Information on the Processing of Client Personal Data

- **Citfin – Finanční trhy, a.s.**, ID No.: 25079069, with its registered office at Bucharova 1423/6, 158 00 Prague 5, registered in the Commercial Register maintained by the Municipal Court in Prague, Section B, File No. 4313; and
- **Citfin, Savings Cooperative**, ID No.: 25783301, with its registered office at Bucharova 1423/6, 158 00 Prague 5, registered in the Commercial Register maintained by the Municipal Court in Prague, Section Dr, File No. 4607 (hereinafter collectively referred to as "Citfin").

Citfin provides services to corporate clients, which include legal entities and self-employed individuals. This document provides information on the processing of personal data of these self-employed individuals, as well as representatives, employees, beneficial owners, account managers, payment cardholders, and other individuals whose personal data Citfin processes in connection with the provision of its services (hereinafter collectively referred to as **"data** subjects").

1. Introductory Information

Citfin – Finanční trhy, a.s. and Citfin, spořitelní družstvo are joint controllers for the processing of personal data described in this document, as they jointly determine the purposes and means of such processing.

The joint controllers have defined their responsibilities for fulfilling obligations in the area of personal data protection through an agreement pursuant to Article 26 of the GDPR, particularly with regard to providing information and handling requests from data subjects. These obligations are primarily fulfilled by the controller to whose service or client relationship the relevant processing relates. In other cases, the joint controllers act in coordination with one another.

This does not affect the data subject's right to exercise their rights against any of the joint controllers. Joint controllers may disclose personal data to one another to the extent necessary for the relevant processing purposes, on an appropriate legal basis, and under the conditions set forth by law, including the relevant confidentiality obligations.

Citfin has appointed a Data Protection Officer ("DPO"), who can be contacted atgdprpoverenec@citfin.cz .

This document also applies to the processing of personal data in connection with the issuance and administration of Visa payment cards and the use of the Citfin mobile app for Android and iOS, operated by Citfin, a savings cooperative.

2. What Categories of Personal Data Do We Process

Depending on the nature of the relationship and the services provided, we process the following categories of personal data in particular:

- **Identification data**—in particular, first name, last name, date of birth, birth number, residential address, nationality, place of birth, and information from the identity card , including its number, photograph, and signature; for self-employed individuals, also the business identification number (IČO) and registered office address.
- **Contact and access data** – specifically, phone number, email and mailing addresses, usernames, authentication data, and other security features.
- **Biometric data** – data generated by the technical processing of a natural person's physical appearance for the purpose of verifying their identity, in particular by comparing their appearance with the photograph on the presented identification document.
- **Data regarding contractual relationships, products, and services**—specifically data on accounts, contracts, products and services used, transactions, individual authorizations, service settings, preferred language, and offers.
- **Data related to compliance with regulatory obligations**—in particular, data on beneficial owners, politically exposed persons, economic activities, sources of funds, the purpose and intended nature of the business relationship, and data obtained during customer due diligence in accordance with anti-money laundering and counter-terrorism financing regulations.
- **Payment card data**—specifically, cardholder information, card number, expiration date, status, and limits; records of completed and verified transactions; and data required for tokenization and adding the card to a digital wallet.
- **Communication data**—specifically, the content of communications and data regarding their course, including complaints, requests, and feedback, as well as data regarding the use of Citfin's websites and applications.
- **Technical and operational data** from **the mobile app**—specifically, activation data from the QR code, security token identifiers, device and app installation information, tokens for delivering push notifications, device model, app and operating system versions, records of approved or rejected transactions, security events, and diagnostic logs of app errors and crashes. If a user uses the "Report a Problem" feature, we also process the feedback they submit and their email address.
- **Records of phone calls** and the data contained in their content.
- **Camera recordings** made for the purpose of protecting people and property.

Data Processing by the Mobile App

In connection with the use of the mobile app, the following also applies:

- Payment card data, including the card number, CVV, and PIN, is transmitted to the device solely for display purposes, and the app does not permanently store this information.

- Biometric authentication via fingerprint or facial recognition is performed using the device's system functions. Citfin does not collect biometric characteristics or their templates through the app, but only information about the authentication result.
- When the app is activated, the camera is used to scan a QR code locally. The app does not send photos or videos.
- The app does not use the device's GPS location, does not access contacts or stored photos, and does not use the device's advertising identifier.

3. Purposes and Legal Bases for the Processing of Personal Data

We process personal data for the following purposes and on the corresponding legal bases.

3.1 Performance of a Contract and Pre-Contractual Measures

We process the personal data of representatives, employees, authorized signatories, payment cardholders, and other authorized persons for the purpose of negotiating and managing contractual relationships with corporate clients and providing the agreed-upon services.

This includes, in particular, the preparation and management of contractual documentation, verification of the authorization of persons acting on behalf of the client, management of accounts and access permissions, execution of transactions, provision of information and statements to authorized persons, issuance and management of payment cards, activation and use of the mobile app, approval of transactions, display of card details, adding cards to digital wallets, and related support.

The legal basis is Article 6(1)(b) of the GDPR, provided that the processing is necessary for the performance of a contract to which the data subject is a party—in particular, a self-employed individual—or for taking steps at the data subject's request prior to entering into a contract. In the case of persons acting on behalf of clients or other authorized persons who are not parties to the contract, the legal basis is generally the legitimate interest of Citfin or its clients in negotiating and properly fulfilling contractual relationships and providing services pursuant to Article 6(1)(f) of the GDPR, or, where applicable, compliance with legal obligations pursuant to Article 6(1)(c) of the GDPR.

Failure to provide the data necessary to identify or verify the authorization of the relevant person may prevent that person from acting on behalf of a client or from using the relevant service.

3.2 Compliance with Legal Obligations

We also process personal data for the purpose of complying with the legal obligations of the relevant Citfin company, in particular:

- identifying and verifying clients and other individuals in accordance with AML regulations, including the processing of identification data and the collection and retention of copies of identification documents to the extent necessary;

- fulfilling obligations in the provision of payment services, including strong user authentication, if required;
- fulfilling regulatory and prudential obligations when providing investment services and in the operations of a savings and credit union;
- retaining data and documents required by law, and creating and retaining records of telephone and electronic communications, if required by law;
- handling claims, complaints, requests from data subjects, and other submissions to the extent specified by law.

The legal basis is Article 6(1)(c) of the GDPR. The relevant obligations arise primarily from Act No. 253/2008 Coll., on Certain Measures Against the Legalization of Proceeds from Criminal Activity and the Financing of Terrorism, Act No. 370/2017 Coll., on Payment Systems, Act No. 256/2004 Coll., on Business Activities on the Capital Market, Act No. 87/1995 Coll., on Savings and Credit Cooperatives, and the GDPR.

3.3 Other Legitimate Interests

Based on a legitimate interest pursuant to Article 6(1)(f) of the GDPR, we also process personal data for the following purposes:

- managing relationships with corporate clients and handling suggestions, requests, and problem reports, unless the processing is based on compliance with a legal obligation;
- preventing fraud and abuse and ensuring the security and stability of the services and mobile app we provide;
- protecting persons and property and ensuring the security of Citfin's premises, including the operation of video surveillance systems;
- establishing, exercising, and defending legal claims;
- evaluating the use of the products and services we provide in order to improve them and tailor them to clients' needs.

In connection with the operation of the mobile app, we also process security and diagnostic logs, particularly logs of app errors and crashes. Users can disable the sending of diagnostic error logs in the app settings under "App Diagnostics." Disabling this feature does not affect the processing of security and transaction logs based on other purposes and legal grounds. Payment card and account numbers, email addresses, and phone numbers are removed from diagnostic logs regarding app errors and crashes.

3.4 Direct Marketing

We may process contact information and other data related to the use of our products and services for the purpose of direct marketing of the relevant Citfin company's own products and services based on a legitimate interest pursuant to Article 6(1)(f) of the GDPR.

3.5 Processing Based on Consent

Marketing Based on Consent

Based on consent pursuant to Article 6(1)(a) of the GDPR, we may process personal data for other marketing purposes specified in the relevant consent, in particular for sending product and service offers or preparing personalized offers.

Biometric Identity Verification

Based on the data subject's explicit consent, we may process biometric data derived from the technical processing of their likeness for the purpose of verifying that it matches the photograph on the presented identification document. The legal basis is Article 6(1)(a) in conjunction with Article 9(2)(a) of the GDPR.

Consent may be withdrawn at any time in the manner specified at the time it was granted or via the contact information provided in this document. Withdrawal of consent does not affect the lawfulness of processing carried out prior to its withdrawal.

4. Method of Processing Personal Data and Retention Period

We retain personal data only for as long as necessary for the purposes for which it is processed and in accordance with applicable laws. The following rules apply in particular to selected categories of data:

- We generally retain **data and documents related to client identification and verification** pursuant to Act No. 253/2008 Coll. for a period of 10 years from the date of the transaction outside a business relationship or the termination of the business relationship.
- We retain **records of the provision of investment services and executed transactions**—in particular, client instructions and related records of telephone and electronic communications—for at least 5 years, or up to 7 years if so decided by the Czech National Bank.

We retain other data related to the provision of services for the period necessary for the relevant purpose and subsequently for the period required by law or necessary to protect legal claims, particularly taking into account statutes of limitations and any ongoing proceedings.

We retain data processed on the basis of consent for the period necessary for the relevant purpose, at most until the consent is revoked, unless there is another legal basis for its further retention. We retain records of the granting, modification, and revocation of consent for the period necessary to demonstrate the lawfulness of the processing and to protect legal claims.

We process personal data manually or automatically and store it securely in paper or electronic form, primarily in Citfin's information systems.

Upon deactivation of the mobile app, the device pairing and the token used to send notifications are deleted. We retain routine diagnostic logs of errors and app crashes for a maximum of 90 days from the occurrence of the recorded event. We retain security logs in accordance with their purpose, the results of security risk assessments, and applicable regulatory requirements. Records related to security incidents may be retained for a longer period if necessary for their investigation or to protect legal claims.

We retain data obtained while handling inquiries and requests, including reports submitted via the "Report a Problem" feature, for the time necessary to resolve them and, if applicable, subsequently to protect legal claims. We retain video surveillance recordings for the time necessary to protect persons and property.

Citfin does not engage in profiling within the meaning of Article 4(4) of the GDPR, nor does it engage in decision-making based solely on automated processing that would produce legal effects on data subjects or similarly significantly affect them within the meaning of Article 22 of the GDPR.

5. Recipients of Personal Data

We may disclose personal data to other recipients to the extent necessary, in accordance with the GDPR and other applicable laws, including confidentiality obligations.

Recipients include, in particular, IT and archiving service providers, marketing agencies, debt management and collection agencies, attorneys, and other professional advisors. Some recipients act as our processors and process data in accordance with our documented instructions under a contract pursuant to Article 28 of the GDPR. Other recipients may act as independent controllers. Personal data may also be disclosed to competent public authorities and other parties if required or permitted by law.

In connection with the provision of card services, personal data may be disclosed primarily to SIA DECTA, which provides card transaction processing and payment card management services, and to MeaWallet AS, which provides technological services enabling the addition of payment cards to digital wallets, particularly Apple Pay and Google Pay. Data may also be transferred to Visa, digital wallet operators, and other entities involved in the execution, settlement, and security of card transactions. Personal data may also be disclosed, to the extent necessary, to service providers responsible for the production, personalization, and delivery of payment cards.

When operating the mobile app, we also use the services of technology providers to diagnose technical errors and ensure the app's security, including the detection of security risks and protection against misuse. For these purposes, technical identifiers of the device and the app installation, information about its operation, security events, and diagnostic data may be processed. Personal data may also be disclosed to service providers responsible for sending push notifications and verifying the authenticity of the app and the device.

Online Identification

When using online identification via the Citfin web interface, personal data may also be processed through the services of **Bankovní identita, a.s.** and **ONFIDO LTD**, depending on the selected method of identification. As part of these services, data necessary to verify identity may be processed by the relevant provider, and the verification results or related data may be transferred to Citfin.

Transfer of Personal Data Outside the European Economic Area

In connection with the use of services provided by certain providers, personal data may be transferred outside the European Economic Area (EEA). We carry out such transfers only under the conditions set forth in Chapter V of the GDPR, in particular based on a decision by the European Commission on an adequate level of protection pursuant to Article 45 of the GDPR or by ensuring appropriate safeguards pursuant to Article 46 of the GDPR. If the transfer is based on standard contractual clauses approved by the European Commission pursuant to Article 46 of the GDPR, information about these safeguards and how to obtain a copy of them can be obtained from our Data Protection Officer atgdprpoverenec@citfin.cz .

When using the ONFIDO LTD service for online identification, personal data may be transferred to the United Kingdom, for which the European Commission has adopted a decision on an adequate level of personal data protection.

We protect personal data using appropriate technical and organizational measures. We encrypt communication between the mobile app and Citfin's servers. Users can view their credit card number, CVV code, and PIN only after verification. We use external providers to handle certain functions of the mobile app, such as processing card data, sending notifications, and diagnosing errors. These providers have access to personal data only to the extent necessary to provide the relevant service. All third parties to whom we disclose users' personal data through the mobile app ensure the same or an equivalent level of protection for this data as described in this policy and as required by App Store guidelines.

6. Sources of Personal Data

We obtain personal data primarily:

- directly from data subjects during negotiations regarding business cooperation, the provision of services, and mutual communication;
- from corporate clients who provide us with data on their representatives, employees, authorized signatories, payment cardholders, and other authorized persons;
- through the use of our products and services, websites, and mobile applications;
- from publicly available sources, particularly public registries and lists;
- from providers of payment, identification, tokenization, and security services;
- from Citfin's own activities, particularly in the administration of contractual relationships, the execution of transactions, and the fulfillment of legal obligations.

7. Rights of Data Subjects

In connection with the processing of personal data, you have the following rights under the conditions set forth in the GDPR:

- **Right of Access** – to obtain confirmation as to whether we are processing your personal data, information about such processing, and a copy of such data.
- **Right to rectification** – to request the correction of inaccurate personal data or the completion of incomplete personal data.

- **Right to erasure** – to request the erasure of personal data if the conditions of the GDPR are met. This right does not apply to the extent that further processing is necessary, for example, to comply with a legal obligation or to protect legal claims.
- **Right to Restriction of Processing** – to request that processing be restricted in cases specified by the GDPR, such as when the accuracy of the data is disputed.
- **Right to** Data **Portability –** to receive the data you have provided to us and that we process automatically based on consent or a contract, in a structured, commonly used, and machine-readable format, and to transmit it to another controller. If technically feasible, you may request that it be transmitted directly to another controller.
- **Right to Object** – You may object to processing based on a legitimate interest for reasons related to your specific situation. In such a case, we will no longer process the data unless we demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or grounds related to the establishment, exercise, or defense of legal claims.
- **Right to Object to Direct Marketing** – You may object to processing for direct marketing purposes at any time without providing a reason. We will no longer process your data for this purpose.
- **Right to Withdraw Consent** – If processing is based on consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of prior processing.
- **Right to File a Complaint** – with the Office for Personal Data Protection, Pplk. Sochora 27, 170 00 Prague 7, www.uoou.gov.cz.

Exercising Your Rights

You may exercise your rights with any of the joint controllers, in particular through the DPO at**gdprpoverenec@citfin.cz** , or via email at**info@citfin.cz** or by phone at **+420 234 092 333**.

We process requests without undue delay, no later than one month after receiving them. In more complex cases, we may extend this deadline by up to two additional months; we will notify you of the extension and the reasons for it within the original one-month deadline.

Exercising your rights is generally free of charge. If a request is manifestly unfounded or excessive, we may charge a reasonable fee to cover administrative costs or refuse to comply with the request. We may also charge a reasonable fee for additional copies of personal data.

Last updated: December 1, 2026