OPayments PERSONAL DATA PROCESSING AND PRIVACY POLICY

This Policy sets out the procedure and conditions for the collection, use, storage, transfer, protection and other processing of Personal Data in connection with the use of the OPayments website and payment technology service.

TERMS AND DEFINITIONS

– **"Personal Data"** means any information relating to an identified or identifiable natural person, including their name, contact details, employment and position information, identification data, information about actions performed within the Service, payment and transaction metadata, network and technical identifiers, device fingerprint and any other information that directly or indirectly enables the identification of a natural person;

– **"Data Subject"** means a natural person whose Personal Data is processed by the Controller, including Website visitors, Users, representatives, employees, officers and beneficial owners of Clients, applicants for connection to the Service, representatives of partners and contractors, and persons submitting enquiries through the Website, by email, through messengers or via other communication channels;

– **"Controller"** means the person specified in Section 8 of this Policy that, independently or jointly with other persons, determines the purposes and means of Processing Personal Data in connection with the operation of OPayments;

– **"Processor"** means any natural or legal person, public authority, organisation or other entity that Processes Personal Data on behalf of and under the instructions of the Controller pursuant to an agreement or another applicable legal ground;

– **"Processing of Personal Data"** or **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, receipt, recording, organisation, structuring, accumulation, storage, clarification, updating, alteration, matching, analysis, use, transfer, provision of access, restriction, blocking, anonymisation, pseudonymisation, deletion, destruction and Cross-Border Transfer;

– **"Automated Processing"** means Processing of Personal Data using software, information systems, computing facilities, algorithms and other automated technologies;

– **"Profiling"** means Automated Processing of Personal Data for the purpose of evaluating certain characteristics or behaviour of a natural person, including risk analysis, fraud prevention, identification of suspicious activities and ensuring the security of the Service;

– **"Anonymisation"** means actions as a result of which it is impossible, without the use of additional information, to determine that data relates to a specific Data Subject;

– **"Pseudonymisation"** means Processing of Personal Data in such a manner that the data can no longer be attributed to a specific person without the use of additional information that is stored separately and protected by appropriate measures;

– **"Website"** means the website available at https://opayments.io, including its pages, forms, interfaces, payment pages, subdomains and other elements on which a reference to this Policy is displayed;

– **"Service"** means the OPayments payment technology service, including the Website, personal accounts, application programming interfaces, payment links and pages, transaction accounting systems, technical support tools and other software and information tools used by the Controller;

– **“Client”** means a foreign legal entity that has connected or applied to connect to the Service for the purpose of accepting and processing payments in connection with the sale of its own goods, works, services, digital products or other products;

– **“User”** means a natural person or legal entity making a payment in favour of a Client using the payment infrastructure available through the Service;

– **“Payment Infrastructure”** means banks, acquiring banks, payment systems, payment providers, payment agents, settlement partners and other persons involved in the processing, confirmation, refunding or disputing of payments;

– **“Technical Data”** means an IP address, browser and operating system data, device type and parameters, language settings, session identifiers, client ID, device fingerprint, network parameters, information about pages visited and actions performed within the Service, referral source, time and duration of use of the Service, and other automatically transmitted technical information;

– **“Cookies”** means small pieces of data stored on a User’s device and used to ensure the proper operation of the Website, retain settings, ensure security and analyse Website traffic and User behaviour;

– **“Cross-Border Transfer”** means the transfer of Personal Data to a recipient located in another country, storage of data on servers located outside the country in which the Data Subject is located, or provision of remote access to data from another country;

– **“Applicable Law”** means mandatory laws and regulations governing the protection of Personal Data, privacy and information security that apply to the Controller, the relevant Processing of Personal Data or the Data Subject, taking into account the place of incorporation and activities of the Controller, the location of the Data Subject, the territory in which the Service is provided and other legally relevant circumstances;

– **“Supervisory Authority”** means a governmental, administrative or other authorised body exercising control and supervision in the field of Personal Data protection in accordance with Applicable Law.

1. GENERAL PROVISIONS

1.1. This Policy sets out the procedure and conditions for the Processing of Personal Data by the Controller in connection with:

1.1.1. visiting and using the Website;

1.1.2. submitting an application for connection to the Service and conducting a review of the applicant;

1.1.3. creating and using a personal account, Access Token and other means of identification;

1.1.4. the Client’s use of the payment, technical, informational and settlement tools of the Service;

1.1.5. initiating, processing, confirming, refunding and disputing payments;

1.1.6. making payouts and maintaining settlement records;

1.1.7. submitting enquiries to technical support, by email, through messengers or via other communication channels;

1.1.8. conducting checks and preventing fraud, abuse and other security threats.

1.2. This Policy is a public document and is published on the Website. The current version of the Policy shall apply to all Processing of Personal Data carried out after it enters into force.

1.3. The Policy has been developed taking into account generally recognised principles of Personal Data protection, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality and accountability of the Controller.

1.4. The Controller shall Process Personal Data only where one or more legal grounds provided for by Applicable Law apply.

1.5. Familiarisation with this Policy shall not, in itself, constitute consent to the Processing of Personal Data where Applicable Law requires the Data Subject's separate, freely given, specific, informed and unambiguous consent.

1.6. Where Personal Data is Processed on the basis of consent, such consent shall be requested separately by means of ticking the relevant box, selecting settings, providing confirmation, signing a document or performing another unambiguous action.

1.7. Depending on the nature of the relevant Processing, the Controller may act as:

1.7.1. an independent controller or equivalent data operator in relation to the data of representatives, employees, officers and beneficial owners of Clients, applicants for connection, Website visitors and persons contacting technical support;

1.7.2. an independent controller or equivalent data operator in relation to data Processed for the purposes of ensuring security, preventing fraud, complying with legal and regulatory requirements, protecting the Controller's rights and maintaining settlement records;

1.7.3. a Processor acting on behalf of the Client in relation to certain User data provided by the Client exclusively for the technical processing of a payment or the performance of other documented instructions of the Client.

1.8. Where the Controller acts as a Processor, the Client shall independently determine the legal grounds and purposes for the initial collection of the relevant Personal Data and shall be responsible for providing Data Subjects with the necessary notices and obtaining consents where required.

1.9. The Controller may engage Processors and other service providers, provided that they assume contractual obligations to comply with confidentiality, security and other requirements of Applicable Law.

1.10. The Controller does not intentionally collect special categories of Personal Data, including data concerning health, racial or ethnic origin, religious or political beliefs, biometric data or genetic data, unless such Processing is expressly required by Applicable Law or is based on a separate legal ground.

2. LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

2.1. Depending on the specific purpose and circumstances, the Controller Processes Personal Data on one or more of the following grounds:

2.1.1. Consent of the Data Subject - where Applicable Law requires consent for a specific purpose, including the use of optional Cookies, receipt of marketing communications or other types of Processing based on the voluntary choice of the Data Subject;

2.1.2. Necessity for entering into or performing a contract - where Processing is necessary for connection to the Service, provision of access, processing of a payment, making of a payout, provision of support or taking steps at the request of the Data Subject prior to entering into a contract;

2.1.3. Compliance with the Controller's legal obligations - including obligations relating to accounting, taxation, financial monitoring, anti-money laundering and counter-terrorist financing, sanctions control, document retention, disclosure of information to competent authorities and compliance with other regulatory requirements;

2.1.4. Legitimate interests of the Controller or third parties - including ensuring the security of the Service, preventing fraud and abuse, reviewing Clients and transactions, protecting the rights and property of the Controller, Clients, Users and the Payment Infrastructure, improving the Service, maintaining internal records and resolving disputes, subject to respect for the rights and legitimate interests of Data Subjects;

2.1.5. Protection of vital interests - in exceptional circumstances where Processing is necessary to prevent an immediate threat to the life or health of the Data Subject or another person;

2.1.6. Performance of a task carried out in the public interest or exercise of official authority - where the relevant ground is provided for by Applicable Law;

2.1.7. Establishment, exercise or defence of legal claims - including claims handling and judicial, arbitral, administrative and other proceedings;

2.1.8. Other grounds expressly provided for by Applicable Law.

2.2. The Data Subject's consent may be expressed, in particular, by:

2.2.1. completing and submitting a form on the Website;

2.2.2. ticking the relevant box in an interface;

2.2.3. selecting Cookie settings;

2.2.4. submitting an enquiry by email or through a messenger;

2.2.5. signing an agreement, application, consent form or other document containing the relevant provision;

2.2.6. performing another unambiguous action which, in the relevant circumstances, confirms the Data Subject's voluntary consent.

2.3. The Data Subject may withdraw consent at any time by submitting a request to the Controller. Withdrawal of consent shall not affect the lawfulness of Processing carried out before such withdrawal and shall not terminate Processing where it may be continued on another legal ground.

2.4. Where Processing is necessary for the performance of a contract or provision of the Service, refusal to provide mandatory data may result in the inability to connect to the Service, process a payment, make a payout, conduct a review or provide the relevant function.

3. PURPOSES, CATEGORIES AND RETENTION PERIODS OF PERSONAL DATA PROCESSING

3.1. Visiting the Website and ensuring its operation

Purposes of Processing: ensuring the availability and proper operation of the Website, configuring the interface, retaining selected settings, diagnosing errors, ensuring information security and protecting against automated attacks.

Categories of data: IP address, browser, operating system and device information, language settings, date and time of visit, referral source, pages viewed, session identifiers, essential Cookies and other Technical Data.

Categories of Data Subjects: Website visitors.

Retention period: for the period necessary to achieve the relevant purpose, investigate incidents and protect the Controller's rights, taking into account the lifetime of Cookies and the requirements of Applicable Law.

3.2. Connection of a Client and provision of access to the Service

Purposes of Processing: reviewing an application, identifying the applicant and its representatives, conducting a review, agreeing the connection terms, creating access to a personal account, maintaining contractual relations and conducting business correspondence.

Categories of data: first name, last name, position, company, business telephone number, email address, messenger identifier, information regarding authority, powers of attorney, corporate and registration documents, links to the Client's websites and projects, communication history and other data provided during connection.

Categories of Data Subjects: representatives, employees, officers and beneficial owners of applicants and Clients.

Retention period: during the review of the application and the relationship with the Client and, following its termination, for the period necessary to comply with legal obligations, resolve disputes and protect the Controller's rights.

3.3. Review of applicants and Clients, risk assessment and sanctions screening

Purposes of Processing: reviewing an application for connection to the Service, confirming the contact details and authority of the Client's representative, reviewing the Client's website, project and declared nature of activities, assessing legal, payment, sanctions-related and reputational risks, and complying with applicable requirements of Payment Infrastructure participants.

Categories of data: first name and last name, if provided; position; name of the represented legal entity; telephone number; email address; messenger identifier, including Telegram or WhatsApp; information regarding the representative's authority; links to the Client's website and other projects; contents of business correspondence; results of checks of publicly available sources, public registers and sanctions lists.

Categories of Data Subjects: representatives and contact persons of applicants and Clients, as well as officers and beneficial owners of Clients solely in respect of information lawfully obtained from publicly available sources, public registers and sanctions lists.

Retention period: during the review of the application and the relationship with the Client and, following its termination, for the period necessary to comply with applicable requirements, resolve disputes, prevent abuse and protect the Controller's rights and legitimate interests.

3.3.1. If, in the future, enhanced identification of the Client, its representatives, officers or beneficial owners becomes mandatory under Applicable Law or the requirements of a bank, payment system or another Payment Infrastructure participant, the Controller may request additional information and documents solely to the extent necessary. Before commencing such Processing, the Controller shall ensure that an appropriate legal ground exists and shall provide the Data Subject with the required information regarding the conditions of Processing.

3.4. Processing of payments and other transactions

Purposes of Processing: initiating and processing payments, redirecting a User to a secure page of a bank or payment provider, receiving and transmitting transaction statuses, maintaining settlement records, processing refunds, resolving payment disputes and preventing duplicate and erroneous transactions.

Categories of data: identifier of the Client and its project, order and transaction identifier, amount, currency, date and time of payment, payment method and route, transaction status, bank and payment provider identifiers, User contact details where entered by the User or provided by a Payment Infrastructure participant, IP address, device and session information, and masked or tokenised payment instrument details where provided by the Payment Infrastructure.

Categories of Data Subjects: Users making payments and representatives of Clients initiating transactions.

Retention period: during the relationship with the Client and, following its termination, for the period necessary for accounting and settlement records, processing refunds and payment disputes, conducting reviews, complying with legal obligations and protecting the Controller's claims.

3.5. Making payouts and maintaining settlement records

Purposes of Processing: processing payout requests, verifying details, transferring amounts due to the Client, maintaining the settlement balance and recording withholdings, reserves, refunds and indebtedness.

Categories of data: contact details and identifiers of the Client's representatives, the Client's banking and other payment details, digital wallet and selected network data where the relevant payout method has been agreed, and information regarding the amount, currency, grounds and status of the payout.

Categories of Data Subjects: representatives and authorised persons of Clients.

Retention period: during the contractual relationship and thereafter for the period necessary to comply with accounting, tax, regulatory and other mandatory requirements and to resolve disputes.

3.6. Processing enquiries and providing technical support

Purposes of Processing: reviewing applications, enquiries, claims and other communications, providing technical and informational support, conducting correspondence and identifying the relevant Client, User or transaction.

Categories of data: first name, last name, company and position, email address, telephone number, messenger identifier, contents of the enquiry, attached documents and files, transaction information and technical metadata of the communication.

Categories of Data Subjects: representatives of Clients, Users, applicants, partners and other persons contacting the Controller.

Retention period: until the purposes of the enquiry have been achieved and thereafter for the period necessary to confirm the contents of communications, perform contractual obligations and protect the Controller's rights.

3.7. Ensuring security and preventing fraud

Purposes of Processing: identifying and preventing fraudulent, illegal, suspicious, unauthorised and high-risk activities, ensuring the security of accounts, Access Tokens, payments and the Payment Infrastructure, and investigating incidents.

Categories of data: IP address, client ID, device fingerprint, device and browser parameters, session identifiers, information regarding logins and actions within the Service, geographical and network parameters, data regarding transactions, declined transactions, refunds, payment disputes, blocking and incidents, correspondence and review results.

Categories of Data Subjects: Website visitors, Users, representatives of Clients and persons whose actions are connected with a potential security breach.

Retention period: for the period necessary to identify and investigate incidents, prevent repeated breaches, comply with Payment Infrastructure requirements and protect the Controller's rights.

3.8. Cookies, web analytics and improvement of the Service

Purposes of Processing: analysing Website traffic and use, assessing the effectiveness of interfaces, identifying errors, improving the Service, ensuring security and generating aggregated statistics.

Categories of data: IP address, Cookie identifiers, client ID, browser and device information, device fingerprint, referral source, pages visited, actions, events, and the time and duration of the session.

Services used: the Controller may use Google Analytics, Yandex Metrica and other analytical systems, information about which is displayed in the Cookie management interface or on the Website.

Categories of Data Subjects: Website visitors and Users of the Service.

Retention period: within the lifetime of the relevant Cookies and the settings of the analytical service. Optional analytical and advertising technologies shall be used on the basis of consent where such consent is required under Applicable Law.

3.9. Informational and marketing communications

Purposes of Processing: sending information regarding operation of the Service, changes to terms, new functions, products, special offers and events, conducting surveys and assessing service quality.

Categories of data: name, company, email address, telephone number, messenger identifier, information regarding delivery, opening and clicking of links, and selected communication settings.

Categories of Data Subjects: representatives of Clients, partners, applicants and other persons who have provided the relevant contact details and necessary consent.

Retention period: until consent is withdrawn or the relevant communications are declined, and for a reasonable period thereafter necessary to document the opt-out.

Service-related, legally significant and security-related notices may be sent irrespective of consent to receive marketing communications.

3.10. Automated Processing and Profiling

3.10.1. The Controller may use Automated Processing and Profiling to assess transaction risks, identify fraud and suspicious behaviour, apply limits, conduct additional checks and protect the Payment Infrastructure.

3.10.2. For these purposes, the Controller may analyse Technical Data, device and session data, the history of transactions, refunds and payment disputes, the frequency and nature of actions, geographical and network parameters and other risk indicators.

3.10.3. Where Applicable Law grants the Data Subject the right not to be subject to decisions based solely on Automated Processing that produce significant legal effects, the Controller shall provide an opportunity to request a review of the decision by an authorised person, express their position and challenge the result.

3.11. Compliance with legal obligations and protection of claims

Purposes of Processing: complying with requirements of laws, competent authorities and the Payment Infrastructure, maintaining accounting and internal records, conducting audits, reviewing claims and establishing, exercising and defending legal claims.

Categories of data: any Personal Data relating to the relevant transaction, agreement, review, enquiry, dispute or legal obligation, to the extent necessary for the specific purpose.

Retention period: for the mandatory retention period and the applicable limitation period, or for a longer period where necessary in connection with an ongoing dispute, review or compliance with a mandatory requirement.

4. COLLECTION, STORAGE, PROTECTION, TRANSFER AND DESTRUCTION OF PERSONAL DATA

4.1. General Processing conditions

4.1.1. The Controller Processes Personal Data by automated and non-automated means to the extent necessary to achieve the stated purposes.

4.1.2. The Controller shall take reasonable measures to ensure that data is accurate and current and may request that it be clarified or confirmed.

4.1.3. Personal Data shall not be retained for longer than necessary for the purposes of Processing, unless a longer period is established by Applicable Law, an agreement, Payment Infrastructure requirements or the need to protect the Controller’s rights.

4.1.4. Once the purposes of Processing have been achieved and the retention periods have expired, the data shall be deleted, destroyed or anonymised, unless its continued retention is required on a lawful basis.

4.2. Processing of bank card data

4.2.1. The Controller does not collect or store full bank card details of Users, including the full card number, expiry date or security code.

4.2.2. Where a card payment method is selected, the User shall be redirected to the secure payment page of an acquiring bank, payment provider or another Payment Infrastructure participant, which shall independently process the bank card details.

4.2.3. The Controller may receive from the Payment Infrastructure limited, masked or tokenised information regarding the payment instrument, a transaction identifier, payment status, the last digits of the card number and other metadata that does not enable the Controller to independently carry out a transaction using the card.

4.2.4. Processing of data on the payment page of a bank or payment provider shall be governed by the privacy policy and terms of the relevant person.

4.3. Personal Data protection measures

4.3.1. The Controller shall take reasonable organisational, technical and physical measures to protect Personal Data against unlawful or accidental access, alteration, disclosure, copying, use, blocking, deletion, destruction, loss and other unlawful actions.

4.3.2. Protection measures may include:

4.3.2.1. separation and control of access to information systems;

4.3.2.2. use of secure communication channels and encryption;

4.3.2.3. event logging and monitoring of suspicious activity;

4.3.2.4. data backup and recovery;

4.3.2.5. software updates and remediation of vulnerabilities;

4.3.2.6. internal privacy and information security policies;

4.3.2.7. restriction of employee and contractor access on a need-to-know basis;

4.3.2.8. contractual requirements applicable to Processors and service providers.

4.3.3. Where a Personal Data security breach is identified, the Controller shall take measures to contain the incident, assess its consequences, eliminate its causes and prevent a recurrence.

4.3.4. The Controller shall notify the Supervisory Authority and affected Data Subjects in the cases and within the procedure and time limits provided by Applicable Law.

4.4. Recipients of Personal Data

4.4.1. The Controller may transfer Personal Data to the following categories of recipients:

4.4.1.1. banks, acquirers, payment systems, payment providers, payment agents and other Payment Infrastructure participants;

4.4.1.2. providers of hosting, cloud infrastructure, software, CRM systems, communications and technical support;

4.4.1.3. providers of information security, fraud prevention, identification and verification systems;

4.4.1.4. providers of web analytics, Cookies and marketing platforms where the necessary legal ground exists;

4.4.1.5. auditors, accountants, legal, tax and other professional advisers;

4.4.1.6. affiliates and contractors of the Controller participating in the provision of the Service;

4.4.1.7. governmental, judicial, law enforcement, tax, financial and other competent authorities where a lawful request exists;

4.4.1.8. a purchaser of the business, assets or rights relating to the Service in the event of a reorganisation, sale, investment or other corporate transaction, subject to compliance with confidentiality requirements;

4.4.1.9. other persons with the consent of the Data Subject or on another ground provided for by Applicable Law.

4.4.2. The Controller does not sell Personal Data for monetary consideration. Where a particular transfer of data for analytics or targeted advertising is deemed to constitute a sale or sharing of data under Applicable Law, the Data Subject shall be provided with the right to opt out of such transfer in the cases provided by law.

4.5. Cross-Border Transfer

4.5.1. Due to the international nature of the Service, Personal Data may be Processed and stored in countries other than the country in which the Data Subject is located.

4.5.2. Cross-Border Transfers shall be carried out where one or more legally recognised mechanisms apply, including:

4.5.2.1. recognition that the recipient country provides an adequate level of protection;

4.5.2.2. execution of standard contractual clauses or other contractual safeguards;

4.5.2.3. application of binding corporate rules;

4.5.2.4. obtaining the Data Subject's separate consent after providing the necessary information regarding the risks;

4.5.2.5. the necessity of the transfer for entering into or performing a contract;

4.5.2.6. the necessity of the transfer for establishing, exercising or defending legal claims;

4.5.2.7. another ground provided for by Applicable Law.

4.5.3. Where the laws of the country in which the Data Subject is located impose additional requirements on Cross-Border Transfers, the Controller shall comply with such requirements to the mandatory extent.

4.6. Sources of Personal Data

4.6.1. The Controller may obtain Personal Data:

4.6.1.1. directly from the Data Subject;

4.6.1.2. from the Client, including in relation to its representatives, employees, officers, beneficial owners and Users;

4.6.1.3. from banks, payment systems, payment providers and other Payment Infrastructure participants;

4.6.1.4. from publicly available sources, public registers, sanctions lists and other screening lists;

4.6.1.5. through the Website, Cookies, analytical systems and technical systems;

4.6.1.6. from representatives and authorised persons of the Data Subject;

4.6.1.7. from other lawful sources permitted by Applicable Law.

4.6.2. A Client transferring Personal Data of third parties to the Controller confirms that it has the necessary authority and legal grounds for such transfer.

5. RIGHTS OF DATA SUBJECTS AND OBLIGATIONS OF THE PARTIES

5.1. Rights of the Data Subject

5.1.1. To the extent provided for by Applicable Law, the Data Subject shall have the right to:

5.1.1.1. obtain confirmation as to whether their Personal Data is being Processed;

5.1.1.2. obtain information regarding the purposes, legal grounds, categories of data, recipients and duration of Processing;

5.1.1.3. obtain access to their Personal Data and a copy thereof;

5.1.1.4. request clarification, rectification or updating of inaccurate or incomplete data;

5.1.1.5. request deletion of Personal Data where there are no grounds for its continued Processing;

5.1.1.6. request restriction of Processing in the cases provided by law;

5.1.1.7. object to Processing based on a legitimate interest, subject to the exceptions provided by law;

5.1.1.8. object at any time to the use of data for direct marketing;

5.1.1.9. withdraw previously provided consent;

5.1.1.10. receive data in a structured, commonly used and machine-readable format and request its transfer to another controller where technically feasible;

5.1.1.11. request review of a decision based exclusively on Automated Processing where such decision materially affects the rights and interests of the Data Subject;

5.1.1.12. opt out of the sale or sharing of data and targeted advertising where the relevant right is provided for by Applicable Law;

5.1.1.13. lodge a complaint with the competent Supervisory Authority and seek judicial protection.

5.1.2. To exercise their rights, the Data Subject shall submit a request using the contact details specified in Section 8 of the Policy.

5.1.3. The request shall contain information enabling the identification of the applicant and the relevant data. The Controller may request additional proof of identity to prevent unauthorised access.

5.1.4. The Controller shall consider the request within the period established by Applicable Law. Where no mandatory period is established, a response shall generally be provided within 30 calendar days after receipt of the complete request and confirmation of identity.

5.1.5. The period may be extended in the cases provided by Applicable Law, subject to notifying the Data Subject of the reasons for the extension.

5.1.6. The Controller may refuse to satisfy a request in whole or in part where continued Processing is required to comply with a legal obligation, prevent fraud, ensure security, perform a contract, defend legal claims or on another lawful ground.

5.2. Obligations of the Controller

5.2.1. The Controller shall:

5.2.1.1. Process Personal Data lawfully, fairly and transparently;

5.2.1.2. use data only for specified and compatible purposes;

5.2.1.3. limit the categories and scope of data to what is necessary for the relevant purposes;

5.2.1.4. take reasonable measures to ensure that data is accurate and current;

5.2.1.5. apply organisational and technical protection measures;

5.2.1.6. ensure the confidentiality of data;

5.2.1.7. enter into the necessary agreements with Processors;

5.2.1.8. consider requests from Data Subjects in the manner provided by Applicable Law;

5.2.1.9. cease Processing and delete or anonymise data where the legal ground for its continued Processing has ceased to exist;

5.2.1.10. cooperate with competent Supervisory Authorities.

5.3. Obligations of the Data Subject

5.3.1. The Data Subject shall:

5.3.1.1. provide accurate, complete and current information;

5.3.1.2. promptly notify the Controller of changes to the data;

5.3.1.3. not transfer Personal Data of third parties without the necessary authority and legal grounds;

5.3.1.4. comply with security requirements when using the Service;

5.3.1.5. immediately notify the Controller of compromised account credentials, unauthorised access or a suspected data breach.

6. LIABILITY

6.1. The Controller shall be liable for breaches of Personal Data Processing requirements in the cases and to the extent provided by Applicable Law.

6.2. The Data Subject may claim compensation for damage caused by unlawful Processing of Personal Data in the manner and to the extent established by Applicable Law.

6.3. The Controller shall not be liable for consequences caused by inaccurate, incomplete, outdated or unlawfully obtained information provided by the Data Subject or the Client.

6.4. The Controller shall not be liable for the Processing of Personal Data by third parties to whom the Data Subject has independently provided the relevant data, or for external websites, applications and services to which the Data Subject is redirected from the Website.

6.5. The Controller shall not be liable for the actions of a bank, payment provider or another Payment Infrastructure participant that independently determines the purposes and means of Processing Personal Data on its side.

6.6. No provision of this Policy shall limit any mandatory rights of Data Subjects or liability of the Controller that cannot be limited under Applicable Law.

7. FINAL PROVISIONS

7.1. This Policy shall be governed by Applicable Law. Where mandatory rules of several countries apply to particular Processing, the relevant rules shall apply to the mandatory extent.

7.2. The Controller may amend the Policy in connection with changes to laws, the structure or functionality of the Service, the composition of Processors, the purposes and methods of Processing or the Controller’s internal procedures.

7.3. A new version of the Policy shall enter into force upon its publication on the Website, unless another effective date is expressly specified in the new version.

7.4. Material changes affecting the purposes of Processing, the categories of data or the rights of Data Subjects may additionally be communicated to Data Subjects through the Website, personal account, email or another available channel.

7.5. Where separate consent is required for a new purpose, the Controller shall request such consent before commencing the relevant Processing.

7.6. In the event of any conflict between this Policy and an agreement entered into with a Client, the provisions of the agreement shall apply to the relationship between the parties to the extent that they do not restrict the mandatory rights of Data Subjects.

7.7. The Service is not intended for independent use by persons who have not reached the age at which they may independently provide consent and perform the relevant actions in accordance with Applicable Law.

7.8. The Controller does not intentionally collect Personal Data of children without the consent of a parent, guardian or other legal representative where such consent is required. Where unlawfully obtained data of a child is identified, the Controller shall take measures to cease Processing and delete the data, unless its continued retention is required by law.

7.9. The effective date of the Policy shall be the date of its publication on the Website.

Document version: 1.0
Date of last update: 27.07.2026.

8. CONTROLLER DETAILS

Controller: OSOLUTION LIMITED
Company Registration Number: 80210378
Jurisdiction of Incorporation: HONG KONG
Registered Address: 7/F MW TOWER 111 BONHAM STRAND SHEUNG WAN HONG KONG
Correspondence Address: 7/F MW TOWER 111 BONHAM STRAND SHEUNG WAN HONG KONG
Website: https://opayments.io
Email Address: customer@opayments.io