Acceptable Use Policy

ERIUS PHONE · Version 2.0 · Version 2.0 effective from 15 October 2026

Golan Europe S.L. · CIF B16546020 · Registro Mercantil de Islas Baleares, Tomo 2729, Folio 223, Sección 8, Hoja PM-82642 · Av. Blai Bonet 8, Bl. 3, Apartamento 301, Santa Ponça, 07180 Calvià, Illes Balears, Spain
Development: Protremix Technology Limited

This Policy sets out what Customers and their Agents may not do with ERIUS PHONE. It forms part of the Terms of Service.

1. Application

1.1 This Policy forms part of the Terms of Service. Words defined there have the same meaning here. It applies to the Customer, to every person the Customer allows to use its Account and to every Agent acting under its API Keys.

1.2 A Device is a real Android system with a real connection to the internet, running on hardware shared with other customers. What is done on it is attributed to the Customer.

2. Unlawful and harmful use

2.1 You must not use the Service, or allow it to be used:

(a) in breach of any law or regulation that applies to you, to the persons you contact or to us, including the laws of Spain and of the European Union;

(b) to commit or facilitate fraud, deception, extortion, money laundering or the evasion of sanctions or export controls;

(c) to create, store or distribute content that is unlawful, that sexually exploits or endangers children, that incites violence or hatred, or that infringes another person's intellectual-property, privacy or other rights;

(d) to harass, threaten, stalk or defame any person;

(e) to obtain or process personal data without a lawful basis, or to track or profile a person without their knowledge.

3. Calls

3.1 In relation to Calls you must not:

(a) place Calls that are unsolicited marketing, automated bulk calls or spam, or call a person who has asked not to be contacted;

(b) use a Persona to make a person believe they are speaking with a human being, or to impersonate a real person, a public authority, a bank, an employer or any organisation you do not represent;

(c) remove, hide, mute, talk over or contradict the AI disclosure applied by the Service, or instruct a Persona to deny that it is an AI system;

(d) record, transcribe or monitor a Call by your own means without the notice or consent that the law of the Guest's location requires;

(e) use Calls to obtain passwords, payment details, one-time codes or other security credentials from a person by deception;

(f) use Calls to contact emergency services, or present the Service as a means of reaching them;

(g) use Calls to give medical, legal or financial advice, or to make a decision about a person that has legal or similarly significant effect, without qualified human involvement.

3.2 The AI Disclosure Policy sets out how Calls are labelled and what you must tell Guests.

4. Accounts, automation and third-party services

4.1 You must not:

(a) create accounts in bulk on a Third-Party Application, or create or operate accounts under false identities, in breach of that provider's terms;

(b) manipulate ratings, reviews, votes, advertisements, follower counts or other engagement measures;

(c) send bulk or unsolicited messages through any application on a Device;

(d) circumvent the access controls, rate limits, fraud checks or device-integrity checks of a Third-Party Application;

(e) use a Third-Party Application on a Device in a way that its provider's terms prohibit.

5. Security and integrity of the Service

5.1 You must not:

(a) attempt to break out of a Device's container, reach another customer's Device or network, or access the host system;

(b) scan, probe or attack our infrastructure, another customer or any third party from a Device, or use a Device as a relay for such activity;

(c) install or distribute malware, or operate command-and-control, phishing or credential-harvesting infrastructure;

(d) mine cryptocurrency or run workloads intended to consume shared resources to the detriment of others;

(e) interfere with metering, evade a limit on Devices, uploads or requests, or use more than one Account to obtain repeated trials;

(f) share an API Key outside your organisation or publish it.

5.2 Testing the security of your own application on your own Device is permitted. Testing our Service is permitted only under the Security Contact and Vulnerability Disclosure.

6. Enforcement

6.1 We may investigate a suspected breach of this Policy, and for that purpose may examine the audit log, the Call records and, where necessary and proportionate, the contents of the Device concerned.

6.2 If we reasonably believe this Policy has been breached we may remove content, suspend a Device, the Calls function or the Account, or terminate, as provided in clause 15 of the Terms. Call Minutes and Fees are not refunded where an Account is closed for breach.

6.3 We may report suspected unlawful activity to the competent authorities and disclose the relevant information where the law requires or permits.

6.4 To report abuse of the Service, write to info@eriusphone.com with the details you have.

Version history

Version	Effective date	Change
1.0	13 October 2026	First published version.
2.0	15 October 2026	The owner, seller and provider of ERIUS PHONE is now Golan Europe S.L. (Spain), the only party to the contract with Customers. Governing law, data-protection references and consumer rights changed to Spanish and EU law. Contact address for legal, privacy and refund matters: info@eriusphone.com. Clause 2.1(a): laws of Spain and of the EU.