

**Data Processing Agreement in accordance with Article 28 GDPR
for using the Unified Communications Service Rainbow**



Agreement

between the

Client

- responsible party - hereinafter referred to as the client -

and the

ALE International

32 avenue Kléber

92707 Colombes cedex / FRANCE

- processor - hereinafter referred to as the contractor

1. The subject matter and duration

(1) Subject

Type and purpose of the processing of personal data by the contractor for the client:

a) Provide an online digital collaboration platform ("Rainbow") under the domain <https://www.openrainbow.com>.

The cloud platform "Rainbow" offers the following functionalities (features):

- the creation of user accounts
- Deleting user accounts
- the creation and management of appointments in the calendar function
- the creation of virtual conference rooms ("Bubbles")
- Displaying user presence status
- Sending invitations from "Rainbow"
- virtual collaboration via chat
- virtual collaboration via audio and video conferencing
- Saving and sharing files

The functionalities can be extended at any time by the contractor. The client is free to use the extensions offered.

b) Technical support

In this respect, the contractor offers technical support. This is done remotely via an encrypted connection.

The provision of contractually agreed data processing takes place on servers in Germany. Maintenance and service work may be carried out from other locations of the contractor in Member States of the European Union or in another Contracting State of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the contracting authority and may only take place if the special conditions of Article 44 e.G. GDPR are met.

(2) Duration

The duration of this contract processing contract shall be valid for an unlimited period or as long as there is a business relationship between the two parties.

2. Categories of data and data subjects

(1) Type of data

The processing of personal data is concerned with the following types/categories:

- Name
- First
- Title
- Username
- Telefon numbers
- E-mail addresses
- Company affiliation
- If necessary, function or department
- Images (profile pictures)
- Audio data in audio conferencing and video conferencing
- Video data in the context of videoconferencing
- Logfiles (registrations and unsubscribes)
- Data uploaded in the context of virtual collaboration by the client

(2) Categories of data subjects

The categories of data subjects affected by the processing include:

- Employees of the client
- If applicable partners, customers or prospect of the client
- If applicable, service providers or suppliers of the client
- If applicable any other unspecified third parties that the client invites to communicate in Rainbow

3. Technical and Organisational Measures

(1) The contractor must document the implementation of the technical and organizational measures set out in the run-up to the award of the contract and hand them over to the client for review before the start of processing, in particular with regard to the specific execution of the contract. If accepted by the client, the documented measures become the basis of the order. If the client's test / audit reveals a need for adjustment, this is to be implemented by mutual agreement.

(2) The contractor must provide security in accordance with Article 28 Paragraph 3 Letter c, 32 GDPR, in particular in conjunction with Article 5 Paragraph 1, Paragraph 2 GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR must be taken into account.

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative, adequate measures. The security level of the specified measures must not be undercut. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data processed in the order without authorization, but only in accordance with documented instructions from the client. Insofar as a person concerned contacts the contractor directly in this regard, the contractor will immediately forward this request to the client.

(2) As far as included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and information must be ensured directly by the contractor in accordance with documented instructions from the client.

5. Quality assurance and other obligations of the contractor

In addition to complying with the provisions of this order, the contractor has legal obligations according to Art. 28 to 33 GDPR; in this respect, he particularly guarantees compliance with the following requirements:

- a) Written appointment of a data protection officer who carries out his work in accordance with Art. 38 and 39 GDPR.

Name and contact details of the ALE International Data Protection Officer:

Louis-Philippe Ollier
dataprivacy@al-enterprise.com

The current contact details of the data protection officer can be found in the data protection declaration of the ALE international website.

- b) Maintaining confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Letter b, 29, 32 Paragraph 4 GDPR. In carrying out the work, the contractor will only use employees who are bound to confidentiality and who have previously been familiarized with the data protection provisions that are relevant to them. The contractor and every person subordinate to the contractor who has access to personal data may only process this data in accordance with the instructions of the client, including the powers granted in this contract, unless they are legally obliged to process them.
- c) The implementation of and compliance with all technical and organizational measures required for this order in accordance with Article 28 Paragraph 3 Sentence 2 Letter c, 32 GDPR.
- d) The client and the contractor work together on request with the supervisory authority in the performance of their tasks.
- e) The immediate information of the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies if a competent authority investigates the processing of personal data during order processing at the contractor's within the framework of an administrative offense or criminal proceedings.

- f) Insofar as the client is exposed to a control by the supervisory authority, an administrative offense or criminal proceedings, the liability claim of a person concerned or a third party or any other claim in connection with the order processing at the contractor, the contractor must support him to the best of its ability.
- g) The contractor regularly checks the internal processes as well as the technical and organizational measures to ensure that the processing in his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.
- h) Verifiability of the technical and organizational measures taken vis-à-vis the client within the scope of his control powers according to section 7 of this contract.
- i) The contractor keeps a register of data processing activities in accordance with Art. 30 Para. 2 GDPR.
- j) Should the property or the confidentiality of the client's data at the contractor be endangered by measures by third parties (such as seizure), insolvency or settlement proceedings or other events, the contractor must inform the client immediately.
- k) The contractor will inform the client immediately in the event of serious disruptions to operations, suspected violations of the protection of personal data, other irregularities in data processing, control activities and measures by a supervisory or investigative authority. The contractor will notify the client immediately if the security measures taken by him do not (no longer) meet the client's requirements.

6. Subcontracting conditions

(1) For the purposes of this regulation, subcontracting relationships are to be understood as those services which relate directly to the provision of the main service.

This does not include ancillary services that the contractor uses, e.g. as telecommunications services, post / transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems in whose context there is no direct access to the client's data.

However, the contractor is obliged to ensure data protection and data security for the client's data, including in the case of outsourced ancillary services, to take appropriate and legally compliant contractual agreements and control measures.

(2) The contractor may only commission subcontractors (further processors) after informing the client in advance. The client has the right to reject the subcontractor.

Outsourcing to subcontractors or changing the existing subcontractor is permitted, provided that:

- the contractor notifies the client of such outsourcing to subcontractors a reasonable time in advance in writing or in text form and
- the client does not raise an objection to the planned outsourcing in writing or in text form by the time the data is transferred to the contractor and
- a contractual agreement in accordance with Art. 28 Paragraph 2-4 GDPR is used.

(3) The transfer of personal data from the client to the subcontractor and its initial activity are only permitted if all the requirements for subcontracting are met.

(4) If the subcontractor provides the agreed service outside of the EU / EEA, the contractor shall ensure admissibility under data protection law by taking appropriate measures. The same applies if service providers are to be used.

7. Control rights of the client

(1) The client is entitled to check compliance with the data protection regulations and the contractual agreements within the scope of the contractual relationship to the extent required or to have them checked by a person commissioned by him, in particular by obtaining information and inspecting the stored data and the data processing programs in the context of inspections.

(2) The contractor ensures that the client can convince himself of the compliance with the obligations of the contractor according to Art. 28 GDPR. The contractor undertakes to provide the client with the necessary information on request and, in particular, to demonstrate the implementation of the technical and organizational measures.

(3) Evidence of such measures, which do not only relate to the specific order, can be provided by

- Compliance with approved rules of conduct in accordance with Art. 40 GDPR;
- Certification according to an approved certification procedure in accordance with Art. 42 GDPR;
- Current certificates, reports or report excerpts from independent bodies (e.g. auditors, auditors, data protection officers, IT security departments, data protection auditors, quality auditors);
- Appropriate certification through an IT security or data protection audit (e.g. according ISO27001 certification).

8. Notification of breaches by the Contractor

(1) The contractor supports the client in complying with the obligations for the security of personal data set out in Articles 32 to 36 of the GDPR, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include

- a) ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the forecast probability and severity of a possible violation of the law through security gaps and enable an immediate detection of relevant violation events.
- b) the obligation to report any personal data breaches to the client immediately.
- c) the obligation to support the client within the scope of his obligation to provide information to the data subject and to provide him with all relevant information immediately in this context.
- d) the support of the client for its data protection impact assessment.
- e) the support of the client in the context of prior consultations with the supervisory authority.

(2) The contractor can claim remuneration for support services that are not included in the service description or that cannot be traced back to misconduct by the contractor.

9. Authority of the Client to issue instructions

(1) The client has the right to issue instructions to the contractor regarding the processing of personal data. These are to be documented.

(2) Verbal instructions are immediately confirmed by the client (at least in text form).

(3) The contractor must inform the client immediately if he is of the opinion that an instruction violates data protection regulations. The contractor is entitled to suspend the implementation of the relevant instruction until it is confirmed or changed by the client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the client. This does not include backup copies of BACK UPs, insofar as they are necessary to ensure proper data processing, as well as data that are necessary in order to comply with statutory retention requirements.

(2) After completion of the contractually agreed work or earlier upon request by the client - at the latest with the termination of the service agreement - the contractor shall have all documents, created processing and usage results as well as databases in connection with the contractual relationship to be handed over to the client or destroyed in accordance with data protection regulations with prior consent. The same applies to test and scrap material. The log of the deletion must be presented on request.

(3) Documentation that serves as evidence of orderly and proper data processing must be kept by the contractor beyond the end of the contract in accordance with the respective retention periods. He can hand them over to the client for his relief at the end of the contract.

11. Liability

The contractor is liable for damage caused by the breach of his obligations. This applies in particular to damage caused by data processing that does not comply with the General Data Protection Regulation or resulting from failure to comply with the client's instructions. The contractor is released from liability if he can prove that he is in no way responsible for any damage incurred.

12. Other

(1) Changes, additions and subsidiary agreements to this contract must be made in writing.

(2) Should one or more provisions in this agreement be or become ineffective or unenforceable, this shall not affect the validity of the remaining contractual provisions. The contractual partners will replace the ineffective or unenforceable provision with a provision that comes closest to its meaning and purpose. The same applies in the event of an unwanted loophole.

Appendix 1 - Sub Processors

NAME	ADRESS	PURPOSE	DATA SHARED WITH SUBPROCESSOR	DATA PROCESSING LOCATION
OVH	2 rue Kellermann, 59100 Roubaix, France	Hosting	Hosting means here data center services: hardware, connectivity: no access to data	France
IBM France	17 avenue de l'Europe 92275 Bois Colombes Cedex France	failover for hosting	Hosting means here data center services: hardware, connectivity: no access to data	France
X-act	Luis Morote 6, 6e Planta, 35007 Las Palmas de Gran Canaria, Spain	L1 and L2 support	description of support ticket as provided by the submitter, and attached logs (logs are anonymized and never contain any content stored or shared by the end-user in the context of her use of Rainbow)	Spain
Slash support / CSS, now "MOVATE" corp.	1900 Mc Carthy Blv. Suite 210, Milpitas California, USA	L1 and L2 support	description of support ticket as provided by the submitter, and attached logs (logs are anonymized and never contain any content stored or shared by the end-user in the context of her use of Rainbow)	USA, India
SalesForce.com EMEA limited	Floor 26 Salesforce Tower, 110 Bishopsgate London EC2N 4AY, United Kingdom	SaaS-mode support ticketing tool	Storage of support tickets (description as provided by end-customer and anonymized logs), and storage of business partners information	UK
LoopUp Ltd.	The Tea Building, 56 Shoreditch High Street, London, E1 6JJ, United Kingdom	Voice conferencing	CDR for billing of traffic related to PSTN conferences. CDR contain the caller number as provided by the PSTN network, and the called conference service DDI. No further personal data is contained in those CDRs.	UK
Amigo Software	33 Hatley Avenue, Barkingside, Ilford, Essex IG6 1EG United Kingdom	L3 support for specific client applications	description of support ticket as provided by the submitter, and attached logs (logs are anonymized and never contain any content stored or shared by the end-user in the context of her use of Rainbow)	UK, Canada, Pakistan
ASAL technologies	3rd floor, Q Center- companies building Rawabi, Palestine	L3 support for specific client applications	description of support ticket as provided by the submitter, and attached logs (logs are anonymized and never contain any content stored or shared by the end-user in the context of her use of Rainbow)	Palestine territories
Zuora	1051 E. Hillsdale Blvd, Suite 600, Foster City, CA 94404, USA	SaaS-mode billing tool	CDR for billing the Rainbow service towards Rainbow partners. CDR contain volume of subscriptions without any end-user personal data. Zuora manipulates partners billing information.	USA

Appendix 2 - Technical and Organisational Measures

Latest documentation available in the Rainbow Help Center:

<https://support.openrainbow.com/hc/en-us/articles/360017424419-Technical-Organisational-Measures>