DATA PROCESSING ADDENDUM

Preamble
This DPA and any relevant DPA Appendix govern IXOPAY's activities to the extent they qualify as Processing of Personal Data under Data Protection Legislation, as defined below. The DPA and any relevant DPA Appendix form an integral part of and are subject to the provisions of the MSA. Each Party's conclusion of an Order Form incorporating this DPA or acceptance through a website signup procedure is considered a signature to this DPA, including any Standard Contractual Clauses incorporated into this DPA by reference.

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, 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 in the course of Customer's use of any Product.

"Processing" means any operation or set of operations performed on Personal Data, whether automated or not, to the extent such operations qualify as processing under Data Protection Legislation. Processing includes, where applicable, collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, combination, restriction, deletion, or destruction.

"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 Processor engaged by IXOPAY to Process Personal Data on its behalf in order to provide any Product to Customer.

2. PROCESSING

2.1. Subject Matter, Nature, Purpose and Duration of Processing. The subject matter, nature and purpose of the Processing are determined by Customer's use of the Products under the MSA, as further specified in the DPA Appendix. The duration of the Processing corresponds to and continues for the MSA 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 Product(s), Customer may act as a Controller or as a Processor acting on behalf of another Controller. Where Customer acts as a Processor, this DPA continues to refer to Customer as the Controller, as IXOPAY has no direct relationship with Customer's Controllers and is not responsible for their instructions. IXOPAY acts as a Processor of Personal Data, except as set out in section 9 below. If Customer acts as a

Processor on behalf of another Controller, Customer warrants that instructions and actions with respect to that Personal Data, including appointment of IXOPAY as another Processor, have been authorized by the relevant Controller. IXOPAY will have no direct obligations toward any Controller other than Customer, nor will it be required to verify whether Customer acts as a Controller or Processor. Customer and IXOPAY mutually serve as a single point of contact for each other regarding IXOPAY's obligations under this DPA.

2.3. Processing Instructions.

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

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

2.3.3. Customer further instructs IXOPAY to irreversibly anonymize Personal Data, and authorizes IXOPAY to use such Anonymized Data for any lawful business purpose that extends beyond the scope of direct service delivery to Customer. This includes, but is not limited to, generalized product and service improvements not specific to Customer, industry-wide research, analytics, benchmarking, and marketing. IXOPAY will ensure that Anonymized Data cannot reasonably be re-identified and that no individual or Customer can be singled out based on such use.

2.3.4. IXOPAY 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 to Customer under documented instructions, such as fraud scoring or routing optimization.

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 IXOPAY's Processing, IXOPAY 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 IXOPAY's responsibility for Processing Personal Data in accordance with this DPA, Customer 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. Customer is also responsible for ensuring compliance by its Authorized Users when accessing or using the Products.

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 IXOPAY's compliance with a Customer instruction results, or would result, in a Restricted Transfer, Customer 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. Customer will indemnify IXOPAY in accordance with MSA, section 8.3 for any third-party claims, fines, penalties, or regulatory actions, including those imposed by supervisory authorities, arising from Customer's breach of its obligations under this section 2.5.

2.6. Ownership and Processing Limitations. Except where IXOPAY processes certain Personal Data as an independent Controller as set out in Section 10 below, all Personal Data provided by Customer and any copies or reproductions thereof remain the sole property of Customer or the respective data owner, and IXOPAY does not retain, use, or disclose Personal Data for any commercial purpose other than relating to the provision of the Service. IXOPAY 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 Applicable Data Protection Legislation.

3. SECURITY AND CONFIDENTIALITY

3.1. Technical and Organizational Measures ("TOMs").

3.1.1. IXOPAY has implemented and maintains TOMs to ensure a level of security appropriate to the risk within its scope of responsibility as a Processor. 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, IXOPAY 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. Customer can consult the most recent version of IXOPAY's TOMs at www.ixopay.com/en/legal/toms, which may be updated from time to time. Customer is solely responsible for evaluating whether the security measures implemented and maintained by IXOPAY meet Customer's needs and requirements. IXOPAY reserves the right to modify the TOMs, provided that such changes do not materially degrade the security of the Processing.

3.1.3. Customer confirms that it has implemented and will maintain appropriate security measures, including TOMs, within its own infrastructure and shall ensure that all Authorized Users do the same, in compliance with Data Protection Legislation.

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

4. SUBPROCESSING

4.1. Authorization and Responsibilities. Hereby, Customer authorizes IXOPAY to engage the Subprocessors listed, including a description of their processing activities and locations, at https://www.ixopay.com/en/legal/subprocessors. Customer can request an up-to-date list of Subprocessors via email to privacy@ixopay.com at any time. IXOPAY enters into a written agreement with each Subprocessor, ensuring that the Subprocessor is bound by contractual obligations substantially similar to those of IXOPAY under this DPA and in compliance with Data Protection Legislation, including where required, Article 28 GDPR. IXOPAY remains responsible for ensuring that its Subprocessors comply with such obligations and for their performance. IXOPAY shall enter into a written agreement with each Subprocessor, ensuring that it is bound by obligations substantially similar to those set out in this DPA and in compliance with Data Protection Legislation, including where required GDPR Article 28(4) or equivalent provisions. IXOPAY remains responsible for ensuring that any Subprocessors comply with the obligations of this DPA and for their performance.

4.2. Notification and Objection Rights. IXOPAY will inform Customer at least 30 days in advance of any intended addition or replacement of a Subprocessor by (i) updating the Subprocessor list available at www.ixopay.com/en/legal/subprocessors, and (ii) via email notification to Customer's Billing and/or Privacy email address specified in the applicable Order Form, which will serve as written notice to Customer. Customer is entitled to object to such changes within 30 days after notice has been received, acting reasonably, particularly if such change would lead to Customer's violation of Data Protection Legislation or other applicable laws. Customer'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 IXOPAY will recommend a reasonable modification to Customer's configuration of the Product 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 Customer's legitimate objection, IXOPAY may, at its reasonable discretion, (i) withdraw the intended change thereby not affecting the previous scope of authorized Subprocessors, or (ii) notify Customer that, provided the further performance under the affected parts of the Agreement is not technically or commercially reasonable without engaging the intended Subprocessor. In case of Customer's notification under (ii), 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 Customer's subscription (if applicable) for which IXOPAY has intended to engage the respective Subprocessor. Customer will be deemed to have consented to the appointment of the Subprocessor and waived its right to object if Customer does not provide an objection in accordance with the aforesaid requirements.

5. DATA SUBJECT RIGHTS

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

5.2. Customer's Part of Responsibility. The Customer is responsible for verifying that the requestor is the data subject in respect of whose Personal Data the request is made. Customer 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. IXOPAY shall notify Customer 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 Customer 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: (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, IXOPAY may provide information in phases without undue delay.

6.3. Customer 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 IXOPAY regarding a personal data breach. Any liability of IXOPAY is excluded if Customer fails to submit a legally required notification despite Processor's timely information.

7. DELETION OF PERSONAL DATA

7.1. Customer instructs IXOPAY to delete all Personal Data in accordance with IXOPAY's industry-standard retention policies no later than 30 days after termination of the Agreement, except to the extent Data Protection Legislation requires storage of the Personal Data by IXOPAY and/or its Subprocessors. In such a case, Personal Data remains subject to this DPA and IXOPAY ensures Processing is restricted to legal retention purposes only. To the extent applicable, Data Export and Migration Support for the Platform are governed by the relevant provisions of the Agreement governing such services, including related timeframes, conditions, and applicable fees.

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

8. AUDIT & COMPLIANCE ASSISTANCE

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

8.1.1. IXOPAY 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 Technical and Organizational

Measures (TOMs). If requested by Customer, IXOPAY shall further cooperate by providing additional clarifications necessary for Customer's understanding of such documentation.

8.1.2. If necessary for Customer's compliance with its own audit obligations or to respond to a competent supervisory authority's request, IXOPAY shall, upon Customer's written notification of such necessity, reasonably assist Customer 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, Customer can mandate an independent auditor with the appropriate skills and knowledge to conduct an onsite inspection at IXOPAY's facilities used to provide the Products under the MSA, under the following conditions: Audits must be conducted during IXOPAY's normal business hours, in a manner that minimizes disruption to IXOPAY'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 IXOPAY's other customers. IXOPAY may impose reasonable limitations or require additional assurances from Customer 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 Customer's rights under Data Protection Legislation, IXOPAY 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 Customer's audit includes any finding of material non-compliance, Customer shall promptly share the relevant findings with IXOPAY.

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 Customer's request, IXOPAY shall provide reasonable assistance to enable Customer 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 IXOPAY's Processing activities under this DPA. Any such assistance shall be subject to the nature of the Processing and the information reasonably available to IXOPAY.

8.3. Authority Requests. Unless legally prohibited, IXOPAY shall inform Customer 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. Customer 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, IXOPAY 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), Customer acts as a Controller and Data Exporter, and IXOPAY acts as an independent Controller and Data Importer.

ii. Where Module Two applies, Customer acts as a Controller and Data Exporter, and IXOPAY acts as a Processor and Data Importer.

iii. Where Module Three applies, Customer acts as a Processor and Data Exporter, and IXOPAY 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 most recent version of IXOPAY's TOMs available at www.ixopay.com/en/legal/toms.

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

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 IXOPAY acts as a Processor, the Customer acts as the Exporter (Controller or Processor, as applicable), and IXOPAY acts as the Importer (Processor).

ii. Where IXOPAY acts as an independent controller under Section 10 (Independent Controllership), the Customer acts as the Exporter (Controller) and IXOPAY 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 Master Services Agreement ("MSA") 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 MSA, this DPA, and applicable Order Form(s); Data Source: Personal Data transferred is provided by the Exporter (Customer) and its Authorized Users as specified in the DPA Appendix; Transfer Frequency: Continuous, as necessary to deliver the Products 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 IXOPAY general written authorization to perform onward transfers to those Subprocessors listed under Section 4 (Subprocessing). IXOPAY shall provide Customer 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 IXOPAY acts as an independent controller under Section 10 (Independent Controllership), no Designated Party is appointed.

10. MISCELLANEOUS

10.1. Independent Controllership. Customer acknowledges and authorizes that in addition to its role as a Processor, IXOPAY and its 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 Customer, including billing operations, account management and legal documentation; (iv) Conducting internal business operations; and (v) subject to prior irreversible anonymization, conducting non-personal evaluations of Personal Data for the IXOPAY's purpose of developing any Products, provided that such anonymization must be irreversible, ensuring that data is no longer identifiable, and therefore falls outside the scope of Data Protection Legislation.

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 MSA, 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 - Payment Orchestration Platform

Preamble
This DPA Appendix amends and specifies the above main body of the Data Processing Addendum for the provision of the Platform.
The current list of provided technical interfaces to Payment Service Providers and 3rd-Party Services (acting as possible recipients) is available at adapters.ixopay.com; Customer and/or its Authorized Users determine the use of such interfaces and the related transmission of Personal Data to the afore-said recipients.

General note: Due to the nature of the service, IXOPAY cannot or not continuously assess the accuracy of the below lists of categories of data subjects and types of Personal Data.

1. Purpose of the Processing. The purpose of the Processing is to provide Payment Orchestration services via the Platform, as defined in the MSA:

- The provision of all functions of the Platform, as detailed in the Platform Description.
- Where Customer subscribes to a Customer Experience Package (CXP), the purpose includes support, troubleshooting, and optimization services related to Customer's use of the Platform, including response handling, configuration assistance, and operational improvements.

2. Categories of data subjects. Categories of data subjects include:

- Authorized User
- End Client as defined in MSA

each if in scope of Data Protection Legislation (e.g., excluding legal entities under (UK) GDPR).

3. Type of Personal Data. Types of Personal Data that may typically be processed as part of the service include:

- Authorized User data (for authentication & Platform access):
  - Name (Company)
  - Email address
  - IP address
- End Client data (for payment transaction processing):*
  - Name
  - Date of birth
  - Gender
  - Billing address
  - Shipping address
  - Telephone number
  - Email address
  - IP address & Device data (e.g. timezone, language, screen height & width)
  - National identification number (e.g., social security number)
  - Account data (e.g., IBAN, PayPal ID–excluding full CC information)
  - Credit card number (CC No. - PCI DSS Level 1 compliant)
  - Variable data field **

*Customer and/or its Authorized Users individually determine the indication of these Personal Data of End-Clients, the purpose of the Processing and any disclosure to Payment Service Providers and 3rd-Party Services or other recipients, as such parties' acceptance of transactions is generally subject to their specific requirements.
**Customer and/or its Authorized Users individually determine the freely selectable content of this data field.

4. Use of Cookies. The Platform uses the following strictly necessary technical cookies, which are exempt from the requirement of consent under Applicable Data Protection Legislation:

Cookie Name	Purpose	Duration
pgateway_session	Identifies Users once logged in, needed to allow authentication on successive visits to the Platform and access authorized content ("Authentication Cookie").	Session Cookie (deleted when the browser is closed)
PHPSESSID	Authentication Cookie.	Session Cookie (deleted when the browser is closed)
_session_server	Distributes web server processing over multiple machines for load balancing.	Session Cookie (deleted when the browser is closed)

****

DPA Appendix - Standalone Payment Modules

Preamble
This DPA Appendix amends and specifies the above main body of the Data Processing Addendum for the provision of IXOPAY's Standalone Payment Modules as defined in the Master Services Agreement ("MSA") and any related Product Descriptions. The currently available Standalone Payment Modules include: **Universal Tokenization, Point-to-Point Encryption (P2PE), Card Account Updater, BIN Lookup, 3-D Secure, Payment Account Reference (PAR), and Network Tokenization.**
General note: Customer individually determines which module(s) are activated and which third-party endpoints are used. Customer and/or its Authorized Users determine the use of individual modules, as well as the scope of Personal Data Processing and transmission to any integrated third-party services, Payment Service Providers, and card schemes. Some services, such as Card Account Updater or 3-D Secure, may rely on card scheme rules or issuer-side authentication flows. Therefore, IXOPAY may be unable to determine in advance the precise extent of data sharing or decisions taken by the relevant networks.

1. Purpose of the Processing

The purpose of the Processing is to provide the subscribed Standalone Payment Modules as part of the IXOPAY Products under the MSA. These modules are designed to support security, compliance, and payment lifecycle optimization. Depending on Customer configuration, such purpose includes:

- **Universal Tokenization:** Conversion of cardholder data and related sensitive identifiers into PCI-compliant token representations for use across payment channels and third-party systems.
- **P2PE:** Secure encryption of cardholder data at the point of interaction, subsequent decryption by IXOPAY to facilitate downstream payment processing, and support of PCI DSS compliance scope reduction for card-present transactions.
- **Card Account Updater**: Submission of limited cardholder account data to the relevant Card Schemes via IXOPAY's integration with external service providers to identify updated payment credentials and update tokenized records accordingly.
- **BIN Lookup**: Extraction of metadata from card numbers to inform payment routing and issuer intelligence (e.g., card brand, country, or funding source).
- **3-D Secure**: Initiation of Strong Customer Authentication (SCA) flows under PSD2 and equivalent regimes; transmission of authentication requests to issuer-side authentication systems via EMV 3DS protocols.
- **Payment Account Reference (PAR):** Retrieval of non-financial, unique identifiers (PAR) linked to underlying payment accounts to enable Customer reconciliation across multiple payment methods and improve tracking and data security.
- **Network Tokenization:** Issuance and management of Card Scheme-issued tokens (Network Tokens) replacing sensitive cardholder data for secure payment processing.

Specific module functionalities are further detailed in IXOPAY's Documentation. Where Customer subscribes to additional support services or Customer Experience Packages (CXP), the purpose includes associated support, troubleshooting, configuration assistance, and service optimization.

2. Categories of data subjects. Depending on the module and Customer configuration, categories of data subjects include:

- Authorized Users (for login, configuration, or access)
- End Clients: cardholders or payers, to the extent falling within scope of applicable Data Protection Legislation.

3. Type of Personal Data. Depending on the module and Customer configuration, the following types of Personal Data may be Processed:

- Cardholder Data

- Name
- Card number (PAN – PCI DSS Level 1 compliant)
- Expiration date
- Card brand
- Card verification data (e.g., CVV, if applicable and permitted)

- Transaction Metadata
    - BIN (Bank Identification Number)
    - IP address
    - Device/browser fingerprinting information
    - Geolocation
    - Time and date of transaction
    - Merchant identifier
    - Authorization result codes (e.g., for 3-D Secure)
- Module-Specific Logic Data
    - **Universal Tokenization:** Token values, token metadata (creation date, usage scope, status)
    - **Account Updater:** Legacy card identifiers and updated card metadata returned by Card Schemes (e.g., replacement PAN, expiry date, closed account flag)
    - **BIN Lookup:** BIN response data (e.g., issuing bank, card type, commercial vs. consumer flag, card region)
    - **3-D Secure:** Authentication identifiers, challenge/response data, issuer result messages
    - **P2PE:** Encrypted payloads from payment terminals, corresponding decryption keys or tokens, and decrypted cardholder data (PAN, expiry date, and related cardholder details) processed and transmitted under Customer instructions via IXOPAY's Technical Gateway API (TGAPI) to designated Payment Service Providers (PSPs).
    - **Payment Account Reference (PAR):** Unique non-financial PAR identifiers associated with cardholder payment accounts, returned from Card Schemes
    - **Network Tokenization:** Network Tokens issued by Card Schemes, token metadata including Token Requestor IDs (TRID), and associated lifecycle management data for tokenized card accounts

Note: Customer and/or its Authorized Users individually determine the exact scope, indication, and content of End-Client data submitted in the use of the respective Product and disclosed to external endpoints (e.g., Card Schemes, fraud systems, and other third parties).

****