



PRIVACY STATEMENT

Last Update: 15/11/2024

This Privacy Statement applies to personal information held by eCREDO. It gives you information about how eCREDO collects and uses your personal data through your use of this website, including any data you may provide when you register as our customer depending on the service/products you use.

This Privacy Statement is issued on behalf of the eCREDO, any reference to 'we', 'us', 'our' in this Privacy Statement is a reference to eCREDO, unless otherwise stated. We place great importance on the protection of your privacy and are committed to handling your personal data in a transparent manner. All personal information is collected and processed in line with the relevant EU legal framework and specifically in compliance with the requirements of the General Data Protection Regulation (EU) 2016/679, the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) as amended and/or replaced from time to time, and any other related applicable legislation. This Privacy Statement describes the policies and practices regarding our collection and use of your personal data and sets forth your privacy rights.

In this Privacy Policy, any reference to "you", "your", "yours" is a reference to any of our customers, potential customers, visitors of our website, and/or an authorised person on your account which includes any of your shareholders, beneficial owners, principals, directors, representatives, contact persons and staff members. 'Personal Data' means any information relating to you that identifies you, directly or indirectly. 'Processing' means any operation or set of operations which is performed on personal data, such as collection, recording, storage, use, disclosure, erasure or destruction.

This Privacy Statement applies to the processing activities of eCREDO as data controller. eCREDO Limited with registration number HE394761 is an Electronic Money Institution, licensed and regulated by the Central Bank of Cyprus with License no. 115.1.3.56/2023 governed by in accordance with the laws of the Republic of Cyprus. eCREDO Limited operates under the brand name "eCREDO" and we provide payment solutions using the "eCREDO" trade name under license. Our headquarter and registered address is 21-23 Vasili Michailidi Street, 3026, Limassol, Cyprus.

Our principles

When we process your personal data, such data is:

(i) Processed lawfully, fairly and in a transparent manner with respect to the data subject ('lawfulness, fairness and transparency'); This means that we provide information to you regarding the processing of your personal data (transparency), that this processing matches the description given to you

(fairness), and that it is based on at least one of the lawful foundations set out in the GDPR (lawfulness)

(ii) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation'); This means that we specify exactly what your personal data is collected for, the purpose of its use, and that we will limit the processing of personal data only to the permissible and necessary extent to meet the relevant purpose

(iii) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); This means that we do not process any personal data beyond what is required

(iv) Accurate and, where necessary, kept up to date. Every reasonable step is taken to ensure that any personal data that are inaccurate with regard to the purposes for which they are processed are erased or rectified without delay ('accuracy'); This means that processes are in place to identify and address out-of-date, incorrect or unnecessary personal data

(v) Kept in a form which permits identification of data subjects only for the period necessary for the purposes for which their personal data are processed ('storage limitation'); This means that we store personal data only for the maximum required period, after which they are deleted in such a way that limits or prevents identification of the data subject

(vi) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Personal data we may collect and process

We collect and process different types of personal data provided by you, or your representatives in the context of delivering our products and services. We may also collect and process personal data, which we have lawfully obtained from other entities within our group, public authorities, business associates, or publicly available sources (such as online registers, websites, security searches and social media).

We collect your personal data when you use:

- Our website www.ecredo.com
- eCREDO's web application
- Any of the products and/or services available to you through the eCREDO Web App or website

We collect information you provide when you:

- Fill in any of our documents or forms
- Communicate with us (either through telephone, email, or our internet banking platform)
- Register to open an account or use any of our services
- Execute transactions and orders
- Respond to any of our queries or surveys
- Register to use our Web App
- Set up your preferences for certain types of products and services
- Give us access to your other financial accounts

- Contact us for any other reason
- Attend our events or events we sponsor

Such personal data may include, amongst others:

- Government issued identifiers and other identification data, such as passport, identification card, social insurance number, tax residency information, tax identification number and any other document you have provided for identification purposes
- Contact information, such as name, surname, billing and shipping address (including proof of address e.g., utility bill), telephone number, fax number, e-mail address, country of residence, details of the device you use (phone, computer or tablet) and or location identifier information
- Personal characteristics, such as date of birth country/place of birth, and nationality
- Financial data, such as data on transactions, IBAN, details of your payment instrument, including, but not limited to, payment account number, credit/financial institution and/or financial information including source of wealth, source of funds, tax income, earnings
- Functions and powers of relevant representative(s)
- Information on transactions and your use of our products and services.
- Employment and occupation information (including but not limited to CV, professional memberships, job title and responsibilities, professional qualifications)
- A record of correspondence/communication and/or the telephone call when you contact us. Such record may include your name, surname, e-mail address, telephone number, name of your company and other personal data you may disclose to us during such communication
- Your username (this is randomly and automatically assigned to you, but you will be able to change it), and other registration information
- Your picture in a photo or video form taken for verification purposes (where required as part of our Know Your Client (KYC) checks)
- If you sign up for our premium products, we may ask you to provide us with additional information. In order to be able to provide you with access to our concierge services or insurance cover we will share your name, contact details and information with our relevant partners
- Information from publicly available information to carry out our due diligence checks to comply with our anti-money laundering or sanctions screening obligations
- Photos/pictures or videos of you taken while attending any of our events or any event we sponsor for promotional, marketing, and archival purposes. This includes, but is not limited to, use on our website, social media platforms, print materials, and other marketing channels

If you provide us with personal data that belong to other people (such as your representative, secretary, employee etc), or you request us to share their personal data with third parties, you confirm that you have brought this Privacy Statement to their attention beforehand.

Other data

Whenever you use our website, Internet Banking, App, or any other system/tool provided by Us we collect the following information:

- Technical information, including the internet protocol (IP) address, login information, browser type and version, the time zone setting, the operating system and platform, the type of device you use, a unique device identified (for example IMEI number of your device, MAC address of the device's wireless network interface)
- Information about your visit and online behaviour, including the links you have clicked on, services you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page (subject to your cookie preferences)
- Company data, such as a company name, product and service offerings, jurisdiction
- Location data, if you turn location services on in the App

We do not provide any services to minors. However, certain transactions may be related to such persons. We may collect personal data in relation to minors who are under the age of eighteen (18) only if we have obtained the explicit consent from their parents or legal guardians or as otherwise permitted by law.

Purposes of processing your personal data

We may process your personal data for the following purposes:

- Meeting and executing our obligations under our business relationship and/or agreement entered into between us, including inter alia in relation to the provision of our financial services
- Processing transactions/payments
- Trading and investment
- Customer acceptance and onboarding procedures, customer communication, customer relationship purposes
- Enrolling/signing you up to any new payment feature provided by our payments networks
- Maintaining and developing our business with our customers or potential customers
- Operation, management and control of the affairs of our business and its purposes
- Maintaining our IT systems, including our human capital, administrative and management systems, processes and policies
- Monitoring against any possible fraud, money laundering, terrorism financing or crime risks
- Developing and carrying out identity verification procedures and processes for legal/regulatory compliance purposes;
- Conducting market research and carrying out marketing activities
- Ensuring that content from the website or App is presented in the most effective manner and to keep our website safe and secure
- Allowing you to use the interactive features of our website or App

- Administering our website or App

Legal basis for processing your personal data

Your personal data is used only for the purpose for which we collected it, unless there are reasonable grounds for using them for any other reason which is compatible with the original purpose. We process your personal data for the purposes mentioned above on the following legal basis:

(i) Processing is necessary for compliance with a legal obligation: In some cases, we have a legal responsibility to collect and store your personal data, in order to carry out various activities for the prevention of fraud and money laundering

(ii) Processing is necessary for entering in or performance of contractual obligations: We process your personal data in order to carry out our contractual obligations towards you as our customer or payer

(iii) Processing is necessary for the purposes of our own legitimate interests or for the legitimate interests of others: We process personal data based on our various legitimate interests, such as to protect you, prevent crimes, fraud and money laundering activities, actions to manage our business and further develop our services, direct marketing, risk management, investigate or settle enquiries or disputes, initiate legal claims and preparing a defence in the event of litigation, disclose information to other data recipients such as our service providers, auditors and technology providers, and/or to monitor and improve our relationship with you and/or to keep our internal records and/or to monitor communication to/from you using our systems and/or to protect the integrity of our IT systems

(iv) Processing is based on your consent: Insofar as you have granted us specific consent for processing, the lawfulness of processing is based on your consent.

Data retention

We will retain your personal data for a period necessary to fulfil the purposes listed above unless a longer retention period is required or permitted by the applicable law and any competent authority. Please be aware that we may be required to retain your personal data for various legal or regulatory reasons, for example, to ensure that transactions are appropriately processed, settled, refunded or charged-back, as well as to investigate any potential fraud and to comply with anti-money laundering and counter-terrorism financing laws and other legal requirements. This means that in the event that you, in the capacity of a payer or a customer, cease to make use of our services, we will still retain certain personal data in order to carry out our legal obligations.

eCREDO will keep personal data for as long as there is a business relationship with the Customer. Following termination of this agreement for any reason, any personal data the Customer has provided to eCREDO for the purposes of providing the services under this agreement shall remain in eCREDO's database for a period of up to ten (10) years in accordance with the directive of the Data Protection Commissioner (<http://www.dataprotection.gov.cy>). eCREDO may keep data for longer than 10 years if for any legal, regulatory or technical reason they cannot be deleted.

Please note that data related to prospective customers (customers who have not been onboarded) will be retained for 6 months.

Who we disclose your personal data to

Under certain circumstances we may disclose the personal data we have gathered about you to the following categories of recipients:

- Our group companies: To provide our services/products to you and for the purposes of collecting/updating/verifying your personal data in compliance with the relevant anti-money laundering compliance framework, we may share your personal data with our group companies (including their employees, sub-contractors, service providers, directors and officers) provided that your prior consent has been obtained
- Third-party credit and financial institutions, financial services partners, and payments networks including Visa and Mastercard: This may include, payment systems, intermediaries, payment service providers, credit and financial institutions based in Cyprus or abroad for facilitating the execution of transactions and any other services you request, and credit/financial institutions where you as a customer or a payer maintain your payment account or other type of account
- Card manufacturing, personalisation and delivery companies: We may share personal data to create and deliver your personalised cards
- Global compliance databases in line with our Know-Your-Customer and Due Diligence procedures
- Credit reference agencies: We may share personal data with credit reference agencies to conduct credit checks and obtain credit reports
- Third-party service providers and partners: We disclose personal data to service providers only when it is necessary to ensure the provision of our services, including, but not limited to processing of payments/transactions, or other added value providers in order to offer specific services to you. We will only share your personal data in this way if you have asked for the relevant service or if it is provided as part of a premium product we provide to you
- Our IT service providers and other companies: Who assist us with the effective operation of our business by providing technological expertise, penetration testing, file storage and record management, logistic services and solutions and other subcontractors
- Cloud computing and storage providers
- Our customers: We may disclose certain personal data, which you have provided to us or which we have received about you as a payer, to the relevant customers, to assist them with carrying out their legal obligations or their obligations towards you as their client
- Third parties in relation to a legal or regulatory obligation or if we are permitted to do so by law: Under certain circumstances we may have an obligation to disclose or share your personal data with auditors, regulatory authorities or law enforcement bodies to comply with a legal or regulatory obligation
- Persons acting on behalf of beneficial owners/shareholders of our clients/contractors being legal entities, including and not limited to payment recipients, beneficiaries, account nominees, intermediary, correspondent and agent banks

- Third parties in relation to transfer of business: For instance, if we sell any business or assets or merge with another business entity, it may be necessary to disclose personal data to the prospective business owners or partners
- Companies providing CCTV and security related management services for attending meetings or visiting our offices
- Companies or individuals you ask us to share your personal data with
- Analytics providers and search information providers to help us improve our website or App
- GDPR compliance when transferring data outside the EEA or if personal data is transferred to non-EEA countries that do not have an **adequacy decision** from the European Commission (i.e. Standard Contractual Clauses, Binding Corporate Rules).

Use of your personal data for marketing purposes

When we provide our products and services to you, and where national laws allow it, we will assume you want us to contact you by push notification, email, text message or post with information about our products, services and offers. Where national laws require us to get your consent to send marketing messages, we will do so in advance. Where the applicable law permits us to do so, we might use your personal data to personalise marketing messages about our products and services so they are more relevant to you, including analysing your transactions and how you use our services. You have the right to object to profiling for direct marketing purposes. You can also adjust your preferences through your account to opt-out or unsubscribe from receiving direct marketing materials at any time. In such cases however, you may still receive generic information about our products and services in our App.

Data collection purposes include:

- **Consent:** Requires explicit agreement from individuals and is appropriate when there is no other valid reason for processing data. It's necessary for actions like marketing or tracking cookies.
- **Legitimate Interest:** Used when processing is needed for the organization's interests, but balanced against the individual's privacy rights. It applies to activities like fraud prevention, some internal business operations, or even basic analytics.

Data transfer to third countries

Your data may be transferred to countries outside the European Economic Area to a recipient (i) who is in a country which provides an adequate level of protection for personal data or (ii) with appropriate safeguards pursuant to the provisions of applicable data protection laws (e.g. under an agreement in the form of standard contractual clauses for data transfer between EU and non-EU countries, adopted by the European Commission). In some (occasional) circumstances we may carry out such transfers where (i) we have obtained the explicit consent (active opt-in, rather than implied consent) from the

relevant data subject in respect of the proposed transfer, provided that the data subject has been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards; (ii) the transfer is necessary for the performance of a contract between the data subject and us, or (iii) the transfer is necessary for the performance of a contract concluded in the interest of the data subject between us and another person or (iv) the transfer is necessary for the establishment exercise or defence of legal claims.

Automated decision-making, including profiling

We do not take decisions solely on the basis of automated processing. However, some of your personal data may be processed by automatic means in order to evaluate certain personal aspects and other factors to predict risks or outcomes, in the following cases:

- Carrying out data evaluations, which may include KYC, identity, address checks, and payment transactions, in the context of fraud prevention, anti-money laundering and anti-terrorism financing measures. We do this for the efficient running of our services and to ensure decisions are fair, consistent, and based on the right information
- Marketing our services and products, subject to your consent
- Profiling is used to offer tailored services and detect fraud.

Your rights

You have certain rights in respect of the way we treat Your personal data:

(i) Right to access: You have the right to request a copy of the information that we hold about you. You have the right to confirmation as to whether we process your personal data and, where we do, access to the personal data, together with certain additional information. Such additional information includes inter-alia, details of the purposes of the processing, the categories of personal data concerned, and the categories of recipients of the personal data. The right to obtain a copy of your data shall not adversely affect the rights and freedoms of others

(ii) Right to rectification: You have the right to request rectification of inaccurate or incomplete personal data concerning you. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed

(iii) Right to erasure ("right to be forgotten"): You have the right to request erasure of personal data, where one of the following grounds applies:

- Personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
- You withdraw your consent on which the processing is based and where there is no other legal ground for the processing
- You object to the processing and there are no overriding legitimate grounds for the processing, or you object to processing for direct marketing purposes

- Personal data has been unlawfully processed
- Personal data must be erased for compliance with a legal obligation

However, as a regulated financial institution, we may not be able to accommodate your request for personal data deletion. Such erasure request cannot be accommodated where processing is necessary for (i) exercising the right of freedom of expression and information; (ii) for compliance with a legal obligation which requires processing by a law to which we are subject; and (iii) for reasons of public interest; or for the establishment, exercise, or defence of legal claims.

(iv) Right to restriction of processing: You have the right to obtain restriction of processing where one of the following applies:

- The accuracy of the personal data is contested for a period enabling us to verify the accuracy of the personal data
- The processing is unlawful, and you oppose the erasure of such data, and you request the restriction of their use instead
- We no longer need the personal data for the purposes of processing, but you require their retention for the establishment, exercise, or defence of legal claims
- You have objected to processing on the grounds of our legitimate interests, until we verify whether the grounds on which we process your information override your rights and freedoms

Where processing has been restricted on the basis of the above, we will continue to store your personal data. However, we will only otherwise process it (i) with your consent; (ii) for the establishment, exercise, or defence of legal claims; (iii) for the protection of the rights of another natural or legal person; or (iv) for reasons of important public interest.

(iv) Right to portability: you have the right to receive the personal data that you have provided us in a structured, commonly used, and machine-readable format, and you have the right to transmit this data to another organisation and/or request that we do it for you, provided that:

- The processing is based on your consent, or on a performance or conclusion of a contract
- Processing is carried out by automated means

(vii) Right to object: You have the right to object to the processing of your personal data, at any time and for reasons related to your particular situation, where the legal basis on which the processing activity is based is our legitimate interests. Should you exercise this right, we will no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights, and freedoms, or for the establishment, exercise, or defence of legal claims. Where you have objected to processing for direct marketing purposes, we shall no longer process your personal data for such purposes

(viii) Right to withdraw consent: Where the processing is based on your written consent, you have the right to withdraw consent at any time. To the extent that the legal basis for our processing of your personal data is consent (as and where applicable), you have the right to withdraw that consent at any time. Such withdrawal will not affect the lawfulness of processing before the withdrawal

(ix) Right to lodge a complaint: You can contact us for any matters related to your personal data as

detailed above. In case you are not satisfied or still have concerns, you may file a complaint with the Office of the Commissioner for Personal Data Protection. To find out how to submit a complaint, visit their [website](https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_en/page1i_en?openDocument) (https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_en/page1i_en?openDocument)

Cookies

Our website uses cookies in order to improve your experience. Our cookies policy can be found on our website.

Data security

All information provided by you to us is stored securely, and we use appropriate organisational, technical, and administrative measures to protect your personal data. Once your information is received, we use strict procedures and security features to prevent any unauthorised access. However, please note that neither the transmission of information via the internet nor its storage is completely secure, and no information system is guaranteed to be entirely secure. If you have any reason to believe that your interaction with us is no longer secure, please contact us immediately. Specific security measures can include; encryption and two-factor authentication.

Changes to this privacy statement

We may update this Privacy Statement from time to time by publishing a new version on our website. You should check this page occasionally to ensure you are happy with any changes. If the changes are substantial, we may notify you of changes by email.

Contact information

Further information and/or queries and/or requests regarding the processing of your personal data and any of your rights with respect to your personal data can be requested by contacting us in writing as follows:

By email: dpo@ecredo.com

By phone: +357 25 508500

By post: 21-23 Vasili Michailidi, Limassol, 3026, Cyprus

For security reasons, we may ask you for proof of identity. If a third party exercises one of these right on your behalf, we may need to ask for proof that they have been authorised to act on your behalf.