

Data Processing Addendum

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 Addendum applies where a business Customer uses ERIUS PHONE to process personal data. It forms part of the Terms of Service between the Customer and Protremix Technology Limited.

1. Scope and roles

- 1.1 This Addendum forms part of the Terms of Service (the **Terms**) and applies to the processing of Customer Personal Data by Protremix Technology Limited (**Protremix**) on behalf of the Customer. Words defined in the Terms have the same meaning here.
- 1.2 **Customer Personal Data** means personal data contained in Customer Data, including personal data of Guests and of persons whose data is held on a Device or in an uploaded file.
- 1.3 For Customer Personal Data the Customer is the controller (or acts for a controller) and Protremix is the processor. For the data described in clause 2.1 of the Privacy Policy Protremix is a controller and this Addendum does not apply.
- 1.4 The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subject are set out in Annex 1.

2. Customer's instructions

- 2.1 Protremix will process Customer Personal Data only on the Customer's documented instructions. The Terms, this Addendum, the Customer's configuration of the Service and each request made through the API or the Dashboard are the Customer's instructions.
- 2.2 Protremix will inform the Customer if it considers that an instruction infringes the law that applies to Protremix. It is not obliged to verify the lawfulness of the Customer's instructions under laws that apply only to the Customer.
- 2.3 Protremix may process Customer Personal Data where the law of the United Arab Emirates requires it and will, where the law permits, tell the Customer before doing so.

3. Customer's obligations

- 3.1 The Customer is responsible for the lawfulness of the Customer Personal Data and of its instructions, including: having a lawful basis for each Call and for the processing of each Guest's voice, image and words; giving the notices and obtaining the consents that the law requires; and not placing on a Device data that it is not entitled to process.
- 3.2 The Customer acknowledges that the Service is not designed for special categories of data such as health data, biometric identifiers used for identification, or data about children, and will not use the Service to process such data unless it has assessed the risks and has a lawful basis.

4. Confidentiality

- 4.1 Protremix will ensure that every person it authorises to access Customer Personal Data is bound by a duty of confidentiality and accesses the data only as needed to operate, maintain, secure or support the Service or to act on the Customer's request.

5. Security

- 5.1 Protremix will maintain the technical and organisational measures described in Annex 2. It may change them provided the overall level of protection is not reduced.
- 5.2 The Customer is responsible for the security of its API Keys, for the applications and accounts it places on a Device, and for deciding whether the measures in Annex 2 are appropriate for the data it processes.

6. Sub-processors

- 6.1 The Customer gives general authorisation to the use of sub-processors in the categories listed in Annex 3.
- 6.2 Protremix will impose on each sub-processor data-protection obligations that are in substance no less protective than those in this Addendum, to the extent applicable to the service it provides, and remains responsible to the Customer for the sub-processor's performance.
- 6.3 Protremix will give notice of the addition of a new category of sub-processor, or of a change that materially affects the processing, at least fourteen (14) days before it takes effect, by updating Annex 3 and notifying the Customer under clause 23 of the Terms. The Customer may object on reasonable data-protection grounds within that period. If the parties cannot resolve the objection, the Customer may close the Account and receive a refund of the unused part of any period it has paid for.

7. International transfers

- 7.1 The Customer acknowledges that Customer Personal Data is stored in the European Union, is accessed by Protremix from the United Arab Emirates and other countries, and may be processed by sub-processors in other countries, including the United States of America.
- 7.2 Where the law that applies to the Customer requires a specific transfer mechanism, the Customer will tell Protremix, and the parties will cooperate in good faith to put in place a mechanism that Protremix is able to perform.

8. Assistance

- 8.1 Taking into account the nature of the processing and the information available to it, Protremix will give the Customer reasonable assistance in: responding to requests from data subjects to exercise their rights; and meeting the Customer's obligations on security, breach notification and, where required, impact assessments and consultation with an authority.
- 8.2 If Protremix receives a request from a data subject about Customer Personal Data, it will pass the request to the Customer without undue delay and will not answer it except to say that it has been passed on.
- 8.3 Assistance that goes beyond the functions of the Service and requires material effort may be charged at a rate agreed in advance.

9. Personal data breach

- 9.1 Protremix will notify the Customer without undue delay, and where feasible within seventy-two (72) hours, after it has confirmed a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data.
- 9.2 The notice will be sent to the Account's contact email and will describe, to the extent known: the nature of the breach, the data and Accounts affected, the likely consequences, and the measures taken or proposed. Information that is not yet available will follow as it becomes known.
- 9.3 A notice under this clause is not an admission of fault or liability.

10. Deletion and return

- 10.1 During the term the Customer can retrieve the contents of a Device through the functions of the Service.
- 10.2 On closure of the Account, Protremix will delete the Account's Devices and their storage. Customer Personal Data in encrypted backups is overwritten as the backups expire, within the period stated in clause 6.5 of the Privacy Policy. Call records are retained as stated in row 3.7 of the Privacy Policy.
- 10.3 Text logs of Calls (row 3.8 of the Privacy Policy) are deleted on the Customer's request. The Customer may make that request at any time and should make it on closing the Account.
- 10.4 Protremix may retain Customer Personal Data to the extent and for the period required by the law of the United Arab Emirates, and will keep it confidential for that period.

11. Information and audit

- 11.1 On written request, and not more than once in any twelve (12) months unless a breach has occurred or an authority requires it, Protremix will give the Customer the information reasonably necessary to demonstrate compliance with this Addendum, in the form of written answers and available documentation.
- 11.2 Protremix holds no third-party audit report or certification at the Effective Date. Where the information under clause 11.1 is not sufficient and the law that applies to the Customer requires an audit, the parties will agree in advance the scope, timing, confidentiality terms and cost of an audit. An audit must not give access to another customer's data or put the security of the Service at risk, and is conducted remotely unless agreed otherwise.

12. Liability and term

- 12.1 The limits and exclusions of liability in the Terms apply to this Addendum.
- 12.2 This Addendum applies for as long as Protremix processes Customer Personal Data and ends when that data has been deleted in accordance with clause 10.
- 12.3 This Addendum is governed by the law and subject to the courts stated in clause 24 of the Terms.

A. Annex 1: Details of the processing

Item	Description
Subject matter	Provision of hosted Devices, the API and the Calls function to the Customer
Duration	The term of the Account, plus the deletion periods in clause 10

Item	Description
Nature and purpose	Hosting and running the Device; executing API requests; transmitting Call audio and video to operate a Persona; logging; backup; support
Types of personal data	Whatever the Customer places on a Device (for example account identifiers, messages, contacts, files); a Guest's voice and image during a Call; the text of what a Guest said and what the Persona replied; where enabled, images of the call screen; technical identifiers such as IP addresses
Categories of data subject	The Customer's staff and users; Guests; persons whose data is contained in applications or files on a Device
Special categories	None intended (clause 3.2)

B. Annex 2: Security measures

Area	Measure
Isolation	Each Device runs in its own container on its own private network. An API Key reaches only the Devices of its own Account; a request for another Account's Device receives the same refusal as for one that does not exist
Credentials	API Keys are stored as one-way hashes. A key is displayed once, through a single-use link
Transport	The website, Dashboard and API are served over encrypted connections only
Exposure	The debugging interface of a Device is bound to the server's loopback address. Internal services listen on loopback addresses
Uploads	Uploaded files are held in a restricted area from which nothing can be executed, with a size limit per upload
Logging	API requests are recorded in an audit log that contains no request bodies and no keys
Backups	Daily encrypted backups to stores from which the production server cannot delete; fourteen daily and eight weekly copies; restore tests on a schedule
Monitoring	Scheduled automated checks of the isolation between Accounts, of exposed network ports and of the integrity of production files
Access	Administrative access by key-based authentication, limited to the people who operate the Service
Not provided	End-to-end encryption of Device contents against Protremix; third-party certification; a contractual availability commitment

C. Annex 3: Categories of sub-processor

Category	Processing	Location
Hosting and data-centre provider	Servers on which the Service and its backups run	European Union
Third-party AI voice and avatar services	Real-time processing of Call audio and, where enabled, call screen images to operate a Persona	May include the United States of America
Third-party AI language-model service	Processing of support assistant messages	May include the United States of America
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. No Call content	Several countries, including the United States of America
Email service provider	Delivery of service emails	May include countries outside the European Union

Category	Processing	Location
Payment processor (when paid plans open)	Payment and billing data only; not Customer Personal Data on Devices or in Calls	May include the United States of America

Version history

Version	Effective date	Change
1.0	13 October 2026	First published version. archived PDF
1.1	13 October 2026	Annex 3: the connection servers used to set up a Call added. They were already in use when version 1.0 was published; this corrects the list and is not a new category under clause 6.3.