Velare Privacy Policy

Version 1.0 | Effective date 01-January-2026

This policy explains how EC VELARE PTE. LTD. ("Velare", "we", "us" or "our") handles personal data in connection with the Velare website, client portal, card programme and customer support. It also explains how you can contact us about your information.

1. Who This Policy Covers

This policy applies to visitors, applicants, cardholders and people who contact us. For a business account, it also covers authorised users, directors, beneficial owners and other individuals whose information is needed to administer or verify the account.

European Credit Investment Bank Ltd ("ECIB") supports customer operations for the programme. Information needed to handle an application, service request or security report may be shared with ECIB for those purposes. Our card issuer and other payment providers may also handle information under their own legal duties and privacy notices. Those notices apply to their separate processing and do not replace our responsibilities under this policy.

2. Personal Data We Handle

The information relevant to your use of Velare may include:

- Identity and verification information, such as your name, date of birth, nationality, identity document, address and verification results. A verification provider may request a photograph or identity check through a designated secure process.
- Contact and account information, such as your registered email, telephone number, account identifiers, account status and authorised user permissions.
- Financial and transaction information, such as funding account details, source of funds information, balances, card identifiers, payments, merchant details, refunds and disputes.
- Business information linked to individuals, including positions held, ownership, authority to act and supporting documents for corporate verification.
- Service and security records, including correspondence, support tickets, complaints, suspicious activity reports, verification events, card restrictions and investigation records.
- Technical information generated when you use our services, such as IP address, browser and device information, session events and security logs. Cookie information is explained in Section 7.

We seek information relevant to the service, verification or legal requirement involved. Please do not send passwords, PINs, one-time passwords or card security codes in an email or support ticket.

3. Where Information Comes From

We obtain information from you when you apply, use the portal, make payments or contact us. We also receive information from an authorised business representative, the issuer, payment networks, funding institutions and providers that help verify identity or detect fraud. Where permitted, we use official registers, screening sources and other reliable public information for due diligence.

If you provide another person's information, you must have authority to do so, give them this policy and obtain any consent required by law. A business should tell its authorised users how it administers their access and which account information its administrators can see.

4. Why We Use Personal Data

We use relevant personal data to:

- Assess applications, verify identity and authority, perform customer due diligence and maintain accurate account records.
- Administer the programme, issue and manage cards through the issuer, process supported funding and payments, and show balances and transaction records.
- Authenticate access and instructions, operate security controls, investigate suspicious activity and handle card restrictions or reactivation requests.
- Respond to enquiries, provide service updates, investigate complaints and help with transaction disputes or recovery requests.
- Meet applicable legal, regulatory, screening, audit and recordkeeping requirements, and respond to lawful requests from authorities.
- Maintain and improve service reliability, diagnose faults and understand use of our services using information appropriate to that purpose.
- Send optional marketing communications where you have consented or another lawful permission applies.

5. Consent And Other Permitted Uses

We collect, use and disclose personal data with consent where required, including any form of consent recognised by applicable law. We may also handle data without consent where the law permits or requires it, for example for specified compliance, investigation or other lawful purposes. We do not treat this policy as unlimited permission to use your data.

If information is necessary for identity checks, fraud prevention or payment processing, we may be unable to open or continue an account without it. We will explain the relevant consequence where appropriate. We will notify you of a materially different purpose and obtain any additional consent required before using your information for that purpose.

6. When We Share Information

We share information relevant to the purpose with ECIB and authorised programme personnel; the card and wallet issuer; payment networks and processors; banks and other payment institutions involved in a transaction; and providers of verification, screening, hosting, security and support services. We also share information with professional advisers, auditors, regulators, courts and law enforcement where there is an appropriate lawful basis.

For a business account, an authorised administrator may receive information about users and transactions within that business's account permissions. We may disclose necessary information in connection with a proposed or completed business transfer, subject to appropriate confidentiality and legal requirements.

Service providers handling information for us must act within the agreed purpose and applicable protection requirements. An issuer, bank or authority acting under its own duties may retain and process information independently. Where MatchMove provides services for your account, its privacy notice is available at https://www.matchmove.com/privacy. Please also review the issuer documents supplied for your programme.

7. Cookies And Marketing Choices

Our website and portal may use cookies or similar storage needed for functions such as sign-in, security and remembering a session. Where optional analytics or advertising technologies are used, the applicable cookie notice or preference control will explain their purposes and choices. We will obtain consent where required. Blocking essential storage through your browser may prevent parts of the portal from working.

You can decline optional marketing or withdraw your marketing preference through an unsubscribe option or by emailing velare@ecibank.com. This does not stop necessary messages about security, transactions, changes to your account or a service you have requested. We will follow applicable direct marketing rules, including Singapore Do Not Call requirements where relevant.

8. Overseas Processing

Your account and international payments may involve organisations in different countries. Information may therefore be processed outside the country where you live or where it was collected. Where Singapore transfer restrictions apply, we will use arrangements that meet those requirements, including a comparable standard of protection where required. Contact us if you need information about the transfers relevant to your account.

9. How Long We Keep Information

Retention depends on the record and the reason it is held. We retain account and transaction information, due diligence records and correspondence for as long as needed for the service, applicable legal or regulatory requirements, audits, investigations and legal claims. Closing an account does not necessarily end those obligations. When there is no continuing lawful business or legal need, we will delete, anonymise or securely dispose of the information. Retention by an independent issuer or authority is governed by its own obligations.

10. Keeping Information Secure

We use reasonable organisational and technical safeguards appropriate to the information and the risks involved. These include restricting access to people who need it for their duties and requiring appropriate handling by service providers. No method of transmission or storage can eliminate every risk.

Use secure devices, keep your registered contact details current and protect your login credentials. If you suspect account compromise, use the emergency steps in the Client Service Level Agreement and report it through the portal or velare@ecibank.com. We assess personal data incidents and notify affected individuals and authorities where required by applicable law.

11. Your Requests And Choices

You may contact us to request access to your personal data and information about its use or disclosure, correct inaccurate information, withdraw consent, or raise a privacy concern. You may also ask us to review whether particular information still needs to be retained. The availability and scope of each request depend on applicable law; this policy does not promise an unconditional right to deletion or transfer of records.

We may verify your identity and authority before acting on a request. We will respond within the applicable legal period and explain any lawful restriction or need for additional time. If a permitted fee applies to an access request, we will explain it before proceeding. Withdrawal of consent operates prospectively and does not prevent processing that remains permitted or required by law. We will explain if withdrawal affects our ability to provide a service.

12. Contact For Privacy Matters

Email velare@ecibank.com with the subject "Privacy Request — Attention Data Protection Officer". Include your registered name, registered email and a brief description of your request. If relevant, include your support reference or the last four digits of the affected card. We will direct the request to the person responsible for data protection. We will arrange a suitable channel if identity documents or other sensitive evidence are necessary.

You may raise a concern with the relevant data protection authority. For matters within Singapore's jurisdiction, information about the Personal Data Protection Commission is available at https://www.pdpc.gov.sg.

13. Children And Third Party Services

The card programme is intended for eligible adults and authorised business users. It is not designed for children. Contact us if you believe a child has supplied personal data without appropriate authority. External websites and services, including supported mobile wallets, have their own privacy notices. Review those notices before using them.

14. Changes To This Policy

We will publish updates with a revised effective date and give additional notice of material changes where appropriate or legally required. A policy update does not replace any consent that the law requires us to obtain. You can request the version relevant to your account by contacting us.