MindPay

LEGAL DOCUMENT

MindPay - Fintech platform for multi-currency payments and financial services

Privacy Policy

Privacy Policy

EFFECTIVE DATE	VERSION	JURISDICTION
18.05.2026	**1.0**	**Czech Republic · EU / GDPR**

www.mindpay.finance

MindPay s.r.o. · Křemenáčová 90/6 · Praha 10 · CZ

MINDPAY · LEGAL DOCUMENT

Contents

Privacy Policy · Version 1.0 · effective from 18.05.2026

PRIVACY POLICY

Privacy Policy

Introduction

This Privacy Policy (the “Policy”) has been prepared in accordance with Regulation (EU) 2016/679 on the protection of personal data (GDPR), the EU ePrivacy Directive 2002/58/EC, and the applicable national legislation of the Czech Republic.

This Policy explains what personal data MindPay collects, the legal bases and purposes for which it processes such data, how it protects personal data, to whom and under what conditions it may disclose data, and what rights data subjects have.

MindPay deeply respects the privacy of its clients and business partners. The protection of personal data is not only a legal obligation, but also the foundation of the trust our clients place in us every day when using the payment infrastructure of the platform.

By using MindPay services, you confirm that you have read this Policy and agree to the processing of your personal data for the purposes described herein. If you do not agree with any provision of this Policy, please refrain from using the platform services and contact us for clarification.

1 Data Controller - who we are

MindPay is a fintech platform providing corporate clients and individuals with multi-currency payment accounts and international payment services. The payment infrastructure operates through a partner EMI provider acting under a licence issued by an authorised regulator in accordance with the EU Payment Services Directive (PSD2).

Pursuant to Article 4(7) GDPR, MindPay acts as the Data Controller, meaning the entity that determines the purposes and means of processing personal data of clients and platform users.

In its relationships with the EMI provider and other subprocessors, MindPay acts as controller, while such parties act as Data Processors within the meaning of Article 4(8) GDPR, unless they act as independent controllers for their own regulatory obligations.

MindPay is not a bank, does not hold client funds on its own balance sheet, and does not conduct banking activities. All payment operations are carried out through a licensed partner.

2 Scope of this Policy

This Policy applies to all personal data processing operations carried out by MindPay in connection with the provision of payment and related services. The Policy applies to the following categories of persons:

- Authorised representatives and employees of corporate clients registered on the platform;
- Directors, executive officers, Ultimate Beneficial Owners (UBOs) and shareholders of corporate clients undergoing KYC/KYB verification;
- Individuals, sole traders and self-employed persons using MindPay services;

- Visitors of the website www.mindpay.finance, including potential clients;
- MindPay counterparties, partners and suppliers, to the extent necessary for business relationships;
- Payment recipients, to the extent necessary for the execution of transactions.

This Policy does not apply to the processing of employee data in the context of employment relationships with MindPay. A separate internal HR data processing policy applies to employees.

3 Categories of personal data we collect

MindPay follows the principle of data minimisation under Article 5(1)(c) GDPR: we collect and process only the data necessary to achieve specific, predefined and lawful purposes. The categories of data we may collect are listed below.

3.1 Corporate data for KYB verification

When a company registers on the platform and undergoes Know Your Business (KYB) verification, we collect:

- Full and abbreviated legal name of the legal entity;
- Country of registration, registration date and registration number;
- Registered office and actual business address;
- Articles of association, memorandum of association and other registration documents;
- Information on the corporate ownership structure, including an ownership chart indicating shareholdings;
- Data of directors, executive officers and other authorised signatories;
- Data of beneficial owners (UBOs) with ownership or control of 25% or more;
- Description of the main business activity, sources of income and geography of operations;
- Copies of valid licences or permits where the activity is licensed;
- Financial statements or other documents confirming the lawful source of funds, where required;
- Information about existing banking relationships.

3.2 Personal data of individuals (KYC)

For Know Your Customer (KYC) checks of directors, UBOs and authorised representatives, we collect:

- Full first name and surname as stated in the identity document;
- Date and place of birth;
- Citizenship, including multiple citizenships where applicable;
- Country of residence;
- Copy of a valid passport, national ID card or other identity document;
- Proof of address issued no earlier than 3 months before submission, such as a utility bill or bank statement;
- Results of Politically Exposed Person (PEP) screening;
- Results of checks against sanctions lists, including OFAC, EU, UN and other lists;
- Contact details: email address and phone number;
- For video verification: facial image processed as part of the liveness check through a KYC provider.

3.3 Transaction data

When using MindPay payment services, we process:

- Data on outgoing and incoming payments: amount, currency, date and time;
- Sender and recipient details: name, IBAN/account number, BIC/SWIFT and bank;
- Payment purpose and documents attached to transactions, such as invoices and contracts;
- Data on currency conversions and applied exchange rates;
- Transaction history and statuses in the personal account dashboard;
- Information on suspended, blocked or returned payments;
- AML screening flags and results for transactions.

3.4 Technical and user data

When you visit the website and use the platform, the following data is collected automatically:

- IP address and geolocation data at country/city level;
- Device type, model and unique device identifier;
- Browser type and version, operating system;
- URLs of visited pages, time on page and navigation paths;
- Cookies and similar technologies, as further described in Section 9;
- Login logs: date, time, IP address and authentication status;
- Error data and service incident data.

3.5 Communication data

When you contact us directly, we process:

- Content of email correspondence or messages sent through a contact form;
- Customer support call recordings, subject to prior notice and where permitted by law;
- Technical support chat and ticket data;
- Feedback, complaints and enquiries.

4 Purposes of processing and legal bases

In accordance with Article 13 GDPR, every personal data processing operation must have a specific legal basis. MindPay processes data only under the following legal bases and for the following purposes.

4.1 Performance of a contract (GDPR Article 6(1)(b))

Processing is necessary for entering into and performing a payment services agreement, including:

- Registering a company account and opening a multi-currency account;
- Processing payment transactions and currency operations;
- Providing access to the personal account dashboard and payment interface;
- Handling technical support requests related to the services;
- Issuing invoices and accounting for fees.

4.2 Compliance with legal obligations (GDPR Article 6(1)(c))

Processing is necessary to comply with mandatory requirements of applicable law:

- Conducting KYC/KYB verification under AMLD4/AMLD5/AMLD6 and national AML legislation;
- Monitoring transactions and detecting suspicious activity as part of AML/CFT controls;
- Screening against sanctions lists of the EU, UN, OFAC and other regulators;
- Retaining documentation for the periods established by regulators, not less than 5 years;
- Providing information to public authorities upon lawful request;
- Complying with tax reporting and financial monitoring requirements.

4.3 Legitimate interests (GDPR Article 6(1)(f))

Processing is necessary for MindPay's legitimate interests, provided that such interests are not overridden by the rights and freedoms of data subjects:

- Ensuring platform security: detecting and preventing fraud, unauthorised access and cyberattacks;
- Conducting internal analytics to improve service quality;
- Maintaining business relationships with partners and counterparties;
- Managing legal risks and defending against claims;
- Checking the business reputation of corporate clients and counterparties through due diligence.

Where processing is based on legitimate interests, you have the right to object under Article 21 GDPR, as further described in Section 11.

4.4 Consent (GDPR Article 6(1)(a))

In certain cases, processing is carried out on the basis of your explicit consent:

- Use of analytical and marketing cookies;
- Sending newsletters and marketing communications;
- Conducting satisfaction surveys and user experience research;
- Processing data for purposes expressly stated in a consent form.

Consent may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal. Withdrawal of consent does not terminate the contractual relationship.

5 Disclosure of data to third parties and subprocessors

MindPay never sells, rents or transfers personal data to advertising networks, data brokers or third-party marketing companies. Data is disclosed to third parties only in the cases listed below, strictly to the extent necessary and on the basis of Data Processing Agreements (DPAs) concluded in accordance with Article 28 GDPR.

5.1 EMI provider (licensed partner)

Data is transferred to the partner EMI provider for the following functions:

- Comprehensive KYC/KYB verification and AML screening of clients;
- Checks against sanctions lists and PEP lists;
- Opening and maintaining payment accounts;

- Transaction monitoring and preparation of suspicious activity reports (SARs);
- Retention of mandatory documentation in accordance with licence requirements.

A DPA containing the mandatory provisions of Article 28 GDPR is concluded with the EMI provider. The EMI provider may act both as an independent controller for its own AML obligations and as a processor of MindPay data.

5.2 Payment systems and correspondent banks

To execute international payment instructions, data is transferred in the minimum necessary scope to payment system operators and correspondent banks through the following rails:

- SWIFT - for international transfers;
- SEPA Credit Transfer and SEPA Instant - for payments within the EEA;
- Other national and international payment systems where necessary.

5.3 KYC/KYB and identity verification providers

Specialised services may be used for remote document verification and identity checks, including:

- Video KYC and liveness verification providers;
- Automated document verification services, including OCR verification;
- Databases for sanctions and PEP screening.

5.4 IT infrastructure and cloud services

Certified providers are used to ensure the functioning of the platform:

- Cloud hosting and computing infrastructure located in the EU or in jurisdictions with an adequacy decision;
- Backup and disaster recovery systems;
- CRM systems and technical support platforms;
- Analytics and performance monitoring tools.

5.5 Professional advisers

Personal data may be disclosed to external legal, tax and audit advisers solely to protect MindPay’s legitimate interests and subject to confidentiality obligations.

5.6 Public authorities and regulators

Data may be disclosed to public authorities in the following cases:

- Responding to a lawful request from a public authority, court or prosecutor;
- Mandatory notification of Financial Intelligence Units (FIUs) about suspicious transactions under AML law;
- Interaction with tax authorities regarding tax compliance;
- Regulatory reporting to financial supervisory authorities.

We will notify you of such requests to the extent not prohibited by law.

6 International transfers of personal data

GDPR imposes strict restrictions on transfers of personal data outside the European Economic Area (EEA). MindPay ensures an adequate level of protection in all cases of cross-border data transfers.

6.1 Priority of data storage in the EEA

By default, MindPay seeks to store and process personal data on servers physically located in the EEA. Subprocessors are selected with regard to the geography of data processing. Transfers outside the EEA are permitted only where one of the safeguards below applies.

6.2 Applicable safeguards

- Adequacy Decisions of the European Commission - for countries recognised as providing an equivalent level of protection;
- Standard Contractual Clauses (SCCs) approved by Commission Implementing Decision (EU) 2021/914 and used in contracts with subprocessors in third countries;
- EU-US Data Privacy Framework - for transfers to certified recipients in the United States;
- Binding Corporate Rules (BCRs) - where necessary for intra-group transfers;
- Explicit consent of the data subject - in exceptional cases where other mechanisms are not available.

6.3 Notification of cross-border transfers

Information on specific third countries to which your data is transferred and the safeguards applied is available upon request sent to support@mindpay.finance. The current register of subprocessors and processing locations is updated when the composition of providers changes.

7 Retention, security and deletion of data

7.1 Retention periods

MindPay retains personal data for the period necessary to achieve the purposes of processing or to comply with legal requirements. Key retention periods are:

- KYC/KYB data, including identity documents and verification results - at least 5 years from account closure or termination of the business relationship, as required by AMLD5/AMLD6 and national AML legislation;
- Transaction data and payment history - at least 5 years, and in some jurisdictions up to 10 years, according to requirements of the EMI provider and regulator;
- Technical logs, security data and access logs - up to 12 months;
- Communication data, including support correspondence - up to 3 years;
- Marketing data and cookie data - until consent is withdrawn or in accordance with applicable cookie retention periods;
- Data relating to blocked or suspicious operations - in accordance with AML legislation, but not less than 5 years.

After the applicable retention period expires, data is irreversibly deleted or anonymised in such a way that identification of the data subject is no longer possible.

7.2 Location of data storage

Primary data repositories are located on secure servers in the European Union. All subprocessors that store data have been reviewed for GDPR compliance. Where storage outside the EEA is necessary, the

mechanisms described in Section 6 apply.

7.3 Technical and organisational security measures

MindPay implements a comprehensive set of measures to ensure the security of personal data.

Technical measures:

- Encryption of data at rest: AES-256 or an equivalent standard;
- Encryption of data in transit: TLS 1.2 / 1.3 for all connections;
- Multi-factor authentication (MFA/2FA) for access to the platform and internal systems;
- Segmentation of network infrastructure and isolation of critical components;
- Automated anomaly monitoring and intrusion detection/prevention systems (IDS/IPS);
- Regular backups with restoration testing;
- Vulnerability management: regular penetration testing and security audits.

Organisational measures:

- Role-Based Access Control (RBAC): access to personal data only for Operations and Compliance staff who need it to perform their duties;
- Least privilege policy when granting access rights;
- Regular employee training on data protection and cybersecurity;
- Internal security incident response policy;
- Procedures for reviewing and auditing subprocessors;
- Maintenance of Records of Processing Activities (RoPA) under Article 30 GDPR.

8 Payment data and PSD2 requirements

MindPay operates within the regulatory environment established by the EU Payment Services Directive (PSD2, Directive 2015/2366/EU) and its implementation in the national laws of EU Member States. PSD2 sets additional requirements for the processing of payment data and transaction security.

8.1 Strong Customer Authentication (SCA)

In accordance with PSD2 and Commission Delegated Regulation (EU) 2018/389 (RTS on SCA), MindPay applies Strong Customer Authentication when:

- Logging into the platform account;
- Initiating payment transactions above established thresholds;
- Performing any actions related to changing payment details or security settings.

SCA is based on using at least two of three factors: knowledge (password), possession (device/token), and inherence (biometrics). The relevant authentication data is processed solely for security purposes.

8.2 Payment purpose and financial data

In accordance with FATF Recommendation 16 on the travel rule and regulatory standards, mandatory payer and payee data is attached to each outgoing transaction. This data is an integral part of the payment instruction and is processed on the legal bases of performance of a contract and compliance with a legal obligation.

8.3 Account access through Open Banking (if applicable)

If MindPay in the future enables third-party applications to connect to a client account through an Open Banking API under PSD2, such access will be provided only:

- On the basis of the client's explicit consent;
- To the extent expressly authorised by the client;
- With the ability to withdraw consent at any time through the personal account settings.

9 Cookies and tracking technologies

Our website and platform use cookies and similar technologies, including web beacons, pixels and local storage, in accordance with the EU ePrivacy Directive 2002/58/EC and GDPR. This section provides comprehensive information on the technologies used.

9.1 Strictly necessary (technical) cookies

These cookies are necessary for the proper functioning of the website and platform. Their use does not require your consent because the service cannot function without them.

- Session identifiers (session_id) - maintaining an authenticated session;
- Security tokens (CSRF tokens) - protection against cross-site attacks;
- Language settings and regional preferences;
- Load balancers - ensuring infrastructure availability.

Retention period: during the session or up to 1 year. These cookies are not transferred to third parties.

9.2 Analytical cookies

Analytical cookies are used to collect anonymised statistics about user behaviour in order to improve the service. They are set only with your explicit consent.

- Google Analytics - analysis of traffic, traffic sources and behaviour on the website. Data is transferred to Google LLC (USA) using the EU-US Data Privacy Framework;
- Internal analytics tools - monitoring platform performance.

Retention period: from 30 days to 2 years. You may opt out of analytical cookies through the cookie banner.

9.3 Functional cookies

Functional cookies allow the platform to remember your preferences to provide a personalised experience. They are set only with your consent.

- Remembering language preferences;
- Saving personal account display settings.

9.4 Marketing and advertising cookies

MindPay does not currently use marketing or advertising cookies. If such tools are introduced, you will be notified and your separate consent will be requested.

9.5 Cookie management

When you first visit the website, a cookie management banner (Consent Management Platform) is displayed, allowing you to:

- Accept all categories of cookies;
- Accept only strictly necessary cookies;
- Configure permissions by category.

You may change your cookie settings at any time through the “Privacy Settings” section on the website or through your browser settings. Withdrawal of cookie consent does not terminate the contractual relationship with MindPay.

10 Profiling and automated decision-making

Article 22 GDPR regulates situations where decisions that significantly affect a data subject are made solely by automated means without human involvement. MindPay strives for maximum transparency on this issue.

10.1 AML scoring and transaction monitoring

As part of AML/CFT compliance, MindPay and its EMI partner use automated monitoring systems for:

- Assigning risk levels to transactions based on predefined rules and algorithms;
- Automatically blocking transactions that exceed risk thresholds;
- Generating alerts for subsequent manual review by the compliance team.

The final decision to block an account or reject a transaction is made with the involvement of a compliance specialist. In the event of an automatic block, you may request a manual review by contacting support@mindpay.finance.

10.2 Risk assessment during KYC/KYB

During client verification, a Risk-Based Approach (RBA) is applied: clients are automatically assigned a risk category (low, medium or high) based on:

- Jurisdiction of company registration and individual residence;
- Main business activity;
- PEP status or matches against sanctions lists;
- Ownership structure and other factors.

The assigned risk category affects the scope of requested documentation and the frequency of reverification. If you believe that your risk category has been assigned incorrectly, you have the right to request an explanation and review.

10.3 Your rights regarding automated decisions

Under Article 22 GDPR, you have the right to:

- Receive information about the logic of the decision-making algorithms used;
- Request human review of any automated decision affecting your interests;
- Challenge the decision and present your position.

11 Your rights as a data subject

GDPR grants individuals a broad range of rights in relation to their personal data. MindPay is committed to ensuring that these rights can be exercised within the prescribed deadlines.

11.1 Right of access (Article 15 GDPR)

You have the right to request confirmation as to whether MindPay processes your personal data and to receive a copy of the processed data, including information about purposes of processing, categories of data, recipients, retention periods and your rights.

11.2 Right to rectification (Article 16 GDPR)

You have the right to request correction of inaccurate or incomplete personal data without undue delay. In some cases, correction of regulatory-relevant data, such as KYC data, will require supporting documents.

11.3 Right to erasure / “right to be forgotten” (Article 17 GDPR)

You have the right to request deletion of your personal data where one of the following grounds applies: the data is no longer necessary for the purposes for which it was collected; you withdraw consent and there is no other legal basis for processing; or the data was processed unlawfully. Important: the right to erasure is not absolute. We cannot delete data that must be retained by law, such as KYC documents retained for 5 years under AML legislation. In such cases, we will inform you of the grounds for refusal.

11.4 Right to restriction of processing (Article 18 GDPR)

You have the right to request suspension of processing where you contest the accuracy of the data for the verification period; the processing is unlawful but you prefer restriction instead of deletion; we no longer need the data but you need it for legal claims; or you have objected to processing while the objection is being considered.

11.5 Right to data portability (Article 20 GDPR)

You have the right to receive the data you provided in a structured, commonly used and machine-readable format such as JSON or CSV and to transmit it to another controller. This right applies to data processed on the basis of consent or contract by automated means.

11.6 Right to object (Article 21 GDPR)

You have the right to object to processing based on legitimate interests under Article 6(1)(f), including profiling. After receiving an objection, MindPay will stop processing unless it demonstrates compelling legitimate grounds overriding your interests. Objections to marketing communications are always honoured unconditionally.

11.7 Right to withdraw consent (Article 7 GDPR)

Where processing is based on consent, you have the right to withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

11.8 Right not to be subject to automated decisions (Article 22 GDPR)

This right is described in more detail in Section 10. You have the right not to be subject to decisions based solely on automated processing where such decisions produce legal or similarly significant effects for you.

11.9 How to exercise your rights

To submit a request to exercise any of the rights listed above:

– Email: support@mindpay.finance (subject line: “Data Subject Request - [type of right]”);

– Written request: Křemenáčová 90/6, Pitkovice, 104 00 Praha 10, CZ.

Response period: 30 calendar days from receipt of the request. In exceptional cases, the period may be extended to 90 days with notification of the reasons for the delay under Article 12(3) GDPR. The response is provided free of charge. For manifestly unfounded or excessively repetitive requests, MindPay may charge a reasonable fee or refuse to respond under Article 12(5) GDPR.

Identity verification may be required when processing a request. We may request clarifying information within reasonable limits and will not request excessive information.

11.10 Right to lodge a complaint with a supervisory authority

If you believe that MindPay has violated your data protection rights, you have the right to lodge a complaint with the supervisory authority in the place of your habitual residence, place of work or place of the alleged infringement.

– Supervisory authority of the Czech Republic: Úřad pro ochranu osobních údajů (ÚOOÚ);
– Website: www.uoou.cz;
– Address: Pplk. Sochora 27, 170 00 Praha 7.

We recommend contacting us directly before submitting a complaint to ÚOOÚ, as most issues can be resolved in the ordinary course of communication.

12 Personal data breach notification

MindPay maintains an internal information security incident response procedure covering identification, assessment, containment and remediation of personal data breaches.

12.1 Notifiable security breaches

A personal data breach means a security event leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data under Article 4(12) GDPR. Examples include unauthorised access to a client database, loss of a storage medium containing client data, or a successful phishing attack on an employee with access to personal data.

12.2 Notification to the supervisory authority (Article 33 GDPR)

In the event of a breach likely to result in a risk to the rights and freedoms of natural persons, MindPay must notify ÚOOÚ, or another competent supervisory authority, within 72 hours after becoming aware of the incident. The notification includes:

– Description of the nature of the incident and the categories and approximate number of affected persons;
– Contact details of the data protection contact person or other contact point;
– Description of likely consequences of the incident;
– Description of measures taken or planned to address the incident and mitigate its effects.

12.3 Notification to data subjects (Article 34 GDPR)

If the incident is likely to result in a high risk to the rights and freedoms of natural persons, MindPay will notify you directly without undue delay in a clear and accessible form. The notification will be sent by email or through the platform dashboard.

12.4 Incident register

All data security incidents, regardless of whether external notification is required, are recorded in an internal incident register under Article 33(5) GDPR, including the circumstances, consequences and measures taken.

13 Data Protection Officer (DPO)

Article 37 GDPR requires the appointment of a Data Protection Officer (DPO) for organisations whose core activities involve large-scale systematic processing of personal data or processing of special categories of data.

At the current stage, MindPay is assessing whether appointment of a DPO is mandatory under the criteria of Article 37 GDPR, taking into account the scale of data processing. As the platform grows and processing volumes increase, a DPO will be appointed and information about the DPO will be published in this Policy.

Currently, all matters related to personal data protection are handled by the MindPay Operations & Compliance team. Contact for data protection matters:

- Email: support@mindpay.finance (subject: “Privacy / Data Protection”);
- Address: Křemenáčová 90/6, Pitkovice, 104 00 Praha 10, CZ.

14 Privacy by Default and Privacy by Design

MindPay applies the principles of Privacy by Design and Privacy by Default under Article 25 GDPR, treating personal data protection as an integral part of the product and business processes rather than as an afterthought.

14.1 Data minimisation principle

At all stages of development and operations, MindPay assesses the necessity of collecting each data field. Only the minimum information actually necessary for a specific purpose is collected. By default, the platform is configured with the strictest privacy settings.

14.2 Data Protection Impact Assessment (DPIA)

Before launching new features or integrations involving personal data processing, MindPay conducts a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of natural persons under Article 35 GDPR. DPIA results are documented and, where necessary, submitted to the supervisory authority for prior consultation.

14.3 Personnel training

All MindPay employees who work with personal data undergo mandatory introductory training on data protection and regular refresher training. Identified incidents are reviewed during training sessions to prevent recurrence.

14.4 Records of Processing Activities (RoPA)

MindPay maintains internal Records of Processing Activities in accordance with Article 30 GDPR. The register is regularly updated and contains information about all processing operations, data categories, purposes, legal bases, retention periods and subprocessors.

15 Policy regarding minors

MindPay services are intended exclusively for legal entities and legally capable individuals who have reached the age of majority (18 years). MindPay does not intentionally collect, request or process personal data of persons under 18 years of age.

If we become aware that personal data of a minor has been provided to us without appropriate consent from a parent or legal guardian, such data will be promptly deleted from all systems. If you become aware of such an incident, please notify us immediately at support@mindpay.finance.

16 Applicable law and regulatory framework

This Policy has been developed in accordance with the requirements of the following legal acts:

- Regulation (EU) 2016/679 (GDPR) - the main EU legal act on personal data protection;
- Directive 2002/58/EC (ePrivacy Directive) and its national implementations - regarding cookies and electronic communications;
- Directive (EU) 2015/2366 (PSD2) and Commission Delegated Regulation (EU) 2018/389 (RTS on SCA) - regarding payment data processing and authentication;
- Directive (EU) 2018/843 (AMLD5) and Directive (EU) 2024/1640 (AMLD6) - regarding AML/KYC data retention requirements;
- Czech Act No. 110/2019 Coll. on the processing of personal data (Zákon o zpracování osobních údajů) - national implementation of GDPR;
- Czech Act No. 253/2008 Coll. on selected measures against legitimisation of proceeds of crime and financing of terrorism (AML Act).

In the event of a conflict between this Policy and applicable legal requirements, the legal requirements shall prevail.

17 Changes to this Privacy Policy

MindPay may periodically update this Policy due to changes in legislation, the composition of subprocessors, business processes or the technological infrastructure of the platform.

We will notify you of material changes to the Policy at least 14 calendar days before the effective date of such changes by the following means:

- Sending a notice to the registered email address;
- Displaying a notice banner on www.mindpay.finance;
- Publishing the current version of the Policy with the effective date and a brief description of changes.

Minor changes, such as clarification of wording, correction of typographical errors or updates to contact details, may be made without prior notice. The date of the latest update is always shown in the document header.

Continued use of MindPay services after changes enter into force means your acceptance of the updated Policy. If you do not agree with the changes, you have the right to stop using the services and request deletion of your data in the prescribed manner.

18 Contact information

For all questions related to this Policy, the processing of personal data, exercising your rights or data incidents, you may contact us as follows:

For data subject requests, please include the following in the subject line: “Data Subject Request - [type of right]”. This will help us process your request faster.

Response time for general questions: up to 5 business days. Response time for rights requests: up to 30 calendar days in accordance with GDPR.