PRIVACY POLICY

GENERAL

FileStreamTech OÜ ("Company", "we", "our", or "us") takes the protection of personal data seriously. We are fully committed to handling personal information in compliance with all applicable data protection laws – including GDPR provisions, their implementing regulations, and internationally recognised privacy standards for payment infrastructure providers. If you reside in certain countries, we may process your Personal Information differently to comply with applicable privacy laws in those jurisdictions.

This Privacy Policy describes how we collect, use, disclose, transfer, store, and otherwise process personal data when individuals: visit or use our website; engage with our payment processing infrastructure; use our platforms or related technical services (collectively referred to as the "Services"); contact us in the context of business relationships or commercial transactions.

Please note that this Privacy Policy applies solely to the Company's own services. It does not extend to third-party services, merchant environments, acquiring institutions, issuing banks, payment method providers, or any other external platforms that integrate with our Services but operate independently.
Our website at ***junbipay.com*** (the "Site") may include links to third-party websites. Those websites are independently operated and governed by their own privacy policies. We bear no responsibility for their content, data practices, or privacy frameworks.

We may update this Privacy Policy from time to time. Any changes will be published on our website, and the revised version will take effect as of the stated effective date.

PERSONAL DATA WE COLLECT

We may collect and process the following categories of personal data:

Contact and identification data including your name, surname, email address, telephone number, date of birth, country of residence, address details, and other identification information you may provide to us or that we may be required to collect for compliance purposes.

Transaction-related data where you act as a payer, beneficiary, or authorised representative of a merchant, including billing and delivery details, transaction amount and date, transaction reference numbers, merchant identifiers, payment instrument metadata, masked card identifiers, and, where required for processing, bank account information.

Compliance and verification data processed where required under applicable AML/CFT legislation or payment scheme rules, including identity verification information, sanctions screening results, politically exposed person (PEP) indicators, fraud and risk assessment signals, publicly available registry data, and, where permitted by law, credit reference or fraud prevention datasets.

Technical, device, and usage data including your IP address, logs relating to your use of our Services, device fingerprinting data, firewall and system logs, session metadata, browser and operating system information, usage activity, behavioural transaction signals, and IP intelligence indicators.

Communication and operational data including records of correspondence with us, telephone call records, CCTV and access control data where applicable, and any personal data you may disclose during your interactions with us.

Third-party and external source data including information we may receive from merchants, business partners, service providers, subcontractors, and other authorised or publicly available sources.

Marketing-related data where permitted under applicable law, including identity and contact information obtained from publicly available professional directories or authorised commercial data sources.

We collect personal data through direct interaction, automated technologies, merchants, payment participants and authorised third-party service providers.

HOW WE USE PERSONAL DATA

We process personal data only where necessary for legitimate business and operational purposes, including the following:

Service provision and account administration to enable access to our infrastructure, administer user or merchant accounts, ensure service continuity, support transaction execution, and provide technical assistance.

Transaction processing and settlement to route payment instructions, communicate with relevant participants in the payment ecosystem, facilitate settlement workflows, and provide transaction-related support.

Regulatory and compliance obligations to comply with applicable AML/CFT laws, sanctions requirements, payment scheme rules, and instructions issued by competent supervisory authorities.

Fraud prevention and system security to detect and prevent suspicious or unauthorised activity, investigate misuse of the Services, protect users and merchants, and maintain the integrity and security of the platform.

Communication and operational updates to respond to enquiries, provide customer support, send service-related notifications, technical alerts, and policy or operational updates.

Dispute management and contract enforcement to investigate claims or complaints, resolve disputes, enforce contractual terms, and where necessary, recover outstanding amounts.

Analytics and service improvement to analyse usage of the Services, monitor performance, improve infrastructure, optimise user experience, and develop or enhance products and functionalities.

Marketing and informational communications where permitted by applicable law, to send newsletters, product or service updates, announcements, and promotional materials. Recipients may opt out of such communications at any time.

DISCLOSURE OF PERSONAL DATA

We may share personal data with selected third parties where this is necessary for the purposes described above.

Payment ecosystem participants such as acquiring institutions, issuing banks, card schemes, payment method providers, and settlement partners, where disclosure is required to facilitate and complete transactions. Only the data strictly necessary for transaction execution is shared.

Compliance and verification service providers, including identity verification providers, AML monitoring and sanctions screening services, and fraud prevention partners, where such processing is required for regulatory compliance and risk management purposes.

Technical and infrastructure service providers, including providers of hosting, cybersecurity monitoring, analytics, communication tools, and IT infrastructure maintenance, all of whom are bound by appropriate confidentiality and data protection obligations.

Payment scheme operators, where personal data is processed in accordance with the applicable operating rules of relevant payment networks, including international card schemes.

Corporate transaction and restructuring contexts, including situations involving mergers, acquisitions, financing arrangements, asset transfers, or other forms of corporate reorganisation, where personal data may form part of the transferred business assets.

Legal and regulatory disclosures, where we are required to disclose personal data under applicable law, regulatory requirements, court orders, or requests from law enforcement or supervisory authorities, or where disclosure is necessary to protect our legal rights, prevent fraud, or mitigate harm.

YOUR RIGHTS

Subject to applicable data protection laws, you may have certain rights in relation to your personal data, including the right to request access to the data we hold about you, to request correction of inaccurate or incomplete information, and to request deletion of your personal data where applicable. You may also have the right to request restriction of processing or to object to certain types of processing, as well as the right to data portability where legally applicable.
Where processing is based on your consent, you may withdraw such consent at any time. You may also have the right to request human review of decisions made solely by automated means, where such decisions produce legal or similarly significant effects.

Please note that these rights may be limited where processing is necessary for compliance with legal or regulatory obligations applicable to payment service providers or where other lawful grounds for processing apply.

AML AND SANCTIONS CONTROLS

Where required by applicable laws and payment network rules, we may process personal data through authorised compliance and screening providers to support anti-financial crime controls, including identity verification, sanctions screening, transaction risk assessment, detection of unusual or suspicious activity, and prevention of financial crime.

INTERNATIONAL DATA TRANSFERS

Given the international nature of our Services and supporting infrastructure, personal data may be transferred to and processed in countries outside the European Economic Area (EEA).
Where such transfers occur, we ensure that appropriate safeguards are in place in accordance with applicable data protection law, including the GDPR. These safeguards may include transfers to countries that are subject to an adequacy decision by the European Commission, the use of standard contractual clauses approved by the European Commission, and the implementation of additional technical and organisational measures where required to ensure an adequate level of protection of personal data.
We may also apply other legally recognised transfer mechanisms where appropriate under applicable law.

DATA PROTECTION AND SECURITY

We apply appropriate technical and organisational measures to protect personal data against unauthorised access, accidental loss, unlawful disclosure, alteration, or destruction. These measures may include encrypted communications, network security controls such as firewalls, access restriction mechanisms, system monitoring tools, and internal confidentiality obligations. Where required by law, we will notify relevant authorities and affected individuals of any personal data breach.

DATA RETENTION

Personal data is retained only for as long as necessary for the purposes for which it was collected, including the provision of Services, compliance with legal and regulatory obligations, dispute resolution, accounting and record-keeping requirements, and the enforcement of contractual rights. Retention periods are determined based on factors such as transaction history, AML and regulatory requirements, statutory limitation periods, and operational needs. Where appropriate, data may be anonymised for analytical or statistical purposes. This means that in the event where you cease to use our Services, we may still retain certain personal data for up to 7 years in order to carry out our obligations.

COOKIES

We use cookies to recognise you as a user and distinguish you from other users of our application. This enables us to ensure a consistent user experience and to analyse and improve the performance and functionality of the application.

SECURITY

All information you provide to us is stored on secure servers, and we apply appropriate technical, organisational, and administrative safeguards to protect your personal data. Once received, we implement strict security procedures and controls designed to prevent unauthorised access, disclosure, or misuse.
However, please be aware that no method of transmission over the internet and no storage system can be guaranteed to be completely secure. If you have any reason to believe that your interaction with us is no longer secure, you should contact us without delay.

CONTACTS

Requests concerning the processing of personal data or the exercise of privacy rights can be submitted using the contact details provided on our website - ***junbipay.com***

FileStreamTech OÜ（以下「当社」、「弊社」、「私たち」）は、個人データの保護を重要視しています。当社は、GDPR、その施行規則、および決済インフラ提供者に適用される国際的に認められたプライバシー基準を含む、適用されるすべてのデータ保護法令を遵守して個人情報を取り扱うことを全面的に約束します。お客様がお住まいの国によっては、当該法域で適用されるプライバシー法に準拠するため、当社による個人情報の処理方法が異なる場合があります。

本プライバシーポリシーは、個人が以下の場合において、当社がどのように個人データを収集、利用、開示、移転、保存、その他処理するかを説明するものです：当社ウェブサイトを訪問または利用する場合；当社の決済処理インフラを利用する場合；当社のプラットフォームまたは関連する技術サービス（総称して「本サービス」）を利用する場合；事業関係または商取引の文脈で当社に連絡する場合。

なお、本プライバシーポリシーは当社自身のサービスにのみ適用されます。第三者サービス、加盟店環境、アクワイアリング機関、発行銀行、決済手段提供者、または当社サービスと連携しつつも独立して運営されるその他外部プラットフォームには適用されません。
当社ウェブサイト junbipay.com（以下「本サイト」）には、第三者ウェブサイトへのリンクが含まれる場合があります。これらのウェブサイトは独立して運営されており、それぞれ独自のプライバシーポリシーに従っています。当社は、それらのコンテンツ、データ取扱慣行、またはプライバシー体制について一切責任を負いません。

当社は、本プライバシーポリシーを随時更新する場合があります。変更がある場合は当社ウェブサイト上で公表され、改訂版は記載された発効日より効力を有します。

当社が収集する個人データ

当社は、以下の種類の個人データを収集および処理する場合があります。

連絡先および識別データ
氏名、メールアドレス、電話番号、生年月日、居住国、住所情報、およびお客様が当社に提供するその他の識別情報、または法令遵守目的で当社が収集を求められる情報。

取引関連データ
お客様が支払人、受取人、または加盟店の権限ある代表者として行動する場合の、請求先・配送先情報、取引金額および日付、取引参照番号、加盟店識別子、決済手段メタデータ、マスク化されたカード識別情報、および処理上必要な場合の銀行口座情報。

コンプライアンスおよび確認データ
適用されるAML/CFT法令または決済スキーム規則に基づき必要な場合に処理される、本人確認情報、制裁スクリーニング結果、PEP（重要な公的地位を有する者）指標、不正およびリスク評価シグナル、公的登録データ、ならびに法律上許容される場合の信用情報または不正防止データセット。

技術・デバイス・利用データ
IPアドレス、本サービス利用に関するログ、デバイスフィンガープリンティングデータ、ファイアウォールおよびシステムログ、セッションメタデータ、ブラウザおよびOS情報、利用活動、行動ベースの取引シグナル、IPインテリジェンス指標。

通信および運用データ
当社との通信記録、電話通話記録、必要に応じたCCTVおよびアクセス管理データ、ならびにお客様が当社とのやり取りの中で開示する個人データ。

第三者および外部ソースデータ
加盟店、ビジネスパートナー、サービス提供者、下請業者、その他認可された情報源または公開情報源から受領する情報。

マーケティング関連データ
適用法令で認められる範囲において、公開されている専門ディレクトリまたは認可された商業データソースから取得される氏名および連絡先情報。

当社は、直接的なやり取り、自動化技術、加盟店、決済参加者、および認可された第三者サービス提供者を通じて個人データを収集します。

個人データの利用目的

当社は、正当な事業目的および運営目的のために必要な場合に限り、個人データを処理します。これには以下が含まれます。

サービス提供およびアカウント管理
当社インフラへのアクセス提供、ユーザーまたは加盟店アカウントの管理、サービス継続性の確保、取引実行の支援、技術サポートの提供。

取引処理および決済
決済指示のルーティング、決済エコシステム内の関係者との通信、決済ワークフローの促進、取引関連サポートの提供。

法令およびコンプライアンス義務
AML/CFT法令、制裁要件、決済スキーム規則、および監督当局からの指示への対応。

不正防止およびシステムセキュリティ
不審または不正な活動の検出・防止、本サービスの不正利用調査、ユーザーおよび加盟店の保護、プラットフォームの完全性と安全性の維持。

通信および運用上の通知
問い合わせ対応、カスタマーサポート、サービス関連通知、技術アラート、ポリシーまたは運用上の更新通知の送信。

紛争管理および契約執行
請求または苦情の調査、紛争解決、契約条件の執行、必要に応じた未払金の回収。

分析およびサービス改善
本サービス利用状況の分析、パフォーマンス監視、インフラ改善、ユーザー体験最適化、製品および機能の開発・改善。

マーケティングおよび情報提供
適用法令で許可される範囲において、ニュースレター、製品・サービス更新情報、告知、販促資料の送付。受信者はいつでもこれらの配信を停止できます。

個人データの開示

当社は、上記目的達成のため必要な場合に、選定された第三者と個人データを共有する場合があります。

決済エコシステム参加者
アクワイアリング機関、発行銀行、カードスキーム、決済手段提供者、決済パートナーなど、取引完了のために必要な範囲で情報を共有します。共有されるのは取引実行に必要最小限のデータのみです。

コンプライアンスおよび確認サービス提供者
本人確認、AML監視、制裁スクリーニング、不正防止サービス提供者など、法令遵守およびリスク管理のために必要な場合。

技術およびインフラサービス提供者
ホスティング、サイバーセキュリティ監視、分析、通信ツール、ITインフラ保守提供者など。これらの事業者は適切な機密保持およびデータ保護義務を負います。

決済スキーム運営者
国際カードスキームを含む決済ネットワークの運営規則に従って個人データが処理される場合。

企業取引および組織再編
合併、買収、資金調達、資産譲渡、その他組織再編の際、個人データが移転対象資産に含まれる場合。

法的および規制上の開示
法令、規制要件、裁判所命令、法執行機関または監督当局からの要請に基づく場合、または当社の法的権利保護、不正防止、損害軽減のため必要な場合。

お客様の権利

適用されるデータ保護法に基づき、お客様は自身の個人データに関して一定の権利を有する場合があります。これには、当社が保有するデータへのアクセス請求、不正確または不完全な情報の修正請求、適用可能な場合の個人データ削除請求が含まれます。また、処理制限請求、特定の処理への異議申立て、法的に適用される場合のデータポータビリティ権を有する場合があります。

処理がお客様の同意に基づく場合、お客様はいつでもその同意を撤回できます。また、法的または同等に重大な影響を及ぼす完全自動化された意思決定について、人による審査を求める権利を有する場合があります。

ただし、これらの権利は、決済サービス提供者に適用される法令または規制上の義務遵守のために処理が必要な場合、またはその他適法な処理根拠が存在する場合には制限されることがあります。

AMLおよび制裁管理

適用法令および決済ネットワーク規則に基づき必要な場合、当社は認可されたコンプライアンスおよびスクリーニング提供者を通じて個人データを処理し、本人確認、制裁スクリーニング、取引リスク評価、異常または疑わしい活動の検出、金融犯罪防止などの金融犯罪対策を支援する場合があります。

国際データ移転

本サービスおよび関連インフラの国際的性質により、個人データは欧州経済領域（EEA）外の国へ移転および処理される場合があります。

その場合、当社はGDPRを含む適用データ保護法に従い、適切な保護措置を講じます。これには、欧州委員会による十分性認定を受けた国への移転、欧州委員会承認の標準契約条項（SCC）の利用、ならびに必要に応じた追加的技術的・組織的措置の実施が含まれます。

また、適用法令に基づき認められるその他の移転メカニズムを採用する場合があります。

データ保護およびセキュリティ

当社は、個人データを不正アクセス、偶発的損失、不法開示、改ざん、破壊から保護するため、適切な技術的および組織的措置を講じます。これには、暗号化通信、ファイアウォール等のネットワークセキュリティ制御、アクセス制限、システム監視ツール、内部機密保持義務など

が含まれる場合があります。法律上必要な場合、当社は関連当局および影響を受ける個人に対し、個人データ侵害を通知します。

データ保持

個人データは、収集目的達成に必要な期間に限り保持されます。これには、本サービス提供、法令・規制義務遵守、紛争解決、会計・記録保持義務、契約上の権利執行が含まれます。保持期間は、取引履歴、AMLおよび規制要件、法定時効期間、運営上の必要性などを考慮して決定されます。適切な場合、データは分析または統計目的のため匿名化される場合があります。したがって、お客様が本サービス利用を終了した場合でも、当社義務履行のため、一定の個人データを最大7年間保持する場合があります。

Cookie（クッキー）

当社は、お客様をユーザーとして認識し、他のユーザーと区別するためにCookieを使用します。これにより、一貫したユーザー体験を提供し、アプリケーションの性能および機能を分析・改善することが可能となります。

セキュリティ

お客様から提供されたすべての情報は安全なサーバーに保存され、当社は個人データ保護のため適切な技術的、組織的、管理的安全措置を講じます。情報受領後、当社は不正アクセス、開示、または不正利用を防止するため厳格なセキュリティ手順および管理体制を実施します。

ただし、インターネット上での送信方法および保存システムのいずれも完全な安全性を保証できるものではありません。当社とのやり取りが安全でなくなったと考える理由がある場合は、遅滞なく当社までご連絡ください。

お問い合わせ

個人データ処理またはプライバシー権行使に関するご要望は、当社ウェブサイト junbipay.com に記載された連絡先を通じて提出することができます。