Data Processing Agreement

Version 1.0 – 13 November 2026

(pursuant to Article 28(3) and (4) of the GDPR)

Based on the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/915, with the adaptations and additional provisions set out in this Agreement

Between:

VISOR.AI PORTUGAL, S.A., a company with registered number 513 889 213 and registered office at Rua João Saraiva, 38, 4th floor, 1700-106 Lisbon, Portugal, represented herein by a person with powers to do so, hereinafter referred to as the **"Processor"** or **"Visor.ai"**;

and

[CUSTOMER'S CORPORATE NAME], a company with registered number [___], with registered office at [full address], represented herein by [name and position of the legal representative] (or the entity identified in the Order Form, where this Agreement is accepted through it), hereinafter referred to as the **"Controller"** or **"Customer"**;

Jointly referred to as the "Parties" and individually as a "Party".

The Parties hereby enter into and mutually accept this Data Processing Agreement (hereinafter, the "Agreement"), which is governed by the following clauses:

PRELIMINARY CLAUSE – DEFINITIONS

For the purposes of this Agreement, and unless the context requires otherwise, the following capitalised terms have the meanings set out below. Terms not defined in this Agreement that correspond to terms defined in the GDPR have the meaning given to them in the GDPR, in accordance with Clause 3 of these Clauses.

a) **"Agreement" or "DPA":** this Data Processing Agreement, including all of its Appendices, which form an integral part of it;
b) **"Appendices":** Appendices I to V to this Agreement, as applicable;
c) **"Clauses":** the clauses contained in this Agreement, based on the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/915;
d) **"Customer":** the entity identified in Appendix I as the Controller, being Visor.ai's counterparty under the Main Agreement;
e) **"Main Agreement":** the Services Agreement entered into between the Parties, including any amendments, addenda and Order Forms, under which the Services are provided or, in the absence of a signed Services Agreement, the Order Form signed by the Customer and the Visor.ai Terms of Service to which it refers;
f) **"EEA":** the European Economic Area, comprising the Member States of the European Union, Iceland, Liechtenstein and Norway;
g) **"Data Protection Officer" or "DPO":** the person designated to perform the tasks set out in Articles 37 to 39 of the GDPR;

h) **"Technical and Organisational Measures" or "TOMs":** the set of technical and organisational security measures implemented by Visor.ai to protect Personal Data, as described in Appendix IV to this Agreement;
i) **"Order Form":** the contractual document, drawn up on the basis of the Visor.ai template and signed by the Customer, that sets out the specific Services ordered, including, in particular, the scope, the modules ordered, the commercial terms and the service parameters. The Order Form may be annexed to a Services Agreement or, in the absence of one, constitute the Main Agreement together with the Visor.ai Terms of Service;
j) **"Parties":** Visor.ai and the Customer, jointly; and "Party", either of them individually;
k) **"GDPR":** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
l) **"Services":** the services provided by Visor.ai to the Customer under the Main Agreement, as described in the Main Agreement and its Annex I (Proposal) or in the Order Form;
m) **"Sub-processor":** any third party engaged by Visor.ai to carry out processing activities on Personal Data on behalf of the Customer, as listed in Appendix V to this Agreement;
n) **"Terms of Service":** the Visor.ai Terms of Service, available at https://visor.ai/legal, in the version identified in the Order Form or, failing that, in the version in force when the Order Form is signed;
o) **"Trust Center":** Visor.ai's online platform, available at https://visor.ai/trust, where information on compliance, security and the processing of personal data is kept up to date, including the list of Sub-processors;
p) **"Visor.ai":** Visor.ai Portugal, S.A., acting as Processor for the purposes of this Agreement, as identified in Appendix I.

SECTION I – GENERAL PROVISIONS

Clause 1 – Purpose and scope

a) The purpose of these clauses (hereinafter, the "Clauses") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, the "GDPR").
b) The Controller and the Processor listed in Appendix I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of the GDPR.
c) These Clauses apply to the processing of Personal Data as specified in Appendix II.
d) Appendices I to V are an integral part of this Agreement.
e) These Clauses are without prejudice to obligations to which the Controller is subject by virtue of the GDPR.
f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR.

Clause 2 – Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Appendices or updating information in them.
b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of Data Subjects.

Clause 3 – Interpretation

a) Where these Clauses use the terms defined in the GDPR, those terms shall have the same meaning as in the GDPR.
b) These Clauses shall be read and interpreted in the light of the provisions of the GDPR.
c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

Clause 4 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Appendices and signing Appendix I.
b) Once the Appendices in point (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Appendix I.
c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of Personal Data and the purposes of processing for which the Personal Data is processed on behalf of the Controller, are specified in Appendix II.

Clause 7 – Obligations of the Parties

7.1. Instructions

a) The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of Personal Data. These instructions shall always be documented.
b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the GDPR or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The Processor shall process the Personal Data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Appendix III.

7.4. Erasure or return of personal data

a) After the end of the processing period specified in Appendix III, the Processor shall, at the choice of the Controller: (i) delete all Personal Data processed on behalf of the Controller and certify to the Controller that it has done so; or (ii) return all the Personal Data to the Controller and delete existing copies, unless Union or Member State law requires storage of the Personal Data. The Processor shall continue to ensure compliance with these Clauses until the data is deleted or returned.
b) The Controller has the right to verify that the Processor has properly completed the return or deletion of the Personal Data, including, where necessary, by means of an audit of the Processor. The Controller may carry out such verification through an independent expert appointed by it, provided that the expert is not in a competitive relationship with the Processor.
c) The Processor shall keep confidential any Personal Data to which it has had access or of which it has become aware in connection with the processing covered by the Clauses, even after the end of the processing period specified in Appendix III. This Agreement remains in force beyond the end of the Main Agreement for as long as the Processor holds data processed on behalf of the Controller.

7.5. Security of processing

a) The Processor shall at least implement the technical and organisational measures specified in Appendix IV to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.
b) The Processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorised to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.6. Sensitive data

If the processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards, as set out in Appendix III.

7.7. Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.
b) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from the GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor, in particular its ISO/IEC 27001:2022 certification.
   i) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor, to be carried out during normal business hours.
   ii) Audits shall be notified to the Processor in writing at least 30 (thirty) calendar days in advance, and the Processor shall provide the Controller, within an appropriate period of no less than 5 (five) calendar days, with all the information necessary for the proper conduct of the audit.
d) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.8. Use of sub-processors

a) The Processor has the Controller's general authorisation for the engagement of the Sub-processors listed in Appendix V. The Processor shall specifically inform the Controller in writing of any intended changes to that list at least 30 (thirty) days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.
b) Where the Processor engages a Sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with these Clauses. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to the GDPR.
c) At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Processor may redact the text of the agreement prior to sharing the copy.
d) The Processor shall remain fully responsible to the Controller for the performance of the Sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-processor to fulfil its contractual obligations.

7.9. International transfers

a) Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of the GDPR.
b) The Controller agrees that where the Processor engages a Sub-processor in accordance with Clause 7.8 for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of Personal Data within the meaning of Chapter V of the GDPR, the Processor and the Sub-processor shall ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the Controller

a) The Processor shall promptly notify the Controller of any request it has received from the Data Subject. It shall not respond to the request itself, unless authorised to do so by the Controller.
b) The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with points (a) and (b), the Processor shall comply with the Controller's instructions.
c) In addition to the Processor's obligation to assist the Controller pursuant to point (b), the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:
    i) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a 'data protection impact assessment' – DPIA) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    ii) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;
    iii) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is processing is inaccurate or has become outdated;
    iv) the obligations in Article 32 of the GDPR.
d) The Parties shall set out in Appendix IV the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.
e) **Additional provision:** without prejudice to the preceding points, the Processor shall inform the Controller without undue delay in the event of disruptions, suspected data breaches, breaches of contractual obligations by the Processor, suspected security incidents or any other irregularities relating to the processing of Personal Data.

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 of the GDPR, where applicable, taking into account the nature of processing and the information available to the Processor.

9.1. Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
b) in obtaining the following information which, pursuant to Article 33(3) of the GDPR, shall be stated in the Controller's notification, and must at least include:

- the nature of the Personal Data including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

c) in complying, pursuant to Article 34 of the GDPR, with the obligation to communicate without undue delay the personal data breach to the Data Subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay and in any event within 48 (forty-eight) hours after having become aware of the breach. The notification shall be sent from **securityoffice@visor.ai** to the email address designated by the Controller, with the subject line "*VISOR.AI - SECURITY NOTIFICATION*", and shall contain at least:

- a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
- the details of a contact point where more information concerning the personal data breach can be obtained;
- its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Appendix IV all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of the GDPR.

SECTION III – FINAL PROVISIONS

Clause 10 – Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of the GDPR, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of Personal Data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.
b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of Personal Data in accordance with these Clauses if:
   i) the processing of Personal Data by the Processor has been suspended by the Controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
   ii) the Processor is in substantial or persistent breach of these Clauses or its obligations under the GDPR;
   iii) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the GDPR.
c) The Processor shall be entitled to terminate the contract insofar as it concerns processing of Personal Data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1(b), the Controller insists on compliance with the instructions.

d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all Personal Data processed on behalf of the Controller and certify to the Controller that it has done so, or return all the Personal Data to the Controller and delete existing copies unless Union or Member State law requires storage of the Personal Data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

Clause 11 – Language versions

This Agreement is executed in Portuguese and English. In the event of any discrepancy between the versions, the Portuguese version shall prevail.

SIGNATURES

The Parties declare that they have read, understood and accepted this Data Processing Agreement and undertake to comply with it in full.

Where the Main Agreement consists of the Order Form and the Visor.ai Terms of Service, this Agreement shall be deemed entered into and accepted by the Parties upon signature of the Order Form that refers to it, identifying the version and date of this Agreement, without the need to sign the table below. In that case, the Controller's details in Appendix I are those set out in the Order Form.

For VISOR.AI PORTUGAL, S.A.	**For the Controller**
Name: _____	Name: _____
Position: _____	Position: _____
Date: _____	Date: _____
Signature:	Signature:

APPENDIX I – LIST OF PARTIES

Controller

Corporate name	[to be completed or as per Order Form]
Tax / company number	[to be completed or as per Order Form]
Registered office	[to be completed or as per Order Form]
Legal representative	[Name and position, or as per Order Form]
Data protection contact / DPO	[Name, email, telephone, or as per Order Form]
Address for personal data breach notifications	[to be completed or as per Order Form]

Processor

Corporate name	Visor.ai Portugal, S.A.
NIPC	513 889 213
Registered office	Rua João Saraiva, 38, 4th floor, 1700-106 Lisbon, Portugal
Data protection contact	privacy@visor.ai
Personal data breach notifications	securityoffice@visor.ai
Trust Center	https://visor.ai/trust
Certifications	ISO/IEC 27001:2022

APPENDIX II – DESCRIPTION OF THE PROCESSING

The details of the processing operations, in particular the categories of Personal Data and the purposes for which they are processed on behalf of the Controller, are described in the table below. The table contains the standard description of the Services, which applies unless the Controller indicates otherwise in the Proposal or the Order Form. The Controller, with the Processor's support where necessary, is responsible for completing or adjusting this description to the actual configuration of the contracted Services.

Categories of data subjects whose personal data is processed	End users who interact with the Customer's AI Agents through the contracted channels (phone calls, chat and messaging), in particular the Controller's customers and prospective customers; platform users authorised by the Customer (the Customer's employees and service providers).
Categories of personal data processed	Identification and contact data provided during the interaction (for example, name, phone number, email, customer number); voice and audio recordings; transcripts and conversation content; interaction metadata (date, time, duration, channel and technical identifiers); account data and activity logs of platform users.
Special categories of data (Art. 9 GDPR)	None, unless expressly indicated by the Controller in the Proposal or the Order Form, in which case the safeguards of Clause 7.6 and Appendix III apply.
Nature of the processing	Collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission to the Controller where applicable, and erasure of Personal Data, within the scope of the contracted Services.
Purpose(s) for which the personal data is processed on behalf of the Controller	Provision of the contracted Services, in particular automated customer service through voice and chat AI Agents, transcription, handover to human agents, quality analysis and production of service metrics for the Controller; technical support, maintenance and security of the platform.

Duration of the processing	Processing of end users' Personal Data only begins after signature of the Services Agreement or, in its absence, of the Order Form. For the term of the Main Agreement and for the period strictly necessary to provide the Services. The retention period is set per data category, according to the purpose of each processing operation, in the table in Appendix III, completed by Visor.ai on the basis of the commercial terms agreed between the Parties before this Agreement is entered into. Where no specific period is set for a category, the standard period stated in Appendix III applies. Periods run from the date of each interaction or from the closure of the relevant process, depending on the data category. After termination of the Main Agreement, any remaining data is deleted within 90 (ninety) days, unless (i) a longer retention period is required by law, or (ii) a different period is set out in a specific annex required by the Controller, which prevails over this paragraph.
Location of the processing	• European Economic Area (EEA), Amazon Web Services (AWS) – European regions (eu-west-1 Ireland, eu-central-1 Frankfurt, among others in line with the Customer's requirements). • Personal Data is stored and processed in EEA regions, and Visor.ai does not, on its own initiative, transfer Personal Data outside the EEA. Some Sub-processors belong to corporate groups headquartered outside the EEA. Where occasional access from a third country takes place, in particular for technical support, security, abuse prevention or in response to a request from an authority, such access is limited to what is strictly necessary and relies on one of the mechanisms provided for in Chapter V of the GDPR, in particular an adequacy decision (including the EU-US Data Privacy Framework, for certified entities) or the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, in accordance with Clause 7.9.

APPENDIX III – DATA RETENTION

Data category	Applicable	Retention period	Criterion / Basis
Interaction Record **(AI Voice / AI Chat Agent)**	*As per contracted Services*	*Standard: 90 days (options: 12 or 24 months)*	*Purpose of providing the service*
Audio Recording **(AI Voice Agent)**	*As per contracted Services*	*30 days*	*Monitoring of call quality*
Quality & Insights Audio **(AI Quality Agent)**	*As per contracted Services*	*24 hours*	*Purpose of providing the service*
Source Transcript for Audit **(AI Quality Agent)**	*As per contracted Services*	*30 days*	*Purpose of providing the service*
Audit Results (AI Quality Agent)	*As per contracted Services*	*Standard: 6 months (option: 12 months)*	*Purpose of providing the service and quality and trend analysis*
Platform Activity Logs	*As per contracted Services*	*Standard: 90 days (option: 12 months)*	*Traceability of actions and identification of platform users. Includes account data of the Customer's users. Cf. CNPD Resolution No. 1638/2013*
Security and Infrastructure Logs	*Yes*	*12 months*	*Security of processing, detection and investigation of incidents (Art. 32 GDPR). Includes technical identifiers of platform users and data subjects (for example, user IDs and IP addresses). Fixed period, not subject to extension.*
Post-termination deletion	*Yes*	*90 days*	*Return or destruction after the end of the Main Agreement, unless a specific annex is required by the Controller*
Personal data of Data Subjects	*Yes*	*Follows the period of the operational category in which the data is included*	*Not a separate category; retention follows the categories above*
Sensitive Data **(Art. 9 GDPR)**	*As per contracted Services*	*Follows the applicable operational category – no automatic extension of the period*	*Applicable only if the Customer's use case involves it. Additional safeguards are agreed in writing before processing begins, in particular: a data protection impact assessment (DPIA) by the Customer with Visor.ai's support, access restricted to authorised personnel, and data minimisation.*

APPENDIX IV – TECHNICAL AND ORGANISATIONAL MEASURES

This Appendix describes the technical and organisational measures implemented by the Processor to ensure the security of the Personal Data processed under this Agreement, in accordance with Article 32 of the GDPR and

with ISO/IEC 27001:2022, a certification held by the Processor.

1. **Physical access control**

The Processor implements measures to prevent unauthorised persons from accessing the premises where Personal Data is processed, in particular:

- Access to the premises subject to mandatory identification and recording of entries and exits;
- Areas where Personal Data is processed are subject to additional access control;
- Cloud infrastructure in AWS data centres with recognised certifications (ISO/IEC 27001, SOC 2, among others), with physical controls managed by the cloud provider.

2. **System access control**

The Processor implements measures to prevent unauthorised access to processing systems, in particular:

- Mandatory multi-factor authentication (MFA) for access to critical systems and production environments;
- Strong password policies with minimum complexity and rotation requirements;
- Automatic locking of inactive sessions;
- Principle of least privilege applied to all user accounts (ISO/IEC 27001:2022 Annex A.5.15, A.8.2).

3. **Data access control**

The Processor implements measures to ensure that only authorised persons access Personal Data, and only to the extent strictly necessary, in particular:

- Role-based access control (RBAC) with differentiated profiles and permissions;
- Encryption of data at rest (AES-256) and in transit (TLS 1.2 or higher);
- Anonymisation and data minimisation wherever technically feasible and appropriate to the purpose;
- Access logging, recording the user, date, time and operations performed (ISO/IEC 27001:2022 Annex A.8.15).

4. **Transfer control**

The Processor implements measures to protect Personal Data during transmission and storage outside controlled systems, in particular:

- Encryption of data in transit with TLS 1.2 or higher for all communications;
- Encryption of data at rest with AES-256 in storage systems;
- Secure transmission mechanisms between the Processor and Sub-processors, with endpoints dedicated to the EEA;
- Verification and recording of the entities receiving data transfers.

5. **Operations control**

The Processor implements measures to ensure the control and traceability of operations on Personal Data, in particular:

- Centralised logging of operations on Personal Data (creation, modification, deletion);
- Modification operations restricted to authorised personnel;

- Segregation of production, development and test environments;
- Continuous monitoring of systems and processes with automatic alerts;
- Formal information security incident management plan with a dedicated team (ISO/IEC 27001:2022 Annex A.5.24 to A.5.28).

6. **Control of compliance with instructions**

The Processor implements measures to ensure that processing is carried out in accordance with the Controller's documented instructions, in particular:

- Information Security Management System (ISMS) certified to ISO/IEC 27001:2022;
- A documented set of internal policies and procedures subject to periodic review;
- Initial and ongoing information security and data protection training for staff, with mandatory confidentiality agreements;
- Documented procedure for the assessment and onboarding of suppliers (Sub-processors), with contractual data protection clauses;
- Annual internal audits and external ISO/IEC 27001 certification audits.

7. **Availability control**

The Processor implements measures to ensure the availability of Personal Data and its protection against accidental destruction or loss, in particular:

- Encrypted backups with tested recovery plans, with RTO and RPO objectives defined by criticality level;
- Documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), with periodic testing and annual review;
- Cloud infrastructure with redundant architecture (multi-AZ) at the compute layers;
- Continuous monitoring of service availability with alerts and escalation procedures (ISO/IEC 27001:2022 Annex A.5.29, A.5.30, A.8.13, A.8.14).

8. **Multi-tenant separation control**

The Processor implements measures to ensure the separation of Personal Data belonging to different Controllers, in particular:

- Strict logical separation between the environments and data of different customers (multi-tenancy);
- Unambiguous identification of the Controller associated with each processing operation;
- Dedicated access controls and encryption per customer where technically feasible (including a dedicated VPC model where contracted);
- Audit of operations that may involve data of multiple customers.

9. **Additional protection measures for the Artificial Intelligence layer**

Given the nature of the Services, the Processor implements additional measures specifically aimed at protecting the AI layer, in particular:

- Use of the native guardrails of the LLMs in use (Amazon Bedrock, Azure OpenAI Content Safety, Vertex AI Safety Filters);

- Use of custom guardrails developed by the Processor to detect and block prompt injection and cross-context access attempts;
- Hosting of LLMs on dedicated EU endpoints, aligning data residency with the EEA;
- Data sent to AI model providers through their APIs is not used to train or improve their models. Such data may be retained temporarily and to a limited extent by the providers, solely for security and abuse-prevention purposes and for the periods set in the respective providers' policies, and is not used for any other purpose.
- The Processor does not use Personal Data processed on behalf of the Controller to train general-purpose AI models.

APPENDIX V – LIST OF SUB-PROCESSORS

The Controller authorises the engagement of the Sub-processors listed in the table below. The up-to-date list is permanently available on the Visor.ai Trust Center at https://visor.ai/trust. Any change to the list is notified to the Controller at least 30 (thirty) days in advance, in accordance with Clause 7.8 of this Agreement.

Sub-processor	Purpose	Location	Storage outside the EEA
Amazon Web Services (AWS)	Cloud infrastructure, storage and compute; large language models through Amazon Bedrock	AWS EU regions (Ireland / Frankfurt; others upon formal request)	No
Out.Cloud	Management and operation of the cloud infrastructure (AWS), including administrative access to the environments where Personal Data is processed	Portugal, with access to the AWS environments in EU regions	No
Microsoft Azure (Speech Services and Azure OpenAI)	Speech-to-text (STT) and text-to-speech (TTS) through Azure Speech Services; large language models and TTS through Azure OpenAI	Azure EU regions (West Europe, Sweden Central, Germany West Central, France Central)	No
Google Cloud / Vertex AI (Gemini)	Gemini large language models for natural language processing	Google Cloud EU regions (europe-west8, Milan)	No
Deepgram	Speech-to-text (STT)	AWS EU/EEA regions[1]	No
AssemblyAI	Speech-to-text (STT)	AWS EU/EEA regions (eu-west-1, Dublin, Ireland)[2]	No
ElevenLabs	Text-to-speech (TTS)	EU/EEA regions, Google Cloud Platform infrastructure[3]	No
Vonage B.V.	Telecommunications services: phone numbers, call routing and messaging	AWS EU/EEA region (eu-west-1, Dublin, Ireland)	No
Google Workspace	Email, document storage and internal collaboration, where these contain Customer Personal Data, in particular when handling support requests and incidents	EU/EEA regions	No
Atlassian (Jira/Confluence)	Support request and incident management and technical documentation, where these include Customer Personal Data	EU/EEA regions	No

1. EU/EEA – dedicated EU endpoint (api.eu.deepgram.com), AWS regions in the EU, subject to the provider's policy; the specific region may vary while remaining within the EEA.
2. EU/EEA – dedicated EU endpoint (streaming.eu.assembly.ai).
3. EU/EEA – Enterprise contract with EU data residency enabled (eu.residency.elevenlabs.io) and Zero Retention Mode enabled via API, subject to the provider's policy; the specific region may vary while remaining within the

EEA.