools, systems or functionality, including artificial intelligence, automation or similar technologies, as part of the ongoing development, operation, security, compliance, support and improvement of the Services, provided that such changes are made in accordance with applicable laws and do not materially reduce the functionality of the Services purchased by the Vendor. Such changes shall not, by themselves, affect the Parties' respective privacy roles or require amendment of this Agreement. Nothing in this Agreement shall be construed as restricting 2Checkout from using artificial intelligence or other automated technologies in connection with the Services, provided that such use complies with applicable laws, this Agreement and 2Checkout's applicable governance, security and compliance requirements.

15. TRANSITION REQUIREMENTS

15.1. Upon termination or expiry of the Agreement, 2Checkout may, acting in its sole reasonable discretion and subject to applicable law, payment industry rules, technical feasibility and this Section, share with any third-party merchant of record provider or other payment service provider designated in writing by the Vendor ("New Provider") only such Payment Information as 2Checkout determines may lawfully, contractually and technically be disclosed, subject to a separate Data Transfer Agreement where required.

15.2. All Payment Information and Shopper Personal Data processed by 2Checkout in its capacity as Merchant of Record are collected, determined and controlled by 2Checkout in accordance with the applicable Data Protection Laws. Nothing in this Addendum creates any right to data transition, migration, portability, business continuity, service continuity or transfer, nor any obligation on 2Checkout to support subscription migration or continuity following termination of the Agreement. Any approved sharing of Payment Information shall be exceptional, discretionary, limited to the specific request approved by 2Checkout in writing, and shall not constitute a waiver of, or create any precedent regarding, 2Checkout's rights or obligations.

15.3. Nothing in the Agreement obliges 2Checkout to transfer recurring payment credentials, payment tokens or subscription credentials where such transition is not supported or permitted by the applicable payment card scheme, token service provider, acquiring bank, payment processor or applicable law.

15.4. Any approved transition of Payment Information is subject to the following conditions:

(i) The Vendor shall demonstrate a valid legal basis for the proposed sharing under applicable data protection, privacy and other applicable laws, including, where required, providing appropriate notices and obtaining valid consent. Where the relevant Shopper has already entered into a contract with the New Provider, the Vendor will provide evidence of such contract. 2Checkout may refuse any request, acting in its sole reasonable discretion, where satisfactory evidence is not provided. Any sharing shall be limited to the minimum amount of Personal Data reasonably necessary for the approved purpose.

(ii) The Vendor acknowledges that payment processing and subscription management are performed by 2Checkout as Merchant of Record and that payment and subscription data remain under 2Checkout's control. 2Checkout makes no representation or warranty regarding the availability, completeness, accuracy, compatibility, continued validity, technical suitability or ability of any Payment Information to enable the migration of subscriptions or recurring payment arrangements.

(iii) The Vendor shall ensure that its customer-facing terms, privacy notices and other required disclosures accurately inform Shoppers that any sharing of Payment Information may occur only in limited circumstances where legally and technically permitted and shall not represent or imply that payment credentials, subscriptions or payment data will be migrated or transferred as a matter of right. Consent, where relied upon, does not override applicable law, payment card scheme rules, acquiring bank requirements, regulatory restrictions or data localization requirements.

(iv) Where the proposed sharing involves an international transfer of Personal Data, the Vendor should ensure that appropriate transfer safeguards are implemented in accordance with applicable law. Where legally required and approved by 2Checkout, such safeguards may include the execution of the EU Standard Contractual Clauses (controller-to-controller) or other legally recognized transfer mechanisms. Consent alone shall not constitute a valid transfer mechanism where prohibited or restricted by applicable law or payment industry rules.

(v) If the New Provider refuses, fails or is unable to execute any required Data Transfer Agreement or other legally required contractual safeguard, no sharing of Payment Information shall take place. In such case, 2Checkout shall have no obligation to facilitate the transition and shall incur no liability arising from its refusal to share Payment Information.

(vi) The Vendor remains solely responsible for selecting, onboarding and ensuring the compliance of the New Provider with all applicable data protection, privacy, security, financial services and regulatory requirements. The Vendor shall ensure that equivalent contractual obligations are imposed on the New Provider and shall indemnify and hold harmless

2Checkout against all claims, losses, damages, liabilities, regulatory actions, fines, penalties, costs and expenses arising from the Vendor's request to share Payment Information or any act or omission of the Vendor or the New Provider, except to the extent caused by 2Checkout's own breach of this Agreement or applicable law.

(vii) The New Provider shall maintain appropriate technical and organizational security measures and hold all certifications, authorizations, licenses and approvals required under applicable law to receive the Payment Information, including, where applicable, PCI DSS certification (or any successor payment security standard) and any required financial services or payment services authorizations. The Vendor shall provide reasonable evidence of such compliance upon request. PCI DSS certification or regulatory authorization alone shall not entitle the Vendor to any transfer of Payment Information. 2Checkout may refuse any request where compliance, regulatory alignment, payment industry requirements or technical feasibility are not adequately demonstrated.

15.5. The Vendor shall reimburse 2Checkout for all reasonable costs and expenses incurred in connection with any approved sharing of Payment Information. Such costs shall be charged on a time and materials basis, with rates and estimated costs agreed in writing before any transition activities commence.

15.6. 2Checkout shall not be required to share Payment Information were doing so would breach applicable law, Data Protection Laws, the EU Data Act (where applicable), financial services legislation, payment card scheme rules, acquiring bank requirements, PCI DSS, contractual obligations or technical limitations. Acting in its sole reasonable discretion, 2Checkout may refuse any request where it reasonably determines that the proposed sharing would expose it to legal, contractual, regulatory or operational risk. No refusal to share Payment Information shall give rise to any liability. Nothing in this Section require 2Checkout to disclose information subject to legal privilege, regulatory confidentiality, supervisory confidentiality, anti-money laundering confidentiality, sanctions-related confidentiality, bank secrecy obligations or any other statutory or contractual restriction on disclosure.

16. VENDOR TRANSPARENCY OBLIGATIONS

16.1. Where the Vendor Products or Vendor Services involve the processing of personal data and information, including through the use of artificial intelligence systems or models, automated decision-making, profiling, cookies, SDKs, pixels, tags, scripts, or other tracking or similar technologies, the Vendor shall comply with all applicable data protection, privacy, and electronic communications laws (including, where applicable, laws governing cookies and similar tracking technologies) and shall ensure that complete, accurate, up-to-date, and legally compliant privacy notices, cookie notices, user-facing disclosures, and any other required transparency information are made available to data subjects prior to or at the time of processing, and are reviewed and updated as necessary.

16.2. The Vendor further acknowledges that such transparency and compliance obligations apply irrespective of whether any relevant technology, tool, system, software, artificial intelligence model, or tracking mechanism is developed by the Vendor, provided by 2Checkout, or sourced from a third party. The Vendor acknowledges and agrees that it is solely responsible for ensuring that its privacy notices, cookie banners and preference mechanisms, and disclosures meet all applicable legal requirements, including transparency, information duties, lawful consent or opt-out mechanisms where required, and data subject rights, and for the content, accuracy, and legal sufficiency of such notices and disclosures.

16.3. Nothing in this Addendum or Agreement shall be construed as requiring 2Checkout to draft, review, approve, monitor, or validate the Vendor’s privacy notices, cookie notices, consent management tools, risk assessments, or transparency determinations, or to assume any obligations or liability under applicable privacy or data protection laws, e-privacy or electronic communications laws, nor as creating any joint controllership, joint determination of purposes or means, or shared transparency obligations between the parties.

17. MISCELLANEOUS

17.1. This Addendum, including the EU Standard Contractual Clauses referenced or attached hereto, the attached Schedules, and any subsequent Annexures constitute the entire agreement between the Parties pertaining to the subject matter of this Addendum and supersedes all prior agreements, understandings, negotiations, representations, and warranties, whether written or oral, relating to such subject matter.

17.2. No failure or delay by either Party in exercising any right, power, or privilege under this Addendum shall operate as a waiver thereof, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise thereof or the exercise of any other right, power, or privilege.

Appendices:
Schedule 1.A.(i) - description of the Shoppers' Personal Data shared on the Data Controller – to – Data Controller basis;
Schedule 1.A.(ii) - description of the Shoppers' Personal Data shared on the Data Controller – to – Data Processor basis;
Schedule 1.B - description of 2Checkout's Personnel Data;
Schedule 1.C - description of the Vendor's Personnel Data;
Schedule 2.A. - Security Measures;
Schedule 2.B. – Supplementary Security Measures;
Schedule 3.A. – A list of 2Checkout's Sub-processors;
Schedule 3.B. – A list of Vendor's Sub-processors;
Attachment 1 - Data Processing Agreement;

SCHEDULE 1.A (i)

SHOPPERS' PERSONAL DATA
DATA CONTROLLER-TO-DATA CONTROLLER

Categories of data subjects whose personal data is shared with

Shoppers, i.e., individuals acting in their own name or on behalf of legal entities, purchasing Vendor's Products, which include any assets, goods, or services sold by the Vendor through the digital commerce site. Vendor Products encompass (i) programs, code, information, or data stored in a digital format, along with their accompanying documentation, activation and reloading electronic codes, as well as subscriptions to hosted, online, software-as-a-service (SaaS), or similar services and (ii) providing technical and product-related support to Shoppers, such as inquiries concerning access to the product or service, usability, technical malfunctions, configuration, installation, feature-related question.

Categories of the Shoppers' Data:

a) Identification data: name/surname, age where the applicable law imposes an age limit.
b) Contact details: e-mail address, phone number, billing/shipping address.
c) Transaction and financial data: such as location, purchase amount, date of purchase, information about the purchased items, past purchases, (auto)renewal, chargeback, and refunds.
d) Any other data provided: in connection with technical support and/or the Vendor's Product related complaints or requests data, such as details of the complaint and/or request filed with 2Checkout and any supporting documentation or evidence relevant to the complaint and/or request, such as identification data, emails, screenshots, photographs, witness statements, etc.

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

N/A

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

On continuous basis.

Nature of the processing

Collection, use, sharing, transferring, access, segmentation, structuring, communication delivery, reporting, anonymization/pseudonymization, storage, retention and deletion, recording and registration, consultation, alignment/combination, restriction, recovery.

Purpose(s) of the data sharing and further processing

a) generation and delivery of all invoices, receipts, and tax documents related to shopper purchases, including both one-time transactions and subscription-based billing.
b) recording and staff training such of support interactions, meetings, or training sessions for the purposes of service quality assurance, internal training, performance evaluation.
c) survey management and feedback analysis through satisfaction surveys, feedback forms, or service evaluations.
d) respond to support inquiries and communicate technical or service-related information to the shopper.
e) enabling delivery of the purchased Vendor Products, provide relevant product information, or troubleshoot related technical issues.
f) resolving the Vendor Products usability issues, respond to complaints, provide troubleshooting, and improve the quality of service or product/service offered.
g) personalize support interactions and facilitate the Vendor Products delivery or technical troubleshooting.
h) responding to shoppers' requests concerning Vendor Products' functionality or performance, and to maintain service continuity and support traceability.
i) analyzing complaints or product-specific queries, improve service delivery, and resolve technical support cases based on evidence provided by the shopper (e.g. screenshots, logs).any other processing activities to ensure the continuity, stability, and resilience of the Vendor Products provided to the shopper, in the event of operational disruptions, system failures, natural disasters, cybersecurity incidents, or other unforeseen circumstances that could impact its delivery.
j) ensuring compliance with the Party's security, regulatory and legal obligations, for example, to comply with applicable laws related to anti-money laundering, anti-corruption, export controls, tax obligations, and similar regulations;
k) pursuing the legitimate interest of the Party receiving the data or a Third-Party, including, but not limited to, the establishment, exercise, or defense of its legal rights.

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

The Shoppers' Personal Data will be retained for the period necessary to fulfill the purposes for which it was received, as required by applicable laws and regulations, or as necessary to comply with contractual obligations. The retention period for the Shoppers' Personal Data shall be determined based on the following criteria:

a) duration of the contractual relationship between the Parties;
b) legal and regulatory requirements applicable to data retention;
c) carrying out audits, or defend or pursuit legal claims.

Upon the expiration of the retention period or upon request from the data subject (where applicable), the Party receiving the Shoppers' Data will securely delete or anonymize them, unless further retention is legally required.

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

Please refer to Schedule 3.A. and Schedule 3.B. of this Addendum.

SCHEDULE 1.A (ii)

SHOPPERS' PERSONAL DATA
DATA PROCESSOR -TO-DATA CONTROLLER

Categories of data subjects whose personal data is shared with

Shoppers, i.e., individuals acting in their own name or on behalf of legal entities, purchasing Vendor Products, which include any assets, goods, or services sold by the Vendor through its digital commerce site. Vendor Products encompass programs, code, information, or data stored in a digital format, along with their accompanying documentation, activation and reloading electronic codes, as well as subscriptions to hosted, online, software-as-a-service (SaaS), or similar services.

Categories of the Shoppers' Data:

a) Identification data: name/surname, proxy data (including any associated legal documentation or authorization).
b) Contact details: e-mail address, phone number, billing/shipping address.
c) Transaction and financial data: such as location, purchase amount, date of purchase, information about the purchased items, past purchases and orders numbers.
d) Computer data collected during the checkout process: such as the IP address, browser type, device type, timestamps, operating system, logs activity and reports, mobile device identifier, and geographical location.
e) Communication data: and, in particular, information collected through various forms of interaction, including support tickets, emails correspondences, and social media engagements and any personal data posted on forums and discussion groups (in line with legal restrictions).
f) Marketing data: and, in particular such as demographic information, purchase history, and engagement metrics across websites, emails and social media platforms, capturing insights into customer interactions, preferences, and responses to our content, social media commentary, customer feedback through surveys and support tickets, and visual or textual content shared by users.
g) Usage of website(s) & platforms: and, in particular information related to usage by the shoppers information such as the type of device used, including its, unique device identifiers, IP address, operating system version, device settings, location, log data detailing the time and duration of website's visits, search data, and cookie-stored information that uniquely identifies the browser or account.
h) Audio-visual data: where applicable and legally permissible, processing of (i) phone or video calls or chats with 2Checkout sales or customer care agents, (ii) recordings of business meetings and training sessions (e.g., screen recording, remote access).
i) Any other data provided to 2Checkout: for example in connection with complaints or requests data, such as details of the complaint and/or request and any supporting documentation or evidence relevant to the complaint and/or request, such as identification data, emails, screenshots, photographs, witness statements, proxy etc.

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

N/A

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

On continuous basis.

Nature of the processing

2Checkout will process the Shoppers Personal Data as necessary to provide the Vendor-Requested Services in accordance with the relevant Work Order(s) or Statement of Work(s), including the following: collection, use, sharing, transferring, access, segmentation, structuring, communication delivery, reporting, anonymization/pseudonymization, storage, retention and deletion, recording and registration, consultation, alignment/combination, restriction, recovery, preference management and engagement tracking, real-time analysis, insight generation.

Purpose(s) of the data sharing and further processing

1. Providing the Vendor-Requested Services under the relevant Work Order(s) or Statement of Work(s), including as follows:

a) Shoppers marketing activities, such as direct and personalized marketing activities aimed at promoting products, services, or offers that may be of interest to shoppers based on their interactions with the Vendors' platforms/websites/apps or their prior purchasing behavior. This includes sending commercial communications via email, optimizing advertising delivery, conducting engagement-based segmentation, and inviting users to participate in surveys or promotional campaigns – strictly in accordance with consent requirements under applicable law.
b) Shoppers' experience customization, such as personalize and enhance the shopper's online experience across checkout interfaces and post-purchase flows by adjusting language, layout, messaging, field requirements, and content delivery based on the shopper's geographic location, device type, interaction history, or known preferences. This includes tailoring

upsell or cross-sell messages, interface elements, or recommendations in a way that improves usability and increases relevance for the shopper.

c) Analytics and optimization, such as analyzing shoppers' use of websites, shopping carts, and checkout processes in order to understand behavior patterns, identify technical issues, and evaluate the effectiveness of platform features and marketing campaigns.

d) survey management and feedback analysis through satisfaction surveys, feedback forms, or service evaluations.

2. Ensuring compliance with the Party's security, regulatory and legal obligations, for example, to comply with applicable laws related to anti-money laundering, anti-corruption, export controls, tax obligations, and similar regulations.

3. Pursuing the legitimate interest of the Party receiving the data or a Third-Party, including, but not limited to, the establishment, exercise, or defense of its legal rights

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

The Shoppers' Personal Data will be retained for the period necessary to fulfill the purposes for which it was received, as required by applicable laws and regulations, or as necessary to comply with contractual obligations. The retention period for the Shoppers' Personal Data shall be determined based on the following criteria:

a) performing the Vendor-Requested Services under the Agreement, in particular under the relevant Work Order(s) or the Statement of Work(s);

b) legal and regulatory requirements of EU (or any EU Member State) or any Swiss or any UK law, or PCI-DSS, to retain some or all of the Personal Data, in which event 2Checkout shall isolate and protect the Personal Data from any further processing except to the extent permitted by such law;

c) carrying out audits, or defend or pursuit legal claims.

Upon the expiration of the retention period or upon request from the data subject (where applicable), the Party receiving the Shoppers' Data will securely delete or anonymize them, unless further retention is legally required.

For sharing with (sub-) processors, also specify subject matter, nature and duration of the processing: Please refer to Schedule 3.A. and Schedule 3.B. of this Addendum.

SCHEDULE 1.B

2CHECKOUT'S PERSONNEL DATA
DATA CONTROLLER-TO-DATA CONTROLLER

Categories of data subjects whose personal data is shared with

Representatives, employees, co-workers, delegated personnel of 2Checkout whose contact personal data are shared with Vendor to manage the business and contractual relationship between the Parties and ensure security, compliance, and legal obligations of the Parties, including but without limiting to:

a) employees: individuals who are formally engaged under an employment contract, regardless of their classification as full-time, part-time, fixed-term, temporary, or permanent staff. This includes, without limitation, administrators, managers, directors, board members, team leaders, interns, and contingent or agency staff integrated into each company organizational structure.
b) workers and authorized personnel: individuals who provide services to each company outside of an employment contract framework. This category includes independent contractors, consultants, and individuals engaged through project-based arrangements, temporary assignments, or service agreements.

Categories of personal data shared

a) name/surname;
b) business e-mail address;
c) business telephone number;
d) function /title;
e) employer's or business partner name
f) department.

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

N/A

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

On continuous basis.

Nature of the processing

Collection, use, sharing, transferring, access, reporting, storage, retention and deletion,

Purpose(s) of the data sharing and further processing:

a) survey management and feedback analysis through the collection and evaluation of satisfaction surveys, feedback forms, and service-related evaluations, for the purpose of improving user experience, service delivery, and customer engagement.
b) management of the business and contractual relationship between the Parties, including coordination, communication, compliance, and administrative responsibilities necessary for the effective execution of the Agreement.
c) processing of comments, inquiries, suggestions, or feedback provided by the Vendor or its representatives in connection with the performance or improvement of the Agreement and related services.
d) operational enablement of services, including account setup, user authentication, role-based access control, platform usage monitoring, customer support delivery, contractual execution, service personalization, internal administration, platform communication, quality assurance activities, and audit and compliance monitoring. This ensures the secure, compliant, and efficient provision of services throughout the term of the Agreement.
e) any other processing activities to ensure the continuity, stability, and resilience of services provided under the Agreement, in the event of operational disruptions, system failures, natural disasters, cybersecurity incidents, or other unforeseen circumstances that could impact service delivery.
f) where applicable and legally permissible recordings of business meetings and training sessions (e.g., screen recording, remote access).
g) ensuring compliance with the Party's security and legal obligations, for example, to comply with applicable laws related to anti-money laundering, anti-corruption, export controls, counter-terrorism financing (CTF), and sanctions compliance, tax obligations, and similar regulations;
h) pursuing the legitimate interest of the Party receiving the data or a Third-Party, including, but not limited to, the establishment, exercise, or defense of its legal rights.
i) internal reporting and corporate governance purposes, including the preparation and transmission of contractual performance reports, financial summaries, and operational updates to the Vendor's parent company or group entities/affiliates.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
2Checkout's Personal Data will be retained for the period necessary to fulfill the purposes for which it was received, as required by applicable laws and regulations, or as necessary to comply with contractual obligations. The retention period for 2Checkout's Personal Data shall be determined based on the following criteria:

a) duration of the contractual relationship between the Parties;
b) legal and regulatory requirements applicable to data retention;
c) carrying out audits, or defend or pursuit legal claims.

Upon the expiration of the retention period or upon request from the data subject (where applicable), the Party receiving the 2Checkout's Personnel will securely delete or anonymize them, unless further retention is legally required.
For sharing with (sub-) processors, also specify subject matter, nature and duration of the processing, please refer to Schedule 3.A. and Schedule 3.B. of this Addendum.

SCHEDULE 1.C

VENDOR'S PERSONNEL DATA
DATA CONTROLLER-TO-DATA CONTROLLER

Categories of data subjects whose personal data is shared

Representatives, employees, co-workers, delegated personnel of the Vendor whose contact personal data are shared with 2Checkout to manage the business and contractual relationship between the Parties and ensure security, compliance, and legal obligations of the Parties, including but without limiting to:

a) employees: individuals who are formally engaged under an employment contract, regardless of their classification as full-time, part-time, fixed-term, temporary, or permanent staff. This includes, without limitation, administrators, managers, directors, board members, team leaders, interns, and contingent or agency staff integrated into each company organizational structure.
b) workers and authorized personnel: individuals who provide services to each company outside of an employment contract framework. This category includes independent contractors, consultants, and individuals engaged through project-based arrangements, temporary assignments, or service agreements.

Categories of personal data shared

1. Personal data relating to the Vendor's authorized personnel (as nominated by the Vendor) who access and use 2Checkout's Services and Vendor-Requested Services. This processing supports the full use of 2Checkout's service offerings and the management of the contractual relationship between the Parties. Such services include contract management and platform operations. The Vendor's Personnel Data is processed for purposes including user authentication, role-based access control, activity logging, support communications, and administrative actions performed within the 2Checkout platform environment. This may include, but is not limited to, the following categories of personal data:

a) identification data: name/surname, access credentials and access role type.
b) contact details: e-mail address, phone number.
c) computer data collected during the checkout process such as the IP address, browser type, device type, timestamps, operating system, logs activity and reports, mobile device identifier, and geographical location.
d) usage of website(s) & platforms: and, in particular information related digital usage, such as the type of device, including its, unique device identifiers, IP address, operating system version, device settings, location, log data detailing the time and duration website visits, search data, and cookie-stored information that uniquely identifies browser or account.
e) communication data and information we collect through various forms of interaction including support tickets, emails correspondences, and social media engagements and interactions, registering for, attend, or participating in industry events, and any personal data posted on forums and discussion groups (in line with legal restrictions).
f) audio-visual data: where applicable and legally permissible (i) phone or video calls or chats with sales or customer care agents, (ii) recordings of business meetings and training sessions (e.g., screen recording, remote access).
g) any other data provided to 2Checkout: for example, in connection with complaints or requests data, such as details of the complaint and/or request and any supporting documentation or evidence relevant to the complaint and/or request, testimonials/interviews regarding 2Checkout's products/services/support etc., such as identification data, emails, screenshots, photographs, witness statements, etc. Verifone does not exert control over the quantity or quality of the data shared.

2. Personal data relating to the Vendor's business and legal representative: the use of 2Checkout's Services and Vendor-Requested Services is subject to regulatory requirements, including a mandatory underwriting and onboarding process conducted within 2Checkout's systems and platforms. This process is a legal obligation imposed by applicable financial and compliance regulations and constitutes an ongoing duty for 2Checkout throughout the duration of the contractual relationship. Accordingly, the Vendor is required to provide 2Checkout with the following personal and business-related information for the purposes of regulatory compliance, risk assessment, and account verification, for the entire duration of the Agreement:

a) Identification data: name/surname, date and place of birth, ID number, title/position/role, nationality and a specimen signature, fiscal code/social security number, proxy data (including any associated legal documentation or authorization), access credentials and access role type.
b) Know our customer data as part of customer due diligence: such as business information, ownership, and control information, identity information, including ID, financial data, information required for Know Your Customer (KYC) obligations, utility bills, credit, litigations and financial history, to prevent fraudulent conduct or behavior that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud.
c) Underwriting data: business information, ownership, and control information, identity information, including ID, financial data, information required for Know Your Customer (KYC) obligations, utility bills, credit, litigations and financial history, full name of the business owner, date of birth of the Vendor/business owner, physical address, e-mail address, phone number, SSN (social security number) or TIN (taxpayer identification number), bank information (bank name, account number, routing

number), business registration details (legal name, commercial name, registration number, date and place of registration), website URL. This process might also include both processing of special categories of Personal data, namely information on criminal convictions and offenses and politically exposed persons.

d) Any other data provided to 2Checkout: for example, in connection with complaints or requests data, such as details of the complaint and/or request and any supporting documentation or evidence relevant to the complaint and/or request, testimonials/interviews regarding 2Checkout's products/services/support etc., such as identification data, emails, screenshots, photographs, witness statements, etc.

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

information on criminal convictions and offenses and politically exposed persons.

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

On continuous basis.

Nature of the processing

Collection, use, sharing, transferring, access, segmentation, structuring, communication delivery, reporting, anonymization/pseudonymization, storage, retention and deletion, recording and registration, consultation, alignment/combination, monitoring, restriction, recovery.

Purpose(s) of the data sharing and further processing:

1. Related to personal data of the Vendor's authorized personnel (as nominated by the Vendor):

a) performance of the Agreement related to the provision of Services and Vendor-Requested Services , including all activities necessary to fulfill contractual obligations between the Parties.

b) survey management and feedback analysis through the collection and evaluation of satisfaction surveys, feedback forms, and service-related evaluations, for the purpose of improving user experience, service delivery, and customer engagement.

c) management of the business and contractual relationship between the Parties, including coordination, communication, compliance, and administrative responsibilities necessary for the effective execution of the Agreement.

d) processing of comments, inquiries, suggestions, or feedback provided by the Vendor or its representatives in connection with the performance or improvement of the Agreement and related services.

e) operational enablement of services, including account setup, user authentication, role-based access control, platform usage monitoring, customer support delivery, contractual execution, service personalization, internal administration, platform communication, quality assurance activities, and audit and compliance monitoring. This ensures the secure, compliant, and efficient provision of services throughout the term of the Agreement.

f) any other processing activities to ensure the continuity, stability, and resilience of services provided under the Agreement, in the event of operational disruptions, system failures, natural disasters, cybersecurity incidents, or other unforeseen circumstances that could impact service delivery of the Agreement;

g) ensuring compliance with the Party's security and legal obligations, for example, to comply with applicable laws related to anti-money laundering, anti-corruption, export controls, tax obligations, and similar regulations;

h) pursuing the legitimate interest of the Party receiving the data or a Third-Party, including, but not limited to, the establishment, exercise, or defense of its legal rights.

2. Related to Vendor's business and legal representative:

a) general purpose of fulfilling regulatory obligations related to onboarding, underwriting, identity verification, and financial due diligence, in line with applicable laws on anti-money laundering (AML), counter-terrorism financing (CTF), and sanctions compliance.

b) performance of the contractual relationship, including the establishment and management of the account, validation of business identity, financial reconciliation, invoicing, payouts, and compliance with accounting and tax obligations.

c) internal reporting and corporate governance purposes, including the preparation and transmission of contractual performance reports, financial summaries, and operational updates to the 2Checkout's parent company or group entities.

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

Vendor's Personnel Data will be retained for the period necessary to fulfill the purposes for which it was received, as required by applicable laws and regulations, or as necessary to comply with contractual obligations. The retention period for the Vendor's Personnel Data shall be determined based on the following criteria:

a) duration of the contractual relationship between the Parties;

b) legal and regulatory requirements applicable to data retention;

c) carrying out audits, or defend or pursuit legal claims.

Upon the expiration of the retention period or upon request from the data subject (where applicable), the Party receiving the Vendor's Personnel Data will securely delete or anonymize them, unless further retention is legally required

For sharing with (sub-) processors, also specify subject matter, nature and duration of the processing: please refer to Schedule 3.A. and Schedule 3.B. of this Addendum.

SCHEDULE 2.A.

SECURITY MEASURES

Upon the written request of the other Party, each Party may provide reasonable information regarding its technical and organizational measures, security controls, security certifications, attestations of compliance (including, where applicable, PCI DSS Attestations of Compliance - AoC), audit reports or other security documentation reasonably required for the requesting Party's compliance, risk assessment or due diligence activities.

Such information shall be provided only where the requesting Party is bound by the confidentiality obligations contained in the Agreement or a separate non-disclosure agreement ("NDA") acceptable to the disclosing Party.

The disclosing Party may redact, limit or refuse the disclosure of any information where it reasonably determines that such disclosure would compromise the security, confidentiality or integrity of its systems, reveal proprietary or confidential information, or conflict with applicable law, regulatory obligations, contractual commitments or industry security requirements.

SCHEDULE 2.B.

SUPPLEMENTARY SECURITY MEASURES

The security measures and disclosure conditions set out in Schedule 2.A apply equally under this Schedule 2.B (Supplementary Security Measures).

SCHEDULE 3.A.

LIST OF THE APPROVED SUB-PROCESSORS OF 2CHECKOUT

Upon the written request of the other Party, each Party may provide information regarding its Processors and Sub-processors, including their identity, location and the processing activities performed on its behalf, to the extent reasonably necessary for the requesting Party's compliance, risk assessment or due diligence activities and subject to applicable Data Protection Laws.
Such information shall be provided only where the requesting Party is bound by the confidentiality obligations contained in this Agreement or a separate non-disclosure agreement ("NDA") acceptable to the disclosing Party.
Nothing in this Agreement shall require either Party to disclose information that is subject to legal privilege, confidentiality obligations owed to third parties, trade secret protection, regulatory restrictions or other applicable legal or contractual limitations.

SCHEDULE 3.B.

LIST OF THE APPROVED SUB-PROCESSORS OF VENDOR

The disclosure provisions set out in Schedule 3.A apply equally to the Vendor's Processors and Sub-processors listed above.

ATTACHMENT 1

DATA PROCESSING AGREEMENT
(DATA CONTROLLER-TO-DATA PROCESSOR)
(UK & EEA & Switzerland)

This Data Processing Agreement is entered into by and between the Parties, who agree as follows:

A. Additional definitions and interpretations

This Data Processing Agreement forms part of the Data Sharing Addendum and should be read in conjunction with it.
The interpretations and defined terms set forth in the Data Sharing Addendum shall apply to this Data Processing Agreement.
Any reference in this Data Processing Agreement to the Appendices, including any Schedules, Attachments, or Annexes that form part of the Addendum shall be deemed to be incorporated herein and have full effect as if set out in this Agreement.
Article 28(3) GDPR. The Parties agree that the obligations set out in this Data Processing Agreement, including those on processing under documented instructions, confidentiality, security, engagement of Sub-processors, assistance with data-subject requests and data protection impact assessments, deletion or return of Personal Data, and audits and inspections are intended to and do satisfy the matters required to be addressed by Article 28(3) of the GDPR.

B. Description of the Personal Data processing

A description of the nature and purposes of the processing, the types of Personal Data, categories of data subjects, the purpose of the Personal Data processing, and the duration of the processing that 2Checkout may carry out on behalf of the Vendor are set out in Schedule 1.A(ii).

C. Obligations of the Parties

Instructions for 2Checkout

(i) 2Checkout shall process the Personal Data only in accordance with Vendor's lawful and documented instructions;

(ii) The Parties agree that the provision of the Vendor-Requested Services under the Agreement (including any Order Forms and Statements of Work entered into under the Agreement), or under any other agreement executed between the Parties, shall constitute the 'documented instructions' referenced herein. Such documented instructions may be provided throughout the duration of the processing of Personal Data, including by email to the address specified in the Agreement or as otherwise agreed and documented by the Parties. 2Checkout shall not process the Personal Data for its own purposes or those of any Third-Party, unless otherwise expressly agreed in this Agreement;

(iii) If 2Checkout is required by applicable law to process Personal Data beyond the scope of the documented instructions, it shall notify the Vendor of that legal requirement prior to commencing the processing, unless prohibited from doing so by law on important grounds of public interest; and

(iv) 2Checkout shall immediately inform the Vendor if, in its opinion, the received instructions to process the Personal Data infringe the Data Protection Laws or any other applicable laws.

D. Security

2Checkout shall implement appropriate technical and organizational measures as set out in Schedule 2.A.

E. Sub-processors

(i) Vendor hereby grants 2Checkout a general authorization to appoint and disclose the Personal Data to 2Checkout's Sub-processors, for the purpose of enabling them to process such data in connection with the provision of the Vendor-Requested Services , as set forth in the Agreement. A list of the authorized Sub-processors is provided in Schedule 3.A.

(ii) Notwithstanding the foregoing, prior to making any changes to the list through the addition or replacement of Sub-processors, 2Checkout shall notify the Vendor in writing at least thirty (30) calendar days prior to engaging any new Sub-processor.

(iii) The Vendor may object to the proposed Sub-Processor on reasonable and documented data protection grounds by providing written notice within fifteen (15) calendar days' notice period. Upon objection, the parties shall seek in good faith to resolve the matter.

(iv) If the Vendor raises such objections, 2Checkout may choose within fifteen (15) days from the date of the Vendor's written objection to:

(v) not to use the Sub- processor; or

(vi) to agree with the Vendor the corrective measures in connection with the objections raised and use the Sub- processor. If neither of these options are reasonably possible, the Parties shall enter into good faith discussions. If no mutually satisfactory resolution is reached within sixty (60) calendar days from the Vendor's objection, either Party may suspend or

terminate the affected processing operations, without prejudice to any fees or charges incurred by 2Checkout prior to the suspension or termination, by providing thirty (30) calendar days' written notice.

(vii) If no objection is received within the fifteen (15) calendar days' notice period, the Data Controller shall be deemed to have consented to the appointment of the Sub-Processor.

(viii) 2Checkout undertakes that any authorized Sub- processor is subject to the same, in substance, data protection obligations as the ones imposed on 2Checkout in this Data Protection Agreement. Subject to the limitation of remedies and damages set forth in the Agreement, and to the extent permitted under applicable law, 2Checkout shall remain fully liable to the Vendor for the performance of the Sub-processors' obligations under their respective contracts.

F. Cooperation and data subjects' rights

(i) From time to time, the Vendor may need to respond to a request from a data subject seeking to exercise its rights under the applicable Data Protection Laws. In such an instance, and if requested by the Vendor, 2Checkout shall provide all reasonable and timely assistance by appropriate technical and organizational measures to enable Vendor to respond to: (a) any request from a data subject to exercise any of its rights under applicable Data Protection Laws (including its rights of access, rectification, objection, restriction, erasure and data portability, as applicable); and (b) any other correspondence, inquiry or complaint received from a data subject, a supervisory authority or other Third-Party in connection with the processing of the Personal Data.

(ii) If any such request, correspondence, inquiry or complaint is made directly to 2Checkout, 2Checkout shall transmit to Vendor such request within a maximum of five (5) working days from its receipt by 2Checkout providing full details of the requested to the e-mail address indicated in the Agreement or in the Order Form or at such other address as may be agreed by the parties. Regarding such requests, 2Checkout shall act pursuant to Vendor's instructions.

(iii) If any such request, correspondence, inquiry or complaint is made directly to the Vendor, the Vendor shall promptly inform 2Checkout of the same.

G. Data Protection Impact Assessment

2Checkout shall, at the Vendor's cost and taking into account the nature of the processing and the information available to 2Checkout, provide the Vendor with reasonable and timely assistance as may be required by the Vendor to carry out a data protection impact assessment and, where applicable, to consult it with the relevant data protection supervisory authority, in accordance with applicable Data Protection Laws.

H. Audits and Inspections

(i) The Vendor acknowledges that 2Checkout maintains technical and organizational security measures that include independent third-party audits, such as certification against the Payment Card Industry Data Security Standards (PCI-DSS). Upon written request, 2Checkout shall provide the Vendor with a copy of its most recent Attestation of Compliance (AOC). To the extent necessary for the Vendor to assess 2Checkout's compliance with its obligations under this Data Processing Agreement, 2Checkout shall provide, on a confidential basis and at reasonable intervals, written responses to reasonable information requests. Such responses may include security summaries, certifications, or whitepapers, and shall be deemed sufficient unless applicable Data Protection Laws or a competent authority require additional review. The Parties acknowledge that any platforms, systems, and infrastructure used by 2Checkout to provide the Services may be hosted in a cloud-based environment ("Cloud Services Environment"), and that 2Checkout maintains sole discretion over the technical architecture, providers, and configurations used to support its service delivery. For clarity, no right of access to 2Checkout's Cloud Services Environment is granted under this DPA.

(ii) 2Checkout shall permit the Vendor and its authorized third-party representatives to audit, at the Vendor's costs, 2Checkout's compliance with this DPA, on at least: (i) 60 days' prior notice for a regular audit; or (ii) 5 days' prior notice in case of the material breach of this DPA or if an investigation is initiated by the relevant data protection supervisory authority concerning 2Checkout's processing of Personal Data, and provided that any such audit shall be conducted during normal business hours, and the Vendor shall take reasonable measures to avoid unnecessary disruption to 2Checkout's operations and to protect 2Checkout's Confidential Information.

(iii) 2Checkout shall maintain adequate documentation verifying its compliance with this DPA. 2Checkout will keep detailed, accurate and up-to-date written records regarding processing of the Personal Data, including the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, any transfers of the Personal Data to a third country and related safeguards, and a general description of the Minimum-Security Measures and the Additional Security Measures. 2Checkout will ensure that the records are sufficient to enable the Vendor to verify 2Checkout compliance with its obligations under this DPA and 2Checkout will provide the Vendor with copies of these records upon request.

I. Cross-border Transfers of Personal Data

(i) Any Transfer of Personal Data outside the EEA that is not covered by an EU Adequacy Decision or the EU-U.S. Data Privacy Framework shall be carried out in accordance with Clause 8 of the Addendum (in particular Clauses 8.2 and 8.3).

(ii) Where 2Checkout engages a Sub-processor in accordance with this DPA for carrying out specific processing activities and those processing activities involve Transfer of Personal Data, 2Checkout undertakes to ensure that the Transfer is made in compliance with the applicable Data Protection Laws, in particular by agreeing with the Sub-processor the relevant Additional Safeguards and the Supplementary Measures, including but not limited to entering with the Sub-processor into the EU SCCs or the Swiss SCCs, or UK IDTA, or the UK Addendum to the EU SCCs, as applicable.

J. Non-compliance with the Data Processing Agreement and termination of the Data Processing Agreement

1. Suspension of processing

2Checkout shall promptly inform Vendor if it is unable to comply with this Data Processing Agreement for whatever reason. The Parties shall negotiate in good faith the measures, remedies and corrections necessary to restore the processing of Personal Data in compliance with this Data Processing Agreement. In the event the Parties will not be able to agree the necessary remedies, and without prejudice to any provisions of the applicable Data Protection Laws, the Vendor may instruct 2Checkout to suspend the processing of Personal Data until the latter complies with this Data Processing Agreement or until the Data Processing Agreement is terminated.

2. Termination of the Data Processing Agreement

The Data Processing Agreement shall terminate automatically upon termination of the Agreement, or any Work of Order, or SOW, or any of their parts relevant to the processing of the Personal Data for the specified Services and Vendor-Requested Services. Vendor shall have the right to terminate this Data Processing Agreement in case of any of the following:

(i) the processing of Personal Data by 2Checkout has been suspended by Vendor, provided that the compliance with this Data Processing Agreement is not restored within a reasonable time and in any event within one month following suspension;

(ii) 2Checkout is in substantial or persistent breach of this Data Processing Agreement or its obligations under the applicable Data Protection Laws;

(iii) 2Checkout fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Data Processing Agreement or the applicable Data Protection Laws.

(iv) 2Checkout shall have the right to terminate this Data Processing Agreement if, after notifying the Vendor, in accordance with this Data Processing Agreement, that its instructions infringe applicable Data Protection Laws, the Vendor nonetheless insists on compliance with such instructions.

(v) Termination of this Data Processing Agreement shall result in the termination of the Agreement and the Addendum to the extent that further performance is either impossible or would impose significantly higher costs on any of the Parties, and provided that the Parties have not, within a reasonable time, reached a mutually satisfactory agreement on measures, remedies, or corrections to the processing of Personal Data necessary to ensure compliance with this Data Processing Agreement.

3. Deletion or return of the Personal Data

(i) Processing of the Personal Data by 2Checkout shall only take place for the duration specified in Schedule A.1(ii).

(ii) Upon termination or expiration of this Data Processing Agreement, 2Checkout shall destroy or return to the Vendor all Personal Data (including all copies of the Personal Data) in its possession or control, as a (sub)processor. This requirement shall not apply to the extent that 2Checkout is permitted by any applicable EU (or any EU Member State) or any Swiss or any UK law, or PCI-DSS, to retain some or all of the Personal Data, in which event 2Checkout shall isolate and protect the Personal Data from any further processing except to the extent permitted by such law.