(version effective as from 01.11.2026)

Privacy Policy

Protecting your personal data is very important to us. This Privacy Policy informs how UniCredit S.p.A. (“us”, “we” or “our”) collects and processes your personal data, notably through your use of our UniCredit Mobile App (“App”), our website www.unicredit.be/be-en/ (“Website”); jointly called “Services” and their functionalities.

For the purpose of the relevant data protection legislation, the data controller responsible for your personal data is UniCredit S.p.A., with registered office at Piazza Gae Aulenti 3, 20154 Milan, Italy, enrolled in the Register of Companies of Milan-Monza-Brianza-Lodi, Tax Code and VAT no. 00348170101, acting through its branch “UniCredit S.p.A. Belgian Branch”, having its office at Square Victoria Régina 1, 1210 Saint-Josse-ten-Noode, and registered with the Crossroads Bank for Enterprises under number 0897.315.623.

We have appointed a data protection officer (“DPO”) who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise any of your legal rights, please contact the DPO using the details set out below:

App: Support Center (logged Users),

Email address: privacy@unicredit.be

Postal address: UniCredit S.p.A. Belgian Branch, Sq. Victoria Régina 1, 1210 Saint-Josse-ten-Noode, Bruxelles, Belgium.

It is important that the personal data we hold about you are accurate and up to date. Please inform us about any relevant changes during your relationship with us using the contact details as set out in the previous paragraph.

Terms not otherwise defined in this Privacy Policy have the meaning given to them in our Terms and Conditions which are available on our Website.

Our App or Website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third-parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our Services, we encourage you to read the privacy notice of every third-party website you visit.

What data we collect about you

Personal data, or personal information means any information about an individual from which the person can be identified. It does not include data from which the identity of the natural person cannot be derived (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data like your first and last name, date of birth, National Registration number, copies of identification documents, username, password, biometric data such as your facial image or movie and any other information we need to verify your identity or prove your eligibility to use our Services.

Contact Data include billing address, delivery address, e-mail address and telephone number.

Data relating to the user account, including in particular: username, date of account creation in the App, history of actions undertaken within the user account, and location data.

Financial Data are data collected and processed in order to provide you with financial products and services. This may include your identification number and bank account numbers, credit or debit card numbers, information on your savings and investments, loans and credits, information necessary to assess your creditworthiness (information about your employment and salary, credit history, marital status and family composition, education) or your investor profile (information on your knowledge and experience of financial instruments, investment targets, your capacity to bear losses and risk tolerance).

Transaction Data include details about payments to and from you like account and card numbers, date, time, amount, currencies used, exchange rate, beneficiary details, details on the location of the merchant or CDM/ATM, IP address of sender and receiver, sender's and receiver's name and registration information, device information used to facilitate the payment.

Technical Data are data about your device or other equipment including information on the internet protocol (IP) address used to connect your device to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, the type of mobile device you use, device's IMEI number, the MAC address of the device's wireless network interface, mobile phone number used by the device, information stored on your device (including, if you allow us, access to contact information from your address book, login information, photos, videos or other digital content).

Data relating to your communications with us:

- the content of messages you send when using the chat feature;
- data you provide to us in the contact form;
- information you choose to provide during a telephone call, chat, or email conversation with us;
- information you provide to us as part of your survey responses.

Usage Data are information about your usage of our Services, your browsing actions and patterns. This may be based on cookies, logs or similar technologies. It may include uniform resource locators (URL), clickstream, services you searched, viewed or used, length of visits, page interaction information. For more information about cookies, please see our Cookie Policy.

- Location data is data determining your location using GPS technology or IP address.
- Information from social media networks or online accounts - information from any account that you share with us.

We may combine the personal data we collect from you, in the Application or on the Website, with data obtained from public sources and third parties:

- technical and usage-related data, which we obtained from analytical service providers (e.g., Google Analytics);
- address and contact details related to business activities, which we obtained from information providers, such as business intelligence agencies and entities building databases of potential contractors, and from publicly available registers (e.g., CBE).

We also collect, use, and share aggregated data, such as statistical or demographic data. Aggregated data may be derived from your personal data, but it is not considered personal data under the law because these data do not directly or indirectly reveal your identity. However, if we combine aggregated data with your personal data that directly or indirectly identifie you, we treat the combined data as personal data and will use it in accordance with this privacy notice.

How we collect personal data

Direct interactions. This is information you give us by filling in forms on the App, Web App or the Website or by corresponding with us. You give us the information when you create an account, order a payment card, apply for a credit or report a problem regarding our Services

etc. The information may include Identity Data, Contact Data, Financial Data, Transaction Data.

Automated technologies or interactions. Each time you interact with our App, Web App, Website or use our Services we may automatically collect Transaction Data, Technical Data, Usage Data and Location Data.

Third parties or publicly available sources. We may receive personal data about you from third-party and public sources as set out below:

- Banks you use to transfer money to the account(s) you hold with us;
- Business partners such as those who offer complementary services (such as investment advisory),
- Credit reference agencies, fraud prevention agencies or data brokers, including bodies charged with tasks in the public interest (e.g. the Official Belgian Gazette, the Individual Credit Register (ICR) and the file of non-governed registrations (ENR) of the National Bank of Belgium (NBB),
- Advertising networks, analytics providers and search information providers based inside and outside the EU,
- Providers of technical, payment and delivery services.

Specific cases of personal data collection. In some cases we can collect information about you whereas you do not have a direct relationship with us in the capacity of one of our clients as such. This may happen if

- You contact us to process your inquiry. The Bank collects the information about you needed to process and potentially process your inquiry (e.g., name, surname, contact information, and any other information you may provide in your inquiry).
- you are for example the beneficiary of a payment made by one of our clients or if you are a client's
    - family member or heir,
    - co-borrower / guarantor,
    - legal representative or contact person,
    - ultimate beneficial owner (UBO),
    - debtor (in case of bankruptcy),
    - creditor (in case of seizure requests),
    - shareholder, director or partner,
    - staff member.

When you share personal data with third parties, such as those listed above, please remember to inform them that we are processing their personal data and refer them to the current Privacy Policy. We will provide them with relevant information where possible and permitted by law (e.g., if their contact information is not provided, we will not be able to contact them).

Legal grounds and purposes for which we process your personal data

We will only process your personal data in accordance with the applicable laws, for the following legitimate purposes and based on the following legal grounds:

Contract. We need your personal data to conclude a contract with you and to carry out our obligations relating to your contract with us or in order to take steps at your request prior to entering into a contract.

If you have not concluded a contract with us, we do not process your personal data on the basis of a contract. We may, however, use your personal data for other purposes, such as fraud detection. We always check first whether using your personal data for those other purposes is permitted.

Legal obligation. We process your personal data to adhere to statutory requirements. As a bank we are subject to various legal obligations which require us to process your personal data. These include our obligations to combat and prevent fraud, money laundering and terrorist financing (AML-CTF) and our obligation to adhere to the rules of conduct in economic and financial law. In some cases, we are also subject to the obligation to disclose your personal data to judicial authorities, intelligence agencies and regulatory and supervisory authorities such as the Financial Services and Markets Authority (FSMA), the European Central Bank (the ECB), the National Bank of Belgium (NBB) and the Federal Public Services Economy and Finance (FPS Economy & FPS Finance). We must also comply with a number of obligations in application of the Foreign Account Tax Compliance Act (FATCA).

Legitimate interest. We have the right to process your personal data if it is necessary for the purposes of the legitimate interest pursued by the controller (us) or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms. Legitimate interests on the basis of our processing activities are for example the following:

1. Research. We study possible trends, problems, root causes of errors and risks in order to prevent complaints and losses. This way, we are able to intervene and issue a warning in time, if need be. We also study trends and our clients' preferences for

the purpose of analysation and continuous development of the products and services we offer.

2. New and improved products and services. We use our clients' personal data for the purpose of deploying and developing our products and services in order to keep up with our clients' evolving wishes and expectations.
3. Marketing relating to our products and services. We process your personal data for the purpose of direct marketing communications through analysing your needs, preferences, habits and situation, and to market and/or communicate our products and services to you.
4. Organizing and conducting competitions in accordance with the provisions of the regulations.
5. Risk management and protection of our legal rights. We use your personal data for the purpose of improving our risk management and to defend our legal rights, including:
    a. providing evidence of transactions you are involved in or communications between you and us;
    b. fraud prevention, for instance by detecting theft of your identity or credentials (e.g. phishing, theft of your ID document), unauthorised access to your data or device (hacking attempts);
    c. IT management, including infrastructure management, business continuity and IT security;
    d. establishing statistical models, (e.g. in order do to assess your credit risk score);
    e. performing internal control and audit;
    f. enforcement of claims and defence within legal disputes.

Public interest. We have the right to process your personal data if and insofar as it is necessary for reasons of substantial public interest (such as ensuring effective AML-CTF processes).

Consent. We may process your personal data if you have given us prior consent to do so for one or more specific purposes. You have the right to adapt or withdraw your consent at any time and free of charge. Adaptation or withdrawal of your consent will not affect past processing activities (the previous processing of your data remains lawful) but will affect and possibly annul those processing activities which were previously based on your consent in the event no other legal ground is available to us to rely on for the specific processing activity.

Further processing. We may use your personal data for other purposes than the purpose for which your personal data was initially collected. In that case, the new purpose must be in line with the purposes for which your personal data was initially collected. In those cases, we

will always check first if such further use of personal data is permitted, taking into account your rights and interests.

How we use your personal data for profiling and automated decision-making

As a credit institution, we make use of profiling. This entails that in certain situations we automatically assemble a profile using a set of your personal data. We do this for purposes of fraud detection when (potentially fraudulent) payment transactions are initiated, unusual transaction detection (based on risk profiles), client and product acceptance (based on profiles relating to creditworthiness) and direct marketing.

We make use of systems to make automated decisions. This helps us to make sure our decisions are quick and based on what we know. Automated decisions may affect the range of products, services or features offered to you now or in the future, or the price that we charge you for them. They are based on personal information that we have or that we are allowed to collect from others. Here are the types of automated decisions we make:

- Detecting fraud. We use your personal information to help decide if your account(s) may be being used for fraud or money-laundering. We may detect that an account is being used in ways that fraudsters work. We may also notice that an account is being used in a way that is unusual for you or your business. If we think there is a risk of fraud, we may stop activity on the account(s) or refuse access to them.
- Opening accounts. When you open an account with us, we check if the product or service is relevant for you, based on what we know. We also check that you or your business meet the conditions needed to open the account. This may include checking age, residency, nationality or financial position.
- Creating your profile (user profile). This means that through automated data processing, we can predict or evaluate various aspects of your personality, such as your age, gender, interests, economic situation, and location. This allows us to better tailor the content displayed or transmitted to your preferences and interests, allowing you to take advantage of better offers and saving you time.
- Approving credit. We use a system to decide whether to lend money to you or your business and on what conditions, when you apply for a credit such as a loan or credit card. This is called credit scoring. It uses past data to assess how you're likely to act while paying back any money you borrow. This includes data about similar accounts you may have had before. Credit scoring uses data from three sources:
  - Your application form
  - Credit reference agencies
  - Data we may already hold.

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or otherwise similarly significantly affects you. You can object to such automated decision-making, including profiling, by adjusting the settings in our App or Web App. We may perform a manual double check upon your request. You do not have this right if the decision is authorised by applicable laws we are subject to.

Use of your personal data for direct marketing purposes

If you have previously purchased a product or service from us, we are legally allowed to keep you informed about similar products and services we offer that are suited to your needs. This also applies if you are a visitor to our Website. In order to do this properly, we use various sources, such as the personal data that we received from you in the context of the contract and information we collect about you through your use of the App or Website.

Also other sources of information, including public sources, are relevant. We will always check first whether a public or another source of information can be used reliably. Where applicable, we will check whether you, as a client, have consented to the use of personal data that comes from another party. You have the unconditional right to object to our use of your personal data for direct marketing where this direct marketing is based on our legitimate interest and includes profiling and this at any time and free of charge. You can object to direct marketing by adjusting the settings in our App or Website

When you visit our App or Website we may, upon your specific consent, show you direct marketing material of our products or services or product or services of third-party partners which are deemed to be relevant to you personally. In such cases your data will not be transferred to such third-party partners. You have the unconditional right to adapt or withdraw your consent to our use of your personal data for direct marketing of third-party partners' products and/or services, and this at any time and free of charge. Withdrawal or adaptation of your consent is possible by adjusting the settings in our App or Website Please note that in such cases of withdrawal your will continue to see marketing material from third parties, which will however not be direct marketing and not based on your personal data, when using the App or Website.

We may, upon your specific consent, transmit advertisements of our products or services or products or services of third parties to you by e-mail or telephone. In such cases your data will not be transferred to such third-party partners. You have the unconditional right to adapt or withdraw your consent to our use of your personal data for direct marketing of third-party partners' products and/or services, and this at any time and free of charge. Withdrawal or adaptation of your consent is possible by adjusting the settings in our App or Website In cases of withdrawal we stop sending you advertisements by e-mail or telephone.

When you visit our App or Website, we can show you advertisements which we deem relevant to you personally based on cookies and similar technologies. In that case, you must have consented to our use of cookies and similar technologies to gather information about your activities on this site and other sites in order to provide you advertising based upon your browsing activities and interests. For more information about cookies, please see our Cookie Policy at www.unicredit.be/be-en/cookie-policy. You have the unconditional right to adapt or withdraw your consent to our use of your personal data for direct marketing of third-party partners' products and/or services, and this at any time and free of charge. Withdrawal or adaptation of your consent is possible by adjusting the settings in our App or Website In the event of withdrawal of your consent, you will only see generic advertisements from then on.

If you provide marketing consent, we will use the information collected about you from various sources, i.e., in connection with other processes (e.g., account management), and we will use it for marketing purposes, pursuing our legitimate interest (Article 6, paragraph 1, letter f of the GDPR). This data may be used for user profiling.

Who do we share your personal data with

In order to fulfil the aforementioned purposes, we only disclose your personal data to:

- UniCredit Group – We may share your data with other companies within the UniCredit Group. These companies help us improve our services, support customers, conduct business analysis, ensure security, and detect fraud. Sharing your data may be necessary for you to use our services.
- Payment processors and networks (e.g. Swift, Visa, Master Card),
- Credit reference agencies,
- Know Your Customer (KYC), analytical and cyber security providers,
- Business partners (those through whom we provide our Services);
- Financial or judicial authorities, state agencies, or public bodies, upon request and to the extent permitted by law;
- Certain regulated professionals such as debt collection agencies, lawyers, notaries or auditors;
- Marketing and analytics providers – to improve our services, we sometimes share information about you with providers such as Google Analytics. They help us analyze how users use the Website and App and support our online marketing. For more information, please see our Cookie Policy available at www.unicredit.be/be-en/cookie-policy
- Other third parties, but only with your prior consent.

Other service providers which process personal data on our behalf, we do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

International transfers of your personal data

In case of international transfers originating from the EEA to a non-EEA country which the European Commission has recognised as providing an adequate level of data protection, your personal data will be transferred on this basis. Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the EEA and the US.

For transfers to non-EEA countries of which the level of protection has not been recognised by the European Commission as adequate, we will either rely on a derogation applicable to the specific situation (e.g. if the transfer is necessary to perform our contract with you such as when making an international payment) or implement one of the following safeguards to ensure the protection of your personal data:

- Standard contractual clauses approved by the European Commission;
- Binding Corporate Rules.

How long do we keep your personal data

We will retain your personal data for the duration required for the purposes of processing as set out above, in order to comply with applicable laws and regulations or as is necessary with regard to our operational requirements, such as account maintenance, facilitating client relationship management, and responding to legal claims or regulatory requests.

The period for which we will retain information about you will vary depending on the type of information and the purposes that we use it for. For instance:

- Data used for the purpose of counteracting money laundering and terrorist financing and crime prevention – for 10 years, counting from the moment following the termination of the business relationship or a single transaction (in the absence of a business relationship);
- Data processed for tax documentation purposes – for 7 years, counting from January 1st of the year following the given settlement period;
- Data processed for accounting documentation purposes – for 10 years, counting from January 1st of the year following the given settlement period;

- Documents, recordings of telephone calls, electronic correspondence, and other information prepared, transmitted, or received in connection with provided services – for 5 years, counting from the first day of the year following the year in which the documents or information carriers were prepared or received;
- Customer complaints – until the expiration of the statute of limitations for potential claims arising from the agreement or other legal basis, determined in accordance with the provisions of applicable law;
- Inquiry or request from persons who are not our customers – for the period of handling and possible execution of your request, and after this period, we may store them for a period no longer than the period of potential claims' statute of limitations, resulting from generally applicable law;
- Data used for marketing purposes – until you object to the processing of your data for marketing purposes;
- Data processed based on your consent – until the expiration of the period for which the consent was given, or until it is withdrawn.

What are your rights and how can you exercise them

In accordance with applicable regulations, you have the following rights:

To access: you can obtain information relating to the processing of your personal data, and a copy of all your personal data that is processed by us.

To rectify: where you consider that your personal data are inaccurate or incomplete, you can require that such personal data be modified or completed accordingly.

To erase: you can require the deletion of your personal data. We are not always able to do this, however, and we do not always have to agree to do this, for example if we are required by law to keep your personal data for a longer period of time.

To restrict: you can request a restriction of the processing of your personal data if:

- you think that your personal data is incorrect;
- you think that we are not supposed to process your personal data;
- we want to destroy your personal data but you still need it (e.g. after the retention period has ended).

To object: you can object to the processing of your personal data, on grounds relating to your particular situation. You have the absolute right to object to the processing of your personal data for direct marketing purposes, which includes profiling related to such direct marketing.

To data portability: where legally applicable, you have the right to have the personal data you have provided to be returned to you or, where technically feasible, transferred to a third party.

To withdraw your consent: where you have given your consent for the processing of your personal data, you have the right to withdraw your consent at any time.

To request that we not base our decisions solely on automated processes, including profiling. You have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects for you or otherwise significantly affects you. You have the right to obtain human intervention from one of our employees, to express your position, and to challenge the decision. Despite your objection, we may continue to process your personal data provided that we demonstrate compelling legitimate grounds for processing that override your interests, rights, and freedoms, or grounds for establishing, pursuing, or defending legal claims.

You can exercise the rights listed above using the details set in Point 3. Please note that in case you contact us by Email or post you are required to provide at least your first and last name, signature and a copy of your ID document. Otherwise we won't be able to identify you and, consequently, take actions on your request. If you make a request on behalf of someone else, you must provide evidence of your authority to make such request.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We strive to respond to all legitimate requests within one month. If your request is particularly complex or we receive multiple requests from you, it may take us longer to process your request. In this case, we will inform you that it will take longer and keep you updated on the status of your request.

Complaints

If you have any complaints regarding this Privacy Policy or on how we protect or use your data, please contact our DPO using the contact details as set out above in Point 3. Please note that in case you contact us by Email or post are required to provide at least your first and last name, signature and a copy of your ID document. Otherwise we won't be able to identify you and, consequently, reply to your complaint.

If you have any concerns about our use of your personal data or if you feel like we have not addressed your questions or concerns adequately, you have the right to lodge a complaint at

any time with the Belgian Data Protection Authority, which regulates and supervises the processing of personal data in Belgium, by e-mail to contact@apd-gba.be, via their helpline on +32 (0)2 274 48 00 or by writing to Rue de la Presse 35, 1000 Brussels.

We would, however, appreciate the chance to deal with your concerns before you approach the relevant authority so please contact our DPO in the first instance.

Changes to this policy

As changes in the law or in our services and products may affect the way we use your personal data, we reserve the right to amend or modify this Privacy Policy, in accordance with the applicable laws. We will inform you of any material changes through our App or Website or through other usual communication channels. Your continued use of the App or Website after a modification of this Privacy Policy entails your acceptance of the modified Privacy Policy.