

Privacy Policy

ERIUS PHONE · Version 1.1 · Effective 13 October 2026

Protremix Technology Limited · Licence no. 07011554 (Innovation City Authority, Government of Ras Al Khaimah) · Office A, Innovation City Business Centre, RAK BANK ROC Office, Ground Floor, Al Rifaa, Sheikh Mohammed Bin Zayed Road, Ras Al Khaimah, United Arab Emirates

This Policy explains what personal data Protremix Technology Limited processes when you visit eriusphone.com or use ERIUS PHONE, why, for how long, who receives it and what rights you have.

1. Who is responsible

- 1.1 The controller of the personal data described in this Policy is Protremix Technology Limited, business licence no. 07011554 issued by the Innovation City Authority, Government of Ras Al Khaimah, Office A, Innovation City Business Centre, RAK BANK ROC Office, Ground Floor, Al Rifaa, Sheikh Mohammed Bin Zayed Road, Ras Al Khaimah, United Arab Emirates (**Protremix, we, us**).
- 1.2 We handle personal data under the laws of the United Arab Emirates. This Policy is written with reference to Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the **PDPL**). We hold no data-protection or security certification and this Policy does not claim that any authority or auditor has confirmed compliance with a law or standard.
- 1.3 Contact for any matter in this Policy: info@eriusphone.com, or by post to the address in clause 1.1.
- 1.4 Words defined in the Terms of Service have the same meaning here.

2. Two roles: your data and your customers' data

- 2.1 **Where we are the controller.** For data about visitors to our website, about people who ask for access, and about Customers and their use of the Service (rows 3.1 to 3.4 and 3.10 to 3.12 of the table below), we decide why and how it is processed, and this Policy applies in full.
- 2.2 **Where we act for a Customer.** The contents of a Device, files uploaded to it and the content of Calls (rows 3.5 to 3.9) are Customer Data. The Customer decides what is put there and why, and we process it on the Customer's behalf under the Data Processing Addendum. If you are a Guest in a Call, or your data is on a Customer's Device, the Customer is responsible for telling you how it uses your data, and requests about that data should go to the Customer first. We will pass on any request we receive.

3. What we process, why, and for how long

No.	Data	Source and content	Purpose	Kept for
3.1	Access request	Email address and anything you choose to add on the website form; time, IP address and browser user-agent	To answer the request; to detect spam and abuse	Until you ask us to delete it or we close the request list
3.2	Sign-up	Email address, device type chosen, IP address, browser user-agent, status of the request, times. The confirmation link is stored as a hash and works once, for 24 hours	To verify the address and create the Account; to enforce sign-up limits	For the life of the Account; a record of the email address and of the dates the Account was created and closed is kept afterwards (clause 6.3)

No.	Data	Source and content	Purpose	Kept for
3.3	Account	Account identifier, contact email, plan and trial dates, a one-way hash of each API Key (never the key)	To provide the Service and authenticate requests	For the life of the Account
3.4	API audit log	Per request: time, Account, a short fingerprint of the key, IP address, method, path, Device, action, response status, duration; for app installs, launches, stops and removals the package name. No request bodies: no typed text, no web addresses opened, no intents, no keys	To operate and secure the Service, investigate faults and detect abuse	A rotating file: when it reaches 50 MB it is set aside and a new one is started; one earlier file is kept and the one before it is overwritten
3.5	Device contents	Whatever the Customer and its Agent place on a Device: applications, application data, signed-in accounts, files, messages, browser history	To provide the Device	Until the Customer removes it or the Device is deleted
3.6	Uploaded files	Application packages, and audio or video clips supplied for the Device's virtual microphone or camera	To install the application or play the clip	Application packages: deleted after installation unless the Customer asks for them to be kept. Clips: until replaced or removed
3.7	Call records	Per Call: Account, Device, call application, times of ringing, connection and end, duration, Call Minutes used and charged, outcome. The other party is stored only as a keyed hash, never as a name or number. A ledger of every change to the Call Minutes balance	To meter Calls, show the balance and resolve billing questions	For the life of the Account and afterwards for as long as accounting and tax law requires
3.8	Call content	During a Call the Guest's voice and, if the Guest shares it, video are streamed to third-party AI voice and avatar services so the Persona can hear and answer. We do not record the audio or video of Customers' Calls. The text of what the Guest said, as transcribed, and of what the Persona replied is written to a log on our server	To operate the Persona; to investigate faults and abuse	Audio and video: not stored by us. Text log: not deleted automatically at present; deleted on request (clause 6.4)
3.9	Call screen images	Where the visual function is enabled for a Call, still images of the Device's call screen, which shows the other party's video, are captured every few seconds and sent to the third-party AI service so the Persona can respond to what is shown. At the Effective Date this function is not enabled for Customer Accounts	To operate the Persona	7 days, then deleted
3.10	Support	Tickets: subject, messages and our replies, the Device named. Website contact form: name, email address, subject and message. Support assistant: the messages you send it and its replies, stored per Account	To answer you and keep a record of what was agreed	For the life of the Account, or until you ask us to delete it
3.11	Billing (not yet in force)	When paid plans open: the plan bought, amounts, dates, a customer and transaction reference from the payment processor. We do not receive or store full card numbers	To take payment, credit Call Minutes, keep accounts	As long as accounting and tax law requires

No.	Data	Source and content	Purpose	Kept for
3.12	Website and server logs	IP address, time, address requested, referring page, browser user-agent. Separately, a page-view count with a campaign tag that holds no IP address and no visitor identifier. Analytics and advertising cookies: see the Cookie and Tracking Notice	To run and secure the website; to measure which announcements work	Web server logs: 14 days. Cookies: as stated in the Cookie Notice

4. Legal bases

- 4.1 We process the data in rows 3.2 to 3.10 because it is necessary to perform the contract with the Customer, or to take steps at the request of a person before entering into it.
- 4.2 We process the data in row 3.11, and keep the records in row 3.7 after an Account closes, to meet obligations under accounting and tax law.
- 4.3 We process the data in rows 3.1, 3.4 and 3.12 to keep the Service and the website secure and working, which is necessary to provide them to you.
- 4.4 We set analytics and advertising cookies on the basis described in the Cookie Notice. Where the law requires consent, we ask for it and you may withdraw it at any time.
- 4.5 For Customer Data, the Customer is responsible for having a lawful basis, including any consent of a Guest that the law requires.

5. Who receives personal data

- 5.1 We do not sell personal data and do not share it for anyone else's advertising.
- 5.2 The following categories of recipient process personal data on our behalf, each only as needed for its task:

Category	What it receives
Hosting and data-centre provider	Everything stored on our servers, as infrastructure. It has no access to the content in the ordinary course
Third-party AI voice and avatar services	During a Call: the Guest's audio, the Persona's speech, and where enabled the call screen images
Third-party AI language-model service	The messages you send to the support assistant and the Account information it looks up to answer you
Email service provider	Your email address and the content of emails we send you
Payment processor (when paid plans open)	Your payment details and the purchase
Analytics and advertising provider	Website visit data, as described in the Cookie Notice
Blog publishing provider	When you open the Blog page: your IP address and browser details, as described in the Cookie Notice
Public connection servers (STUN) operated by network providers	When a Call is set up: the public IP address of the Guest's browser and of the Device, so that the two can connect directly. These servers receive no audio, video or other content of the Call

- 5.3 We may disclose personal data where the law or an order of a competent authority requires it, or where it is necessary to establish or defend a legal claim or to protect a person or the Service from serious harm.

- 5.4 If the business of the Service is transferred, personal data will pass to the successor, which will remain bound by this Policy until it is changed in accordance with clause 12.

6. Retention and deletion

- 6.1 The retention periods are stated in the table in clause 3. Where no fixed period is stated, we keep the data for as long as the Account exists or until you ask us to delete it.
- 6.2 When an Account is closed we delete its Devices and their storage, its private network, its API Key hashes and its calling configuration. Deleting a Device is permanent.
- 6.3 After closure we keep a record that the Account existed (the contact email address and the dates of creation and closure) to prevent abuse of sign-up limits and to answer later questions, and the call and billing records that the law requires us to keep.
- 6.4 The Call text log in row 3.8 is not yet subject to automatic deletion. On request from the Customer we delete the entries of its Calls.
- 6.5 We take encrypted backups of the Service every day and keep fourteen daily and eight weekly copies. Data deleted from the live Service remains in those backups until they expire, and is not restored except to recover the Service.

7. Where data is stored and international transfers

- 7.1 The Service runs on servers that we rent in data centres in the European Union. Backups are stored, encrypted, on other servers that we operate in the European Union.
- 7.2 We are established in the United Arab Emirates and operate the Service from the United Arab Emirates and other countries. The recipients in clause 5.2 may process data in other countries, including the United States of America. Personal data is therefore transferred to, and accessed from, countries other than the one in which you live, some of which may not give the same protection as your own.
- 7.3 Where the law that applies requires a safeguard for such a transfer, we rely on the contract terms offered by the recipient and on the necessity of the transfer to perform the contract with you.

8. Security

- 8.1 The measures in place at the Effective Date are:
- (a) each Device runs in its own isolated container on its own private network, and an API Key reaches only the Devices of its own Account;
 - (b) API Keys are stored only as one-way hashes;
 - (c) connections to the website, the Dashboard and the API are encrypted in transit;
 - (d) the debugging interface of a Device is not exposed to the internet;
 - (e) uploaded files are held in a restricted area from which nothing can be executed;
 - (f) API requests are recorded in the audit log described in row 3.4;
 - (g) backups are encrypted and are written to stores from which the production server cannot delete;
 - (h) the integrity of production files and the isolation between Accounts are checked by automated tests on a schedule;
 - (i) logs and databases are readable only by the people who operate the Service.

- 8.2 Devices are not end-to-end encrypted against us. People who operate the Service have the technical ability to access a Device and its contents. We do so only to operate and maintain the Service, to act on your request, to investigate a suspected breach of the Terms, or where the law requires.
- 8.3 No system is completely secure. If we become aware of a breach of security that affects your personal data and is likely to put you at risk, we will tell you without undue delay and will notify the competent authority where the law requires.

9. Your rights

- 9.1 Subject to the conditions and exceptions in the law that applies to you (in the United Arab Emirates, the PDPL), you may ask us to:
- (a) confirm whether we process your personal data and give you a copy of it;
 - (b) give you the data you provided in a structured, commonly used form;
 - (c) correct data that is inaccurate or incomplete;
 - (d) delete your data, or restrict or stop its processing;
 - (e) not be subject to a decision based solely on automated processing that has legal or similarly significant effects on you. We make no such decisions.
- 9.2 To exercise a right, write to info@eriusphone.com from the email address on your Account, or open a support ticket in the Dashboard. We may ask for information to confirm your identity. We answer within thirty (30) days and do not charge a fee unless a request is manifestly unfounded or repetitive.
- 9.3 Where processing is based on consent you may withdraw it at any time. Withdrawal does not affect processing carried out before it.
- 9.4 You may complain to the data-protection authority that is competent for you. In the United Arab Emirates that is the UAE Data Office.

10. Children

- 10.1 The Service is offered to businesses and adults. It is not directed at persons under eighteen (18), and we do not knowingly collect their personal data. If you believe a child has given us personal data, contact us and we will delete it.

11. Automated processing and AI

- 11.1 A Persona and the support assistant generate their replies automatically using AI systems. Their output is not reviewed by a person before it is delivered.
- 11.2 We do not use the contents of Devices, the content of Calls or support messages to train AI models. The third-party AI services process this data on our behalf to provide the function concerned; their own retention for abuse monitoring is governed by their terms.

12. Changes to this Policy

- 12.1 We may change this Policy. We publish each version with a new version number and date, record it in the version history, and for a material change notify Customers by email or in the Dashboard before it takes effect.

Version history

Version	Effective date	Change
1.0	13 October 2026	First published version. archived PDF
1.1	13 October 2026	Clause 5.2: two categories of recipient added that were already in use when version 1.0 was published (the blog publishing provider, and the connection servers used to set up a Call). Clause 9.1: reference to the PDPL. No change to how personal data is processed.