Privacy Policy

ERIUS PHONE · Version 2.1 · Version 2.1 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 explains what personal data Golan Europe S.L. 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 Golan Europe S.L., a Spanish private limited company (sociedad de responsabilidad limitada) with tax identification number (CIF) B16546020, registered in the Registro Mercantil de Islas Baleares, Tomo 2729, Folio 223, Sección 8, Hoja PM-82642, with its registered office at Av. Blai Bonet 8, Bl. 3, Apartamento 301, Santa Ponça, 07180 Calvià, Illes Balears, Spain (**Golan Europe**, **we**, **us**).

1.2 We handle personal data under Regulation (EU) 2016/679, the General Data Protection Regulation (the **GDPR**), and the Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (the **LOPDGDD**). 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, including a request to exercise your rights: info@eriusphone.com, or by post to the address in clause 1.1. We have not appointed a data protection officer; all data-protection questions are handled at this address.

1.4 Words defined in the Terms of Service have the same meaning here.

1.5 The software of the Service is developed and operated for us by an external software developer, named in the "Development" line at the end of this document. It processes personal data only on our behalf and on our instructions, under a data processing agreement (clause 5.2 and clause 7).

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, the content of Calls, the instructions given to the agent and the agent's memory (rows 3.5 to 3.9, 3.13 and 3.14) 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, the voice and face chosen for the Persona (a woman's or a man's), whether the agent's memory is to be on, 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)
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. A stopped Device: seven (7) days after it is stopped (clause 6.2)
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. What the Guest says is transcribed to text; during the Call that text is held in working memory only. Our log of a Call records times, events and the length of each utterance, not its text. Where the Customer has connected its own agent, the Guest's questions, as restated by the Persona, are sent to that agent as text (clause 5.5)	To operate the Persona and the agent; to investigate faults and abuse	Audio, video and the text of the Call: not stored by us, except as a summary and facts in the agent's memory (row 3.14). Text logs written before the Effective Date of version 1.2: clause 6.4

No.	Data	Source and content	Purpose	Kept for
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
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
3.13	Agent settings	Per Device: the Persona, whether Calls are voice only or voice and video, whether the hosted agent or the Customer's own agent answers, the agent's name and language, the Customer's instructions to it (up to 1,500 characters); for an own agent, its web address, model name and access key. The access key is stored on our server, is never shown again after it is saved and is never written to a log	To operate the agent the Customer has chosen	Until changed by the Customer, or the Device is deleted
3.14	Agent memory	Where the hosted agent answers a Device's Calls and its memory is on (for an Account opened on or after 13 October 2026 it is on unless the Customer unticks it at sign-up; for an Account opened earlier it is off until the Customer turns it on): after each Call, a short summary and up to forty (40) short facts about the caller and the matters discussed, written by a third-party AI language-model service from the text of that Call and the existing memory. One memory per Account, used at the start of later Calls on any Device of that Account and of no other Account. The Customer can read it and delete it in the Dashboard or through the API	To let the agent continue a conversation across Calls	Until the Customer deletes it, or the last Device of the Account is deleted. Turning the memory off stops its use and update but does not delete it

4. Legal bases

4.1 We process the data in rows 3.2 to 3.10, 3.13 and 3.14 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 (Article 6(1)(b) GDPR). For row 3.1 the basis is the same, applied to the steps you ask for before a contract.

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 Spanish accounting and tax law (Article 6(1)(c) GDPR). These records are kept for six (6) years under Article 30 of the Spanish Commercial Code, or longer where tax law requires.

4.3 We process the data in rows 3.1, 3.4 and 3.12, and use rows 3.2 and 3.3 to enforce sign-up limits, for our legitimate interest in keeping the Service and the website secure and working and in preventing abuse (Article 6(1)(f) GDPR). You may object to this processing under clause 9.1(f).

4.4 We set analytics and advertising cookies only with your consent (Article 6(1)(a) GDPR and Article 22.2 of the Spanish Law 34/2002 on Information Society Services, **LSSI**), as described in the Cookie Notice. You may withdraw consent 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
Software developer and operator of the Service (the Developer, clause 1.5; United Arab Emirates)	All data on our servers, as needed to develop, operate, maintain, secure and support the Service on our behalf
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. After a Call in which the agent's memory is on: the text of that Call and the existing memory, to write the updated memory (row 3.14)
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.

5.5 **A Customer's own agent.** A Customer may connect its own agent to a Device by giving us the web address of a service that answers in the standard chat-completions format. During each Call of that Device we then send to that address, as text, the questions of the Call as restated by the Persona, together with the earlier questions and answers of the same Call, and the Persona speaks the answer. The Customer chooses that service and is responsible for it; it is not our recipient or sub-processor, and what it does with the data

is governed by the Customer's own arrangements. We send the data only to a public internet address over an encrypted connection.

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. When an early-access trial ends without a paid plan, or a paid plan ends because it was cancelled or its renewal was not paid, the Device is stopped, not deleted: it and its data are kept for seven (7) days so that you can subscribe or renew and continue, and are then deleted. We tell you by email when the Device is stopped, with the date on which it will be deleted.

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 Since the Effective Date of version 1.2 of this Policy the text of Customers' Calls is not written to a log. Before that date the text of what the Guest said and of what the Persona replied was written to a log on our server; that log is not subject to automatic deletion, and 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.

6.6 The agent's memory (row 3.14) is deleted when the Customer selects "Forget everything" in the Dashboard or sends the deletion request through the API, and when the last Device of the Account is deleted. A Guest who wants a fact removed from it should ask the Customer; if the request reaches us, clause 2.2 applies.

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 Spain. Our Developer operates the Service from the United Arab Emirates, and other recipients in clause 5.2 may process data in other countries, including the United States of America. Personal data is therefore accessed from, and transferred to, countries outside the European Economic Area (EEA).

7.3 For each transfer outside the EEA we rely on an adequacy decision of the European Commission where one exists (for recipients in the United States, the EU-US Data Privacy Framework where the recipient is certified), and otherwise on the Standard Contractual Clauses adopted by the European Commission (Implementing Decision (EU) 2021/914), with additional measures where needed. The United Arab Emirates has no adequacy decision; the transfer to our Developer is covered by Standard Contractual Clauses. You may ask for a copy of the safeguards at info@eriusphone.com.

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;

(j) the agent's memory of each Account is stored in its own file, readable only by the service that operates the agent and by the people who operate the Service, and the Account to which a Call belongs is taken from our device register, not from any account identifier carried by the Call;

(k) the access key of a Customer's own agent is never returned by the API or the Dashboard and is never written to a log, and the address of an own agent is checked, when it is saved and again at each connection, to be a public internet address.

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 in Articles 15 to 22 of the GDPR, you have the right to 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;

(f) stop processing your data on the basis of our legitimate interests (clause 4.3), on grounds relating to your particular situation, and in any case for direct marketing.

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 one (1) month, which may be extended by two further months for complex or numerous requests, and do not charge a fee unless a request is manifestly unfounded or excessive.

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 a data-protection supervisory authority, in particular in the EU Member State where you live or work. Our lead authority is the Spanish Agencia Española de Protección de Datos (AEPD), C/

Jorge Juan 6, 28001 Madrid, www.aepd.es.

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. (Under Article 7 of the LOPDGDD the age of consent to data processing in Spain is fourteen (14); the Service sets a higher age.) 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, and the agent's memory (row 3.14) is written automatically by an AI system. Their output is not reviewed by a person before it is delivered or stored. The memory can contain errors; the Customer can read and delete it.

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.
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.
1.2	13 October 2026	Describes the agent functions added to the Service: the choice of Persona and of the agent's memory at sign-up (row 3.2), the agent settings of a Device (new row 3.13), the hosted agent's memory (new row 3.14, clauses 5.2, 6.6 and 11.1) and a Customer's own agent (new clause 5.5). Row 3.8 and clause 6.4: the text of Customers' Calls is no longer written to a log. Clause 8.1: items (j) and (k) added.
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. Clauses 1.1 to 1.5, 4, 5.2 (the Developer as a recipient), 7.2, 7.3, 9 and 10.1 changed. Clause 6.2: data of an early-access trial that ends without a paid plan is kept for 7 days, then deleted.
2.1	15 October 2026	Clause 6.2 and row 3.5: the same seven-day keep period, then deletion, also applies when a paid plan ends because it was cancelled or its renewal was not paid; the stop email states the deletion date.