

Data processing agreement (DPA)

As required by the EU and UK GDPR, this Data Processing Agreement (DPA) is a mutual agreement between ComplyVox, as the data processor, and you, the client, as the data controller. We, in turn, have signed DPAs with our suppliers (sub-processors), listed below. This agreement forms part of our overall business agreement and does not replace our contract or terms of business.

Processor details

Data processor	ComplyVox Ltd, registered in Ireland, company number 823614
Registered address	The Hatch Lab, Gorey, Co. Wexford, Ireland, Y25 A8H2
Data Protection Officer	dpo@complyvox.eu
Purpose of processing	ComplyVox provides an AI-based compliance tool to gather, research and collate business-related information and a systems inventory, to produce a GDPR compliance framework.
Personal data processed	Personal data of the client’s personnel and business contacts, being: (a) business contact details (name, work email, role, department) used to set up accounts, administer the contract and provide customer care; (b) audio of voice conversations, and the resulting transcripts, of the client's staff who use the voice interface (audio is processed transiently; transcripts are stored in Supabase); and (c) any other personal data the client chooses to include in its compliance records, such as names of staff or supplier contacts.
Data subjects	The client's employees, contractors and other business contacts.
Duration	The term of the contract, plus the retention periods set out below.
Special category data	We will never ask for special category data.
Retention period	Your compliance file is deleted automatically 2 months after your contract ends, to allow for transfer of your documentation. Call transcripts are kept for no longer than 6 months.
Sub-processors	See below.

EU representative

Not required.

Sub-processors

Sub-processor	Purpose	Location	Data involved
Supabase	Primary data storage: the only place client data is stored long-term	Ireland, EU	All client account, compliance and transcript data
Hostman	Orchestration layer connecting the AI processing steps, and website hosting	Frankfurt, Germany, EU	Data in transit between AI processing steps only; never stored
Mistral	Voice AI processing (speech-to-text, response generation, text-to-speech)	EEA	Conversation audio and text, processed transiently under a contractual zero-retention commitment
ElevenLabs	Voice AI processing (speech-to-text, response generation, text-to-speech)	UK and EU	Conversation audio and text, processed transiently under a contractual zero-retention commitment
Google Cloud (Firebase)	Delivers application code only	EU (Belgium)	No client data stored. Technical connection data (such as IP address) may be processed when the app is delivered.

Terms

- **Written instruction.** ComplyVox will process personal data only on the client's documented instructions, which are set out in this DPA, the Terms and the client's use and configuration of the Platform. This includes instructions on transfers of personal data outside the EEA, unless ComplyVox is required to act otherwise by law, in which case it will tell the client before processing unless the law prohibits this. ComplyVox will tell the client immediately if, in its opinion, an instruction infringes data protection law.
- **Compliance.** ComplyVox complies with the GDPR, the ePrivacy rules and the AI Act, and ensures that anyone involved in processing personal data is subject to a duty of confidentiality and has experience in data protection matters.
- **Privacy rights.** The client has full control of the data and can exercise privacy rights for anyone whose data is in its care. Any request outside self-service, such as access or deletion, will be supported and actioned without delay and within 30 days.

- **Data breaches and investigations.** ComplyVox will notify the client with immediate effect of any personal data breach or incident that may infringe data protection law, and will support the client to investigate and mitigate it. The client is responsible for investigating, for assessing the privacy risk, for deciding whether to notify its supervisory authority within 72 hours, and for deciding whether to notify the individuals affected. ComplyVox will co-operate with the relevant supervisory authority in any investigation.
- **Suppliers and transfers.** ComplyVox will give the client at least 30 days' prior written notice of any intended addition or replacement of a sub-processor, by email and by updating the sub-processor list. The client may object on reasonable data protection grounds within that period. The parties will work together in good faith to resolve the objection and, if it cannot be resolved, the client may terminate the affected Services on written notice. We understand that all sub-processors are subject to the same data protection obligations as the processor. If a sub-processor fails to comply with data protection law or the relevant data processing agreement, the processor remains directly liable to the client. Client personal data is stored in the EU (Ireland). Voice AI processing is carried out in the EEA and, by ElevenLabs, in the UK, which is covered by an EU adequacy decision. Any other transfer outside the EEA will only take place with a valid Chapter V GDPR transfer mechanism and with prior notice to the client.
- **Audit.** ComplyVox will make available to the client all information necessary to demonstrate compliance with this DPA and Article 28 GDPR, and will allow for and contribute to audits, including inspections, carried out by the client or an auditor the client appoints. Audits will be on reasonable written notice, during normal business hours, and generally no more than once a year, unless required by a supervisory authority or following a personal data breach. ComplyVox will first refer the client to the Trust Centre documentation.
- **Return or deletion at the end of the Services.** When the Services end, the client may choose whether ComplyVox returns all client personal data to the client or deletes it, and ComplyVox will then delete all existing copies unless the law requires it to keep them. The client should tell ComplyVox its choice within the 2-month period after the contract ends; if it does not, the data will be deleted automatically at the end of that period.
- **Retention and deletion.** Your compliance file is deleted automatically 2 months after your contract ends, to allow for transfer of your documentation. Call transcripts are kept for no longer than 6 months.
- **Obligations and security.** Where practical, ComplyVox will assist the client in meeting its accountability obligations, including access to our Trust Centre to review our documentation, to demonstrate transparency and compliance with the regulation. ComplyVox will always use best endeavours to safeguard all personal data from unauthorised or unlawful processing, including (but not limited to) accidental loss, destruction or damage, and will ensure the security of processing by implementing appropriate technical and organisational measures.
- **Onboarding.** The client is responsible for engaging with the onboarding process set out by ComplyVox.
- **Due diligence.** The client retains responsibility for carrying out its own due diligence on processors and sub-processors, before and during the contract. ComplyVox provides full transparency for that due diligence in our Trust Centre.

Signatures

Signed on behalf of ComplyVox

Company name ComplyVox Ltd

Print name

Signature

Position

Contact

Date

Signed on behalf of the client

Company name

Print name

Signature

Position

Contact

Date