PRIVACY NOTICE

This is the privacy notice of VarsoviaFX Ltd (VFX) and in this document, “we”, “our”, or “us” refer to VFX. For the purposes of UK data protection law, VarsoviaFX Ltd is the Data Controller.

We are a company registered in England and Wales under company number 08746313. Our registered office is at Regus, 79 College Road, Harrow, England, HA1 1BD. Our Data Protection Officer is Robert Kaczmarek and can be contacted at robert.kaczmarek@varsoviafx.com. General privacy and data subject rights enquiries may also be sent to bok@varsoviafx.com.

Introduction

1. This Privacy Notice explains how we collect, use, disclose, retain and protect personal data in connection with our website and our money transfer services. “Personal data” means information relating to an identified or identifiable individual.
2. This Notice applies to our customers and prospective customers, beneficiaries or recipients of transfers, visitors to our website, and other individuals who contact us or whose personal data is provided to us in connection with a payment or compliance obligation.
3. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended, including by the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 (PECR) where applicable.
4. We do not sell personal data. We disclose personal data only where necessary for the purposes described in this Notice, where required or permitted by law, or where you have given a valid consent.

Information we collect and where it comes from

Depending on how you use our services, we may process identity and contact information; account and authentication information; transaction information; beneficiary name and bank account details; information required for customer due diligence (CDD) or enhanced due diligence (EDD), including identity documents and source-of-funds evidence where required; payment-related information such as a payment token, masked card details, transaction reference and status; correspondence, complaints and customer service records; call recordings where applicable; website, device, IP address, session and security-log information; and marketing preferences.

We obtain personal data directly from you, from a customer who provides beneficiary information, from identity verification and screening providers, public registers and publicly available sources, payment service providers and banks, and from competent authorities where it is lawful and relevant to do so. Where we obtain personal data from another source, we use it only for the relevant service, verification, compliance, security or legal purpose.

Some information is required in order for us to enter into or perform a contract with you. Other information is required by law, including for identity verification, anti-money laundering, sanctions, transaction-monitoring and record-keeping purposes. If you do not provide information that is required, we may be unable to open or maintain your account, process a transaction, or continue providing the service.

The bases on which we process information about you

We identify a lawful basis for each purpose for which we process personal data. The lawful basis may differ depending on the information and the purpose. The principal bases relevant to our services are contract, legal obligation, legitimate interests and consent.

1. Information we process because we have a contractual obligation with you

When you create an account, agree to our Terms and Conditions or ask us to take steps before entering into a contract, we process information that is necessary to provide the requested service. This includes administering your account, authenticating you, receiving and processing your payment instruction, calculating and displaying transaction information, facilitating payout in Poland, providing transaction information and customer support, and dealing with cancellations, rejections or other operational matters.

For these purposes we rely on Article 6(1)(b) UK GDPR. We do not rely on consent where the processing is necessary to perform our contract with you.

2. Information we process because we have a legal obligation

As a payment service provider and money service business, we are subject to legal and regulatory obligations. We process personal data where necessary to verify identity, carry out CDD and EDD, screen for sanctions and politically exposed person (PEP) risk, monitor transactions, prevent and investigate financial crime, keep required records, respond to lawful requests from regulators and public authorities, and meet other statutory obligations.

For these purposes we principally rely on Article 6(1)(c) UK GDPR. We may have to retain or disclose information even after a customer relationship ends where the law requires us to do so.

3. Information we process for our legitimate interests

We may process personal data where this is necessary for our legitimate interests or those of a third party and those interests are not overridden by your rights and interests. These interests include maintaining the security and integrity of our systems, preventing or detecting fraud beyond specific legal obligations, protecting customers and the Company, managing and improving our services, administering our business, and establishing, exercising or defending legal claims.

Where we rely on legitimate interests, we consider the purpose, necessity and impact of the processing and apply proportionate safeguards. You may object to processing based on legitimate interests as explained below.

4. Information we process with your consent

We rely on consent only where consent is an appropriate lawful basis, for example for certain direct marketing communications and for non-essential cookies or similar technologies where consent is required by PECR.

You may withdraw your consent at any time. Withdrawal does not affect processing that took place before consent was withdrawn and does not affect processing that we carry out on another lawful basis, such as contract or legal obligation. You can withdraw marketing consent by using the unsubscribe method provided or by contacting us.

5. Identity verification, AML, sanctions and transaction monitoring

We carry out identity verification and financial-crime controls at onboarding and during the customer relationship. Depending on the circumstances, this may include electronic identity checks, CDD or EDD, sanctions and PEP screening, transaction monitoring, review of transaction patterns and links, and requests for additional information or supporting evidence such as proof of address or source of funds.

We use automated systems to perform screening and to identify alerts or activity requiring review. Alerts are reviewed by authorised personnel, including Compliance and the MLRO, before decisions are taken where human review is required. We may delay, suspend or decline a transaction, request further information, or take other steps where required by law, our regulatory obligations or our Terms and Conditions.

Our systems are designed to support compliance review rather than to make, as a general practice, solely automated decisions that produce legal or similarly significant effects without appropriate human involvement. Third-party payment or verification providers may operate their own risk controls under their own legal responsibilities and privacy information.

6. Information relating to your method of payment

Card payment information is processed through specialist payment service providers and acquiring banks. VarsoviaFX does not store complete debit or payment card details in its own customer database. Where supported by the payment service, we may receive and retain a payment token, masked card information such as the last four digits, a transaction reference, payment status and other information necessary to identify, reconcile and support the payment.

We use payment-related information only for purposes such as processing your instruction, confirming or reconciling payment, preventing unauthorised use, dealing with refunds or failed payments, responding to queries and meeting legal or regulatory obligations.

Payment service providers and acquiring banks may process personal data as independent controllers for their own fraud-prevention, security, payment-network and regulatory purposes. Their own privacy notices apply to such processing.

7. Your rights under data protection law

Depending on the circumstances and the lawful basis we rely on, you may have the right to access your personal data, have inaccurate data corrected, request erasure, request restriction of processing, object to processing, receive certain data in a portable format, and withdraw consent where consent is the lawful basis. You also have the right to make a data protection complaint to us and to complain to the Information Commissioner's Office (ICO).

These rights are not absolute. In particular, we may need to continue processing or retaining information where this is required by anti-money laundering, payment services, tax, regulatory or other legal obligations, or where information is required for legal claims.

Your right to object

You have the right to object to processing based on legitimate interests. We will stop that processing unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is required for legal claims. You may object to direct marketing at any time and, where you do so, we will stop using your personal data for direct marketing.

8. Access to your personal information

You may make a subject access request verbally or in writing. Requests may be sent to bok@varsoviafx.com or to our Data Protection Officer. We will respond without undue delay and normally within one month after the applicable time limit begins.

Where permitted by law, the time limit may be extended by up to a further two months because of the complexity or number of requests. If clarification is reasonably required in order to respond effectively, the response period may be paused while we await that clarification. In most circumstances no fee is charged. A reasonable fee may be charged only where permitted by law, for example for a manifestly unfounded or excessive request or for further copies.

9. Erasure and restriction of your information

You may ask us to erase or restrict your personal data where the relevant legal conditions are met. Closing or deleting an online account does not necessarily require us to erase underlying records that we must retain by law. We may refuse or limit an erasure request where retention is necessary for legal or regulatory compliance, the establishment, exercise or defence of legal claims, or another applicable exemption.

10. Verification of your identity

Before responding to a data protection rights request, we may take reasonable and proportionate steps to confirm your identity or the authority of a person acting on your behalf. We will ask only for information that is necessary for this purpose.

11. Sending a message to our support team and call recordings

When you contact us by telephone, email, website or another approved channel, we process the information you provide, together with our response and relevant account or transaction information, in order to answer your enquiry, provide support, maintain an appropriate business record and, where relevant, establish or defend legal rights.

Customer service calls may be recorded for service, quality, security, complaint-handling and compliance purposes. Where card details are collected by telephone, recording is excluded or paused where configured for card-data capture. Call recordings are handled in accordance with our retention and security controls.

12. Complaints and data protection complaints

When we receive a complaint, we record the information necessary to investigate and resolve it. Complaint information may include contact details, account or transaction references, correspondence, investigation notes, evidence and the outcome.

If you believe we have infringed data protection law in relation to your personal data, you may make a data protection complaint to us by contacting our Data Protection Officer at robert.kaczmarek@varsoviafx.com or by emailing bok@varsoviafx.com and making clear that your concern is a data protection complaint. We will facilitate the making of complaints, acknowledge receipt within 30 days, take appropriate steps to investigate and keep you informed where appropriate, and communicate the outcome without undue delay.

If you remain dissatisfied, you may complain to the Information Commissioner's Office. The ICO can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, telephone 0303 123 1113, or through www.ico.org.uk/make-a-complaint.

13. Cookies

Our website uses cookies and similar technologies. Strictly necessary technologies may be used where required for the operation, security or authentication of the service. Where PECR requires consent for a non-essential cookie or similar technology, we will seek your consent before using it.

You can manage your choices through the cookie controls made available on our website and through your browser settings. Refusing non-essential cookies should not prevent use of the core service, although some optional functionality may be affected.

Further information about the cookies and similar technologies used on our website, including their purposes and duration, is set out in our Cookie Policy.

14. Personal identifiers from your browsing activity

When you use our website, our systems may record technical information such as your IP address, browser and device information, session or authentication events, pages or functions used, approximate location derived from technical data, and security events. This information may be linked to your account where necessary for security, fraud prevention, authentication, investigation or support.

We use this information to operate and secure our website, understand service performance, investigate suspicious activity and improve usability. Website, registration and security logs are retained only for the period justified by their operational or security purpose, subject to the retention section below.

15. Direct marketing

We may send you marketing by email or text only where we have a lawful basis to do so and the requirements of PECR are met. Where we rely on consent, you may withdraw it at any time. Every electronic marketing communication will provide an appropriate way to opt out.

We do not sell personal data or disclose it to third parties for their own direct marketing without a lawful basis. We may keep the minimum information necessary to record an opt-out or objection so that we can continue to respect your preference.

16. Disclosure of your information

We may share personal data with categories of recipients where necessary for the purposes described in this Notice. These may include card payment gateways and acquiring banks; banks and payment partners used to facilitate payout in Poland; identity verification, sanctions and screening providers; hosting, IT, communications and security providers; authorised agents or service providers where relevant; professional advisers and accounting service providers to the extent necessary for their role; and other suppliers processing data on our behalf.

We may also disclose personal data to the FCA, HMRC, ICO, OFSI, NCA, police, courts and other competent authorities where disclosure is required or permitted by law, and where necessary to establish, exercise or defend legal rights. We provide only the personal data that is necessary and proportionate for the relevant purpose.

Where a third party acts as our processor, we require appropriate contractual, confidentiality and security commitments. Some recipients, such as banks, acquiring institutions or public authorities, may act as independent controllers for their own legal and regulatory purposes.

17. International transfers

Personal data used in our services may be processed or accessed in the United Kingdom and Poland. Transfers from the UK to countries covered by UK adequacy regulations, including EEA countries such as Poland, may be made on the basis of those adequacy arrangements.

Where a restricted transfer is made to a country or recipient not covered by UK adequacy regulations, we will use an appropriate transfer mechanism where required, such as an approved UK transfer agreement or addendum and any required transfer risk or data protection assessment, or another lawful exception.

You may contact our Data Protection Officer if you would like further information about the safeguards applying to a particular international transfer.

Other matters

18. Use of the service by children

Our money transfer services are intended for adults. You may use the service only if you are 18 or over. We do not knowingly provide the service to children or market our money transfer service to children.

19. Security of your personal data

We use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures include access controls, authentication, encryption where appropriate, secure hosting arrangements, monitoring, staff training and procedures for handling security incidents.

No transmission or storage system can be guaranteed to be completely secure. You are responsible for keeping your login and security credentials confidential and for notifying us promptly if you believe your account or credentials have been compromised.

20. Retention period for personal data

We retain personal data only for as long as necessary for the purpose for which it was collected and in accordance with legal, regulatory and operational requirements and our Data Retention Policy. Where more than one retention requirement applies, we use the longest mandatory period that is lawful and necessary. A legal hold, investigation, regulatory enquiry or litigation may require specific records to be retained for longer.

Customer identification, KYC, CDD and EDD records that fall within anti-money laundering record-keeping requirements are generally retained for five years after the end of the business relationship, or for five years after completion of an occasional transaction where applicable. Relevant payment-services compliance records are retained for at least five years from creation.

Relevant customer transaction and AML, sanctions, PEP and compliance investigation records are generally retained for the applicable five-year statutory period. Service complaint records are normally retained for three years from receipt, customer service call recordings for five years from recording, website and security logs for 12 months by default, and records of data subject rights requests for three years from closure, unless a longer legal or regulatory requirement applies.

Regulatory, supervisory and law-enforcement request records are normally retained for six years after closure of the matter. Financial, accounting and tax records are normally retained for six years from the end of the relevant financial year or accounting period, subject to any longer statutory enquiry or hold.

Marketing consent and preference records are retained while they are relied on and for an appropriate evidential period afterwards. Minimum suppression information may be retained for as long as necessary to honour an opt-out or objection. When an applicable retention period expires and no exception applies, personal data is securely deleted or anonymised.

21. Review of this Privacy Notice

We review this Privacy Notice regularly and update it where necessary to reflect changes in law, regulation, our services, systems, suppliers or processing activities. The current version will be made available on our website.

If you have any questions about this Privacy Notice or how we use your personal data, please contact our Data Protection Officer at robert.kaczmarek@varsoviafx.com or contact us at bok@varsoviafx.com.