DATA PROCESSING ADDENDUM

Preamble
This Data Processing Addendum & Appendix ("**DPA**") forms part of the **General Services Agreement** ("**GSA**") between **Aperia Compliance, LLC** ("**Vendor**") and the client identified in the GSA ("**Client**"). This DPA applies **only if and to the extent** Vendor Processes **Personal Data** that is subject to **Data Protection Legislation** (as defined below). Our privacy notice is available at www.aperiacompliance.com for your information.

1. DEFINITIONS

"Data Protection Legislation" means all data protection and privacy laws and regulations applicable to the Processing of Personal Data under this DPA, including but not limited to the GDPR and any European Economic Area ("**EEA**") member state laws implementing the GDPR, UK GDPR, LGPD, CPRA, U.S. state privacy laws, applicable financial privacy laws referenced in the GSA and any amendments or successors thereto.
"Personal Data" means any information defined as "personal data" under GDPR, or an equivalent term under Data Protection Legislation that is Processed by Vendor on behalf of Client under the GSA. For clarity, Personal Data may constitute a subset of "Client Data" or "Confidential Information" under the GSA; however, the obligations of this DPA apply exclusively to Personal Data.
"Processing" has the meaning given under Data Protection Legislation.
"Controller" means the person or organization that determines the purposes and means of Processing, including the definitions of "Controller" under the GDPR, UK GDPR, and LGPD, and "Business" under the CPRA and other U.S. state privacy laws.
"Processor" means the person or organization that Processes Personal Data on behalf of the Controller, including the definitions of "Processor" under the GDPR, UK GDPR, and LGPD, and "Service Provider" under the CPRA and other U.S. state privacy laws.
"Restricted Transfer" means a transfer of Personal Data to a country or jurisdiction that is not recognized under Data Protection Legislation as providing an adequate level of data protection, including but not limited to transfers (i) from the EEA or the UK to a third country that lacks an adequacy decision under the GDPR or UK GDPR, or (ii) any other transfer subject to cross-border data transfer restrictions under Data Protection Legislation.
"**Standard Contractual Clauses"** or "**SCCs**" means the contractual clauses adopted under Data Protection Legislation that legally facilitate Restricted Transfers, including the contractual clauses annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for transfers subject to the GDPR ("**EU SCCs**"); the International Data Transfer Addendum issued by the UK Information Commissioner's Office (ICO) for transfers subject to UK GDPR ("**UK Addendum**"); and the Standard Contractual Clauses adopted by the Brazilian Data Protection Authority (ANPD) under Resolution No. 19/2024 for transfers subject to the LGPD ("**Brazilian SCCs**"), in each case as updated, replaced, or amended from time to time. Where other Data Protection Legislation mandates the use of standard contractual clauses for cross-border transfers, SCCs shall also refer to any such clauses formally recognized under the relevant legal framework.
"Subprocessor" means any third-party (including IXOPAY Group affiliates) engaged by Vendor to Process Personal Data on behalf of Client.

2. PROCESSING

2.1. Subject Matter, Nature, Purpose and Duration of Processing. The subject matter, nature and purpose of the Processing are determined by Client's use of the Services under the GSA, as further specified in the DPA Appendix. The duration of the Processing corresponds to and continues for the GSA term, unless otherwise stated elsewhere in the Agreement or longer retention is required by Data Protection Legislation.
2.2. Roles of the Parties. Given the nature of the Service(s), Client may act as a Controller or as a Processor acting on behalf of another Controller. Where Client acts as a Processor, this DPA continues to refer to Client as the Controller, as Vendor has no direct relationship with Client's Controllers and is not responsible for their instructions. Vendor acts as a Processor of Personal Data, except as set out in section 10 below. If Client acts as a Processor on behalf of another Controller, Client warrants that instructions and actions with respect to that Personal Data, including appointment of Vendor as another Processor, have been authorized by the relevant Controller. Vendor will have no direct obligations toward any

Controller other than Client, nor will it be required to verify whether Client acts as a Controller or Processor. Client and Vendor mutually serve as a single point of contact for each other regarding Vendor's obligations under this DPA.

2.3. Processing Instructions.

2.3.1. Vendor will Process Personal Data only on documented instructions, as set forth in the Agreement and this DPA (which includes Client's instructions via APIs made available by Vendor as part of the Services and any Processing initiated in the use of the Services), and as required by applicable laws. In the latter case, Vendor will inform Client of the legal requirement before Processing, unless that law prohibits such information on important public interest grounds. Client warrants that its instructions are lawful and that it has a valid legal basis under Data Protection Legislation for the Processing described herein. If, in Vendor's reasonable opinion, an instruction infringes Data Protection Legislation, Vendor will inform Client without undue delay, and may suspend the performance of the instruction until Client has modified or confirmed the instruction's lawfulness via email to privacy@ixopay.com.

2.3.2. As a specific instruction, Client authorizes Vendor and its authorized IXOPAY Group Subprocessors to use Personal Data to monitor, maintain, and improve the Services and services as part of the service delivery provided to Client ("Service Improvement"). Service Improvement includes (i) ensuring the security, stability, and performance of the Services, (ii) optimizing and enhancing the features and functionality of the Services in light of Client-specific configurations, use patterns, or performance feedback, (iii) developing new Service features or functionalities, provided they are reasonably expected to be made available to Client as part of the contracted service. Such use shall remain limited to the scope of service delivery and operational support owed to Client.

2.3.3. Client further authorizes Vendor and its authorized IXOPAY Group affiliates to irreversibly anonymize Personal Data and to use such anonymized data for lawful business purposes beyond the scope of direct service delivery to Client. This includes, but is not limited to, generalized product and service improvements not specific to Client, industry-wide research, analytics, benchmarking, and marketing.

2.3.4. Vendor shall not use Personal Data to develop, train, or fine-tune any Generative AI. For the purposes of this DPA, "Generative AI" means artificial intelligence systems specifically designed to generate new content (such as text, images, audio, video, code, or other media) in response to prompts or based on patterns learned from training data (e.g., large language models, text-to-image generators, and other content creation AI systems). This restriction does not apply to machine learning used solely to support service delivery or improvements to Client, such as fraud scoring or anomaly detection.

2.4. Changes to Processing. Any changes to the above Processing instructions shall be agreed upon as part of a written Order and/or Statement of Work. If such changes significantly increase the scope of Vendor's Processing, Vendor shall be entitled to appropriate remuneration for the additional work.

2.5. Compliance with Legal Obligations, Restricted Transfers & Indemnity.

2.5.1. Without prejudice to Vendor's responsibility for Processing Personal Data in accordance with this DPA, Client is responsible for ensuring that all Processing activities carried out under this DPA comply with Data Protection Legislation, including securing a lawful basis for Processing, fulfilling transparency obligations, and responding to data subject rights requests. Client is also responsible for ensuring compliance by its authorized users when accessing or using the Services.

2.5.2. Where the Processing of Personal Data under this DPA involves a Restricted Transfer, such transfers shall be governed by the relevant SCCs, as set forth in Section 9. of this DPA. The SCCs incorporated into this DPA shall apply where no other valid transfer mechanism under Applicable Data Protection Legislation is available. Where Vendor's compliance with a Client instruction results, or would result, in a Restricted Transfer, Client must, in its sphere of responsibility, ensure compliance with the conditions set forth in Chapter V (UK) GDPR and equivalent provisions under Data Protection Legislation.

2.5.3. Client will indemnify Vendor in accordance with the GSA's Indemnification Procedures, for any third-party claims, fines, penalties, or regulatory actions, including those imposed by supervisory authorities, arising from Client's breach of its obligations under this section 2.5.

2.6. Ownership and Processing Limitations. Except where Vendor processes certain Personal Data as an independent Controller as set out in Section 10 below, all Personal Data provided by Client and any copies or reproductions thereof remain the sole property of Client or the respective data owner, and Vendor does not retain, use, or disclose Personal Data for any commercial purpose other than relating to the provision of the Service. Vendor will not sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to any third party for targeted

advertising, cross-context behavioral advertising, or any other secondary purpose where such restrictions apply under Data Protection Legislation.

3. SECURITY AND CONFIDENTIALITY

3.1. Technical and Organizational Measures.

3.1.1. "**Vendor Group**", comprising Vendor and any entity directly or indirectly controlling, controlled by, or under common control with Vendor has implemented and maintains technical and organizational measures to ensure a level of security appropriate to the risk, as published on aperiacompliance.com/legal/toms ("**Vendor TOMs**"). These measures include protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data that is transmitted, stored or otherwise Processed. In particular, Vendor ensures that persons authorized to Process Personal Data are granted access only on a need-to-know basis and have committed themselves to confidentiality, either by contract or by law.

3.1.2. Client is solely responsible for evaluating whether the security measures implemented and maintained by Vendor meet Client's needs and requirements. Vendor reserves the right to modify the Vendor TOMs, provided that such changes do not materially degrade the security of the Processing.

3.1.3. Client confirms that it has implemented and will maintain appropriate security measures within its own infrastructure and shall ensure that all authorized users of the Services do the same, in compliance with Data Protection Legislation.

3.2. Data Protection by Design and by Default. Vendor considers the principles of data protection by design and by default when developing and designing its Services, to the extent required under Data Protection Legislation. However, Client remains solely responsible for choosing and configuring the functions of any Service in accordance with Data Protection Legislation applicable to Client's use thereof.

4. SUBPROCESSING

4.1. Authorization and Responsibilities. Hereby, Client authorizes the engagement of (i) Vendor Group affiliates and (ii) of all third parties listed as Subprocessors at aperiacompliance.com/legal/subprocessors. Client can request an up-to-date list of Subprocessors via email to privacy@ixopay.com at any time. Vendor enters into a written agreement with each Subprocessor, ensuring that the Subprocessor is bound by contractual obligations substantially similar to those of Vendor under this DPA and in compliance with Data Protection Legislation, including where required, Article 28 GDPR. Vendor remains responsible for ensuring that its Subprocessors comply with such obligations and for their performance.

4.2. Notification and Objection Rights. Vendor will inform Client at least 30 days in advance of any intended addition or replacement of a Subprocessor by (i) updating the Subprocessor list available at aperiacompliance.com/legal/subprocessors, and/or (ii) via email notification to Client's Billing and/or Privacy email address specified in the applicable Order Form, which will serve as written notice to Client. To the extent required by applicable Data Protection Legislation and/or incorporated Restricted Transfer clauses, Client is entitled to object to such changes within 30 days after notice has been received, acting reasonably, particularly if such change would lead to Client's violation of Data Protection Legislation or other applicable laws. Client's objection must include its reasonable grounds for the objection together with any options to mitigate. In the event of an objection in accordance with the aforesaid requirements, the Parties shall cooperate to find a feasible solution, including that Vendor will recommend a reasonable modification to Client's configuration of the Service or conduct changes thereto to avoid Processing of Personal Data by the intended new Subprocessor. If the Parties cannot find a feasible solution within 30 days of Client's legitimate objection, Vendor may, at its reasonable discretion, (i) withdraw the intended change thereby not affecting the previous scope of authorized Subprocessors, or (ii) notify Client that, provided the further performance under the affected parts of the Agreement is not technically or commercially reasonable without engaging the intended Subprocessor.

Only where and to the extent required by applicable Data Protection Legislation and/or incorporated Restricted Transfer clauses, either Party may terminate the affected parts of the Agreement by providing 30 days' prior written notice. Such a termination right is limited to any severable part of Client's subscription (if applicable) for which Vendor has intended to engage the respective Subprocessor. Client will be deemed to have consented to the appointment of the Subprocessor and waived its right to object if Client does not provide an objection in accordance with the aforesaid requirements.

5. DATA SUBJECT RIGHTS

5.1. Assistance. Vendor will assist Client in fulfilling its obligations to respond to data subject requests by providing the functionality of the Products and by providing information required for the request as set out in this section 5 to the extent required by applicable Data Protection Legislation. Vendor will, taking into account the nature of the Processing and the information available to Vendor, reasonably assist Client to the extent that, via the functionalities of the Products, Client is unable to address a data subject request without Vendor's assistance. Client shall cover all material reasonable costs incurred by Vendor in connection with its provision of such assistance. If Vendor receives a data subject request that is associated with the Client, it shall forward such request to Client without undue delay and shall not respond to the request unless legally required to do so.

5.2. Client's Part of Responsibility. Client is responsible for verifying that the requestor is the data subject in respect of whose Personal Data the request is made. Client is responsible for handling all data subject requests and ensuring that requests are responded to within applicable timeframes under Data Protection Legislation.

6. PERSONAL DATA BREACH NOTIFICATION

6.1. Vendor shall notify Client without undue delay upon becoming aware of a personal data breach affecting Personal Data Processed under this DPA, as defined under Article 4 (12) GDPR and equivalent provisions under Data Protection Legislation. Such notification shall provide sufficient details to enable Client to assess whether it has an obligation to notify a supervisory authority, data subjects, or other affected entities under Data Protection Legislation.

6.2. The notification shall include, where available and required under Data Protection Legislation: (i) a description of the nature of the breach, including the categories and approximate number of data subjects and/or records affected; (ii) the likely consequences of the breach; and (iii) the measures taken or proposed to mitigate the breach and prevent its recurrence. Where it is not possible to provide all details at once, Vendor may provide information in phases without undue delay.

6.3. Client remains solely responsible for determining whether to notify any supervisory authority, data subjects, or other entities under Data Protection Legislation.

6.4. Nothing in this section shall be construed as an admission of fault or liability by Vendor regarding a personal data breach. Liability of Vendor is excluded if and to the extent caused by Client's failure to submit a legally required notification despite Processor's timely information.

7. DELETION OF PERSONAL DATA

7.1. Client instructs Vendor to delete all Personal Data in accordance with Vendor's industry-standard retention policies within a reasonable time after termination of the Agreement, except to the extent Data Protection Legislation requires storage of the Personal Data by Vendor and/or its Subprocessors. In such a case, Personal Data remains subject to this DPA and Vendor ensures Processing is restricted to legal retention purposes only.

7.2. Client is responsible for retrieving all necessary Personal Data prior to deletion, including via the functionalities of the Services. Vendor is not liable for any Client loss of Personal Data following deletion in compliance with this Section.

8. AUDIT & COMPLIANCE ASSISTANCE

8.1. Audit Rights. Vendor assists Client and provides it, or an auditor mandated by Client (if under an appropriate statutory or contractual obligation of confidentiality towards Vendor), with any necessary information to verify compliance with this DPA to the extent required under Data Protection Legislation, as follows:

8.1.1. Vendor shall primarily provide the most recent security documentation, certifications, and/or summary third-party audit reports conducted to assess and evaluate the effectiveness of the Vendor TOMs. If requested by Client, Vendor shall further cooperate by providing additional clarifications necessary for Client's understanding of such documentation.

8.1.2. If necessary for Client's compliance with its own audit obligations or to respond to a competent supervisory authority's request, Vendor shall, upon Client's written notification of such necessity, reasonably assist Client in providing further relevant information.

8.1.3. To the extent that compliance with mandatory audit obligations cannot be achieved through the measures in Sections 8.1.1. and 8.1.2. above, Client can mandate an independent auditor with the appropriate skills and knowledge to conduct an onsite inspection at Vendor's facilities used to provide the Services under the GSA, under the following conditions: Audits must be conducted during Vendor's normal business hours, in a manner that minimizes disruption to Vendor's operations.

Unless legally required or where there is documented evidence of an actual or reasonably suspected material breach of this DPA, onsite inspections shall not take place more than once per year. The Parties shall coordinate a reasonable audit date and agree on appropriate security and confidentiality measures to prevent risks to Vendor's other Clients. Vendor may impose reasonable limitations or require additional assurances from Client on a case-by-case basis.

8.1.4. The Parties shall bear their own costs for activities under Section 8.1.1. Without prejudice to Client's rights under Data Protection Legislation, Vendor is entitled to reasonable compensation for any assistance under Sections 8.1.2 and 8.1.3 subject to the applicable provisions of the Agreement.

8.1.5. If an audit report generated as a result of Client's audit includes any finding of material non-compliance, Client shall promptly share the relevant findings with Vendor.

8.1.6. Nothing in this Section 8.1 modifies or limits any applicable Standard Contractual Clauses, nor does it affect any rights of a supervisory authority or a data subject thereunder.

8.2. DPIA and Prior Consultation. Upon Client's request, Vendor shall provide reasonable assistance to enable Client to conduct a Data Protection Impact Assessment (DPIA) and/or consult with a supervisory authority where required under Data Protection Legislation, to the extent such assistance relates to Vendor's Processing activities under this DPA. Any such assistance shall be subject to the nature of the Processing and the information reasonably available to Vendor.

8.3. Authority Requests.

Unless legally prohibited, Vendor shall inform Client without undue delay of (i) any legally binding request for disclosure of Personal Data by a law enforcement authority, and (ii) any relevant inquiry or investigation by a supervisory authority relating to Personal Data. For Restricted Transfers governed by Standard Contractual Clauses, IXOPAY shall comply with its obligations under the SCCs, including obligations relating to governmental access requests.

8.4. Communication Requirements. Client shall submit all instructions, requests for assistance, inquiries, and other communications under this DPA via email to privacy@ixopay.com.

9. RESTRICTED TRANSFERS

9.1. Application of Transfer Mechanisms. To the extent that the Processing of Personal Data under this DPA involves a Restricted Transfer, such transfers shall be subject to a valid transfer mechanism under Applicable Data Protection Legislation. The obligations under the applicable transfer mechanism apply only to the respective Restricted Transfer, as determined by the jurisdiction from which the Personal Data is exported: Subject to the details provided in the following of this Section, (i) for transfers subject to GDPR, the EU SCCs shall apply, (ii) for transfers subject to UK GDPR, the UK Addendum shall apply alongside the EU SCCs, and (iii) for transfers subject to LGPD, the Brazilian SCCs shall apply in full without any change in their text. If and as soon as IXOPAY obtains a certification under the EU-U.S. Data Privacy Framework (DPF), the UK Extension to the DPF, or the Swiss-U.S. DPF, Vendor may rely on such certification as a lawful basis for Restricted Transfers to the United States.

9.2. EU Standard Contractual Clauses (EU SCCs). To the extent that the EU SCCs apply, the parties agree that:

i. Where Module One applies for Processing under Section 10 (Independent Controllership), Client acts as a Controller and Data Exporter, and Vendor acts as an independent Controller and Data Importer.
ii. Where Module Two applies, Client acts as a Controller and Data Exporter, and Vendor acts as a Processor and Data Importer.
iii. Where Module Three applies, Client acts as a Processor and Data Exporter, and Vendor acts as a Processor and Data Importer.
iv. Clause 7: The optional docking clause does not apply.
v. Clause 9(a): The parties select "Option 2 – General Written Authorization", with prior written notice of 30 days for engaging new Subprocessors as set out in Section 4 (Subprocessing) of this DPA.
vi. Clause 11: The optional language shall not apply.
vii. Clause 17: The parties select Option 2 and the EU SCCs are governed by the law of Austria in exclusion of its conflict of law rules.
viii. Clause 18(b): Disputes shall be resolved before the courts of Austria.
ix. Annex I.A is deemed completed with the information set out in any applicable Order Form and point i. above, Annex I.B with the information set out in the DPA Appendix.
x. Annex I.C is deemed completed with the "Austrian Data Protection Authority".
xi. Annex II is deemed completed with the Vendor TOMs most recent version.

xii. Annex III is deemed completed with those Subprocessors listed in accordance with Section 4 (Subprocessing) due to the General Authorization granted.

Where Vendor is not established in the European Union and GDPR applies to the Processing, Vendor has appointed IXOPAY GmbH, Vorgartenstrasse 206c, A-1020, Vienna, Austria as its Article 27 GDPR representative. Client may contact the representative via privacy@ixopay.com.

9.3. UK International Data Transfer Addendum (UK Addendum). To the extent that the EU SCCs apply, the parties agree that:

i. The EU SCCs shall be deemed the "Approved EU SCCs" and apply as modified by the UK Addendum. In the event of a conflict between the EU SCCs and the UK Addendum, the UK Addendum shall prevail for Restricted Transfers subject to UK GDPR.
ii. Table 1: Completed with the same information included in Annex I of the EU SCCs per Section 9.2 above. The start date shall be the effective date of the Order Form of any relevant Product.
iii. Table 2: The parties select the EU SCCs (Module One, Two, or Three, as applicable per Section 9.2.(i)-(iii)) and the optional clauses are selected or excluded as set forth for the EU SCCs per Section 9.2 above.
iv. Table 3: Completed as set forth for the EU SCCs per Section 9.2(ix), 9.2(xi),(xii) above.
v. Table 4: Neither party may unilaterally terminate the Addendum under this section.

9.4. Brazilian SCCs. To the extent that the Brazilian SCCs apply, the required information in Annex II Section I shall be completed as follows:

i. Where Vendor acts as a Processor, the Client acts as the Exporter (Controller or Processor, as applicable), and Vendor acts as the Importer (Processor).
ii. Where Vendor acts as an independent controller under Section 10 (Independent Controllership), the Client acts as the Exporter (Controller) and Vendor acts as the Importer (Controller).
iii. Clause 2 (Object and Scope of Application): The details of the transfers covered by Brazilian SCCs are deemed completed as follows: the purpose of processing, personal data transferred, categories of data subjects, and duration of data transfers are governed by the General Services Agreement ("GSA") and specified by reference to all service descriptions of the Agreement, this DPA and the DPA Appendix; Information on the Related Contract: Governed by the GSA, this DPA, and applicable Order Form(s); Data Source: Personal Data transferred is provided by the Exporter (Client) and Client personnel as specified in the DPA Appendix; Transfer Frequency: Continuous, as necessary to deliver the Services and services under the Agreement and related Order Form(s); Brazilian SCCs shall be governed exclusively by Brazilian law, excluding its conflict of law rules, which choice of law is without prejudice to the governing law specified in the Agreement.
iv. Clause 3 (Onward Transfers): The parties select "Option B," granting Vendor general written authorization to perform onward transfers to those Subprocessors listed under Section 4 (Subprocessing). Vendor shall provide Client with prior written notice of 30 days before engaging new Subprocessors.
v. Clause 4 (Designated Party): The parties select Exporter as the Designated Party. However, where Vendor acts as an independent controller under Section 10 (Independent Controllership), no Designated Party is appointed.

10. MISCELLANEOUS

10.1. Independent Controllership. Client acknowledges and authorizes that Vendor and Vendor Group affiliates may process, at their own responsibility and in compliance with Data Protection Legislation, certain Personal Data in their role as an independent controller for the following legitimate business purposes: (i) Ensuring fraud prevention, including identity verification, risk mitigation, and compliance with security policies; (ii) Meeting legal and regulatory obligations; (iii) Managing the relationship with Client, including billing operations, account management and legal documentation; (iv) Conducting internal business operations; and (v) subject to prior irreversible anonymization ensuring that data is no longer identifiable, conducting non-personal evaluations of data for their purpose of developing Vendor Group products and services.

10.2. Entire Agreement, Conflict. This DPA, including the Standard Contractual Clauses, constitute the entire agreement and understanding of the parties, and supersedes any prior agreement or understanding between the parties, in each case in respect of the Processing of Personal Data for the purposes specified herein. In the event of a conflict between this DPA and the GSA, this DPA prevails with respect to the Processing of Personal data. In the event of a conflict between this DPA and the DPA Appendix, the DPA Appendix prevails to the extent it imposes stricter or more specific obligations.

****

DPA Appendix - Aperia Compliance Services

Preamble
This DPA Appendix amends and specifies the main body of the Data Processing Addendum to describe Processing where such detail is required by Data Protection Legislation.

General note: Client individually determines the use and configuration of the Services and the scope of Personal Data Processing including related transmissions to any integrated third-party services.

1. Subject Matter and Purpose of the Processing
The purpose of the Processing is to provide the subscribed Services to Client as outlined in the GSA and applicable Order Forms. Depending on Client's configuration, purposes include:

- **PCI Apply**: Browser-based application and management console facilitating PCI DSS self-assessments, compliance reporting, and document management for Client and its Clients.
- **Script Monitor:** Monitoring payment pages for malicious activity to support compliance with PCI DSS requirements.
- **Endpoint Scanning:** A suite of tools for identifying known vulnerabilities (missing patches, open services, back doors).
- **Endpoint Protection:** Provision of cloud-based security services to protect endpoints from viruses, spyware, and unauthorized access.
- **Endpoint Management:** same as Endpoint Protection, plus automated software patch management.
- **Website Compliance Suite:** Automated auditing of website accessibility (ADA) and Data Protection Legislation compliance (incl. GDPR), including cookie consent management and age-gating.

2. Categories of Data Subjects
Depending on the specific Services subscribed to and Client's configuration, categories of data subjects include:

- **Client personnel:** Employees, agents, or representatives of Client who use the Services and/or access the Application Platform.
- **End merchants:** Client's customers as relevant to the Services' processing activities.
- **Cardholders/Consumers:** Only as part of the provision of Endpoint Scanning Services and to the extent that cardholder data is identified or incidentally processed.

3. Types of Personal Data
Depending on the Service and Client configuration, the following types of Personal Data may be Processed:
3.1. General Personal Data (Processed for all Services):

- Name (First/Last)
- Business contact information (Email, Telephone, Physical address)
- Login credentials and authentication data
- IP address and connection logs

3.2. Service-Specific Logic Data:

- **PCI Apply**: Self-Assessment Questionnaire (SAQ) responses, evidence/support documentation, and compliance status.
- **Script Monitor**: Network/device hostnames, operating system details, payment page URLs, script integrity hashes, device/browser fingerprinting and browser versions.
- **Endpoint Scanning:** Vulnerability scan results and network/system identifiers.

- **Endpoint Protection & Management**: Endpoint telemetry metadata including device, user, process, file, and network activity.
- **Website Compliance Suite:** Cookie consent interaction and log data (e.g., consent status, timestamp, consent record/identifier, website/app identifier, user agent/browser information, language/region, and event/log data relating to accessibility checks and age-gating where enabled)