

Data Processing Addendum (DPA)

This Data Processing Addendum (“**DPA**”) forms part of and supplements:

- (i) the Frontline CRM Platform Terms of Service accepted by the Customer through the Services;
 - (ii) any applicable Subscription Order;
 - (iii) any Enterprise Order Form;
 - (iv) any Pilot Order Form; and/or
 - (v) any separately executed Master SaaS Subscription Agreement,
- (collectively, the “Agreement”).

This DPA applies whenever **Frontline CRM GmbH** (“**Processor**” or “**Frontline CRM**”) Processes Personal Data on behalf of the Customer in connection with the Services.

Preamble

This DPA sets out the Parties' respective rights and obligations regarding the Processing of Personal Data in connection with the Services.

In the event of any conflict between this DPA and the applicable Agreement, the terms of this DPA shall prevail with respect to the Processing of Personal Data.

The Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, on behalf of its Authorized Affiliates, if any.

Electronic Acceptance

For Customers using the Services through website registration or self-service onboarding, acceptance of this DPA may occur electronically.

By creating an Account, activating a subscription, purchasing a subscription, accepting the Terms of Service, clicking an "I Agree", "Accept", "Continue" or similar button, or otherwise using the Services, the Customer agrees to be bound by this DPA.

For Customers entering into separately negotiated agreements, this DPA shall be deemed accepted upon execution of the applicable Agreement.

Electronic acceptance shall have the same legal effect as a handwritten signature.

1. Definitions

All capitalized terms not defined herein shall have the meaning given in the applicable Agreement or the GDPR. In addition:

"Agreement" means, as applicable, the Terms of Service, Subscription Order, Enterprise Order Form, Pilot Order Form and/or any separately executed Master SaaS Subscription Agreement.

"Data Protection Laws" means the GDPR, the Swiss Federal Act on Data Protection, Romanian Law No. 190/2018, and any other applicable data protection legislation.

"GDPR" means Regulation (EU) 2016/679.

“Standard Contractual Clauses” means the EU Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914.

“Subprocessor” means any third party engaged by the Processor that Processes Personal Data on behalf of the Controller.

"Subscription Order" means the electronic or written order confirmation, checkout flow, order summary or other commercial document specifying the Customer's selected subscription plan, pricing, billing cycle and applicable usage limits.

"Terms of Service" means the Frontline CRM Platform Terms of Service available at: <https://frontline-crm.com/terms-of-service>

2. Roles and Scope

2.1 The Customer is the Controller and Frontline CRM is the Processor of the Personal Data Processed in connection with the Services.

2.2 The Controller is solely responsible for determining the lawful basis for Processing Personal Data and for ensuring that all required notices, consents and transparency obligations have been satisfied.

2.3 The Processor shall Process Personal Data only on documented instructions from the Controller (including the applicable Agreement, Service configuration, account settings and other documented Customer instructions) and in accordance with Data Protection Laws.

2.4 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable Data Protection Laws.

2.5 Details of the Processing (subject matter, duration, nature, purpose, categories of Data Subjects and Personal Data) are set out in **Annex I**.

3. Aggregated and Anonymized Analytics

The Processor may collect, use, process and disclose aggregated and anonymized data derived from the Customer's use of the Service and from the Personal Data for the purposes of analysing usage patterns, improving and developing the Service, statistical analysis, and product enhancement.

Such aggregated and anonymized data must not contain any Personal Data and must not allow for the identification of the Customer or any Data Subjects (including Candidates). The Processor shall implement appropriate technical and organisational measures to ensure that no Personal Data can be re-identified from such aggregated data.

For the avoidance of doubt, the Processor shall not use any Personal Data for its own model training, service improvement of third-party AI providers, or any other purpose not expressly authorised under this DPA, unless expressly agreed in writing by the Controller.

4. Controller Responsibilities

The Customer, as Controller, remains solely responsible for:

- determining the lawful basis for Processing;
- providing legally required Candidate notices and disclosures;
- obtaining any required consents or opt-ins;
- responding to data subject requests;
- determining retention periods;
- ensuring that imported Personal Data was lawfully collected; and
- ensuring that its use of the Services complies with applicable employment, privacy, telecommunications and AI laws.

5. Processor Obligations

The Processor shall: (a) Process Personal Data solely in accordance with the Controller's documented instructions; (b) Ensure that persons authorised to Process Personal Data are bound by confidentiality obligations; (c) Implement and maintain appropriate Technical and Organisational Measures as set out in **Annex II**; (d) Assist the Controller (at Controller's reasonable expense) in responding to Data Subject requests and fulfilling GDPR obligations (Articles 32–36); (e) Notify the Controller without undue delay and, in any event, within 48 hours of becoming aware of a Personal Data Breach; (f) Upon termination or expiry of the applicable Agreement, handle return, deletion or anonymization of Personal Data in accordance with Section 11 of this DPA.

6. Data Subject Rights

6.1 The Processor shall promptly notify the Controller of any Data Subject Request it receives.

6.2 The Processor shall not respond to such requests itself, except by redirecting the Data Subject to the Controller.

6.3 The Processor shall provide commercially reasonable assistance to the Controller in responding to Data Subject Requests.

7. Subprocessors

7.1 The Controller grants the Processor general written authorisation to engage Subprocessors. The Processor shall impose on each Subprocessor data protection obligations substantially equivalent to those contained in this DPA and shall remain responsible for the acts and omissions of its Subprocessors in accordance with this DPA and applicable Data Protection Laws.

7.2 The current list of Subprocessors is set out in **Annex I**. The Processor shall notify the Controller in writing of any intended addition or replacement of a Subprocessor at least 14 days in advance.

7.3 The Controller may object to a new Subprocessor on reasonable data protection grounds within 10 business days. If the objection cannot be reasonably accommodated, the Controller may terminate the affected Service without penalty.

7.4 The Processor may replace a Subprocessor immediately where required to address security, legal, operational or service continuity concerns, provided that the Processor informs the Controller without undue delay.

8. AI-Assisted Processing

8.1 The Customer acknowledges that certain functionality of the Service may involve Processing by third-party AI service providers engaged by the Company as Subprocessors.

8.2 Such Processing may include:

- conversation summarization;
- transcription;
- translation;
- AI-assisted communication functionality;
- preliminary candidate categorization; and

other Customer-configured assistive recruitment workflows.

8.3 The Company shall use commercially reasonable efforts to configure third-party AI providers in a manner intended to restrict the use of Customer Personal Data for generalized model training or unrelated service improvement purposes, where such controls are commercially and technically available.

8.4 The Customer acknowledges that:

- (i) certain AI providers may process Personal Data in multiple jurisdictions;
- (ii) certain provider-side retention, logging or security practices may not be fully controlled by the Company; and
- (iii) AI-generated outputs may be probabilistic, incomplete or inaccurate.

8.5 The Customer remains solely responsible for reviewing AI-assisted outputs before using them in connection with recruitment or employment-related decisions.

9. International Transfers

9.1 The Processor shall not transfer Personal Data outside the European Economic Area (EEA), Switzerland or any other jurisdiction that has been recognised as providing an adequate level of data protection, unless appropriate safeguards are in place in accordance with applicable Data Protection Laws.

9.2 The Controller acknowledges and agrees that certain Subprocessors process Personal Data outside the EEA/Switzerland, in particular:

- ElevenLabs (United States) – for AI voice agent, call recording and transcription;
- Cloudflare (global) – for CDN and security services.

9.3 For all transfers of Personal Data to third countries, the Parties shall apply the EU Standard Contractual Clauses (Module 2 – Controller to Processor) as approved by the European Commission Implementing Decision (EU) 2021/914, which are hereby incorporated by reference into this DPA.

Where applicable, the Standard Contractual Clauses shall be interpreted in accordance with the requirements of the Swiss Federal Act on Data Protection and guidance of the Swiss Federal Data Protection and Information Commissioner.

9.4 The Parties agree that:

- Annex I, II and III of the Standard Contractual Clauses shall be deemed completed with the information set out in **Annex I** of this DPA;
- The Processor shall ensure that each Subprocessor in a third country executes the Standard Contractual Clauses (Module 3 – Processor to Processor) or equivalent safeguards.

9.5 Additional Safeguards

In addition to the Standard Contractual Clauses, the Processor has implemented (and shall maintain) the following supplementary measures for transfers presenting higher risk (particularly to ElevenLabs):

- Encryption of Personal Data in transit and at rest using industry-standard algorithms;
- Strict access controls and “need-to-know” principle;
- Reduced retention periods (where technically configurable);
- Regular reviews of the laws and practices in the recipient country;
- Prompt notification to the Controller in case of any government access request or change in circumstances that may affect the safeguards.

9.6 Transfer Impact Assessment

The Processor has conducted a Transfer Impact Assessment (TIA) for material international transfers. A high-level summary of the TIA and supplementary measures is available to the Controller upon reasonable request.

9.7 The Controller acknowledges that it is responsible for ensuring that its own instructions and use of the Service (including call recording, AI voice usage and candidate communications) comply with applicable laws regarding international transfers.

9.8 If the safeguards described in this Section become insufficient to comply with Data Protection Laws, the Parties shall work together in good faith to implement additional measures or, as a last resort, suspend or terminate the affected part of the Service.

10. Audits

10.1 Upon reasonable written request and no more than once annually, the Company shall make available information reasonably necessary to demonstrate compliance with this DPA.

10.2 Where such information is insufficient to demonstrate compliance with applicable data protection law, the Customer may request an audit conducted:

- (i) during normal business hours;
- (ii) subject to reasonable confidentiality, security and access restrictions;
- (iii) in a manner that avoids disruption to the Company’s business operations; and
- (iv) without access to data relating to other customers or internal proprietary systems unrelated to the Services.

10.3 The Company may satisfy audit obligations through:

- third-party certifications;
- independent audit reports;
- security questionnaires;
- compliance reports; or
- remote assessments,

where reasonably appropriate.

10.4 Unless a material breach of this DPA is identified, the Customer shall bear its own audit costs.

10.5 The Company may object to any auditor reasonably considered unsuitable due to confidentiality, security or competitive concerns.

11. Return and Deletion

11.1 Upon termination or expiry of the Services, the Company shall make available a reasonable mechanism allowing the Customer to export Customer Personal Data for a limited period.

11.2 Following such period, the Company shall delete or anonymize Customer Personal Data unless retention is required:

- (i) by applicable law;
- (ii) for security, fraud prevention or dispute resolution purposes; or
- (iii) as part of standard backup, logging or disaster recovery systems.

11.3 Personal Data retained in backups, logs or disaster recovery systems shall remain protected under this DPA and shall not be actively Processed except as required for security, legal or operational purposes.

11.4 Where technically and commercially feasible, the Company shall use reasonable efforts to ensure deletion or expiration of Customer Personal Data stored by Subprocessors in accordance with applicable retention settings and contractual arrangements.

12. Limitation of Liability

12.1 Except as expressly stated otherwise in this DPA, the exclusions, disclaimers and limitations of liability set out in the applicable Agreement shall apply to this DPA and to all Processing activities conducted under it.

For the avoidance of doubt:

- (i) all references in the applicable Agreement to the “Service”, “Agreement”, “Fees”, “Claims” or similar terms shall be deemed to include this DPA and any Processing of Personal Data conducted hereunder;
- (ii) any liability of the Processor arising out of or in connection with this DPA, including any breach of this DPA or any Personal Data Breach, shall be subject to the same exclusions, disclaimers and aggregate liability limitations set forth in the applicable Agreement; and
- (iii) nothing in this DPA shall be construed as expanding the Processor’s liability beyond the limitations expressly set out in the applicable Agreement.

The Parties acknowledge that the liability limitations and exclusions set forth in the applicable Agreement constitute an essential basis of the bargain between the Parties, reflect the agreed allocation of risk and responsibility, and are reflected in the pricing of the Services, including any Pilot or beta-stage pricing.

12.2 The Processor shall have no liability for any recruitment, hiring or employment-related decisions made by the Controller or its Users, including decisions based on AI-assisted outputs, summaries, transcripts, candidate categorizations or communications generated through the Services.

All such decisions remain solely the responsibility of the Controller.

13. Miscellaneous

13.1 This DPA survives termination of the applicable Agreement for as long as the Processor Processes Personal Data on behalf of the Controller.

13.2 This DPA is governed by the law applicable to the applicable Agreement, without prejudice to the governing law and jurisdiction provisions applicable to the Standard Contractual Clauses in Annex III.

14. Order of Precedence

In the event of any inconsistency between the applicable documents, the following order of precedence shall apply:

1. Master SaaS Subscription Agreement (if applicable);
2. Enterprise Order Form, Pilot Order Form or Subscription Order;
3. This DPA (with respect to Personal Data Processing matters);
4. Terms of Service;
5. Privacy Policy;
6. Pricing Page.

For the avoidance of doubt, the Privacy Policy and Pricing Page are informational in nature and shall not override contractual obligations contained in this DPA or the applicable Agreement.

COMPANY **Frontline CRM GmbH**

CUSTOMER _____

Signature: _____

Signature: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Address: _____

Address: _____

Annex I – Details of Processing and List of Subprocessors

A. Details of Processing

- **Subject Matter:** Provision of the Frontline CRM SaaS platform for recruitment workflow management.
- **Duration:** The term of the applicable Agreement and any applicable Subscription Order, Pilot Order Form or Enterprise Order Form, plus any post-termination deletion period.
- **Nature and Purpose:** Storage, processing, transmission, AI-assisted summarization, communication (WhatsApp, SMS, voice), and management of Candidate Data.
- **Categories of Data Subjects:** Job candidates, Client Users.
- **Categories of Personal Data:** Name, phone number, email, location, application data, WhatsApp/SMS/call content, call recordings & transcripts, AI summaries, CVs/documents (if uploaded), technical metadata.
- **Special Categories:** Not intentionally processed. Customer shall not instruct processing of special category data without prior written agreement.

B. List of Subprocessors

Provider	Service / Purpose	Candidate Data	Region
OVH	Cloud hosting & storage	Yes	Europe
Self-managed Postgres	Main application database	Yes	Europe
Scaleway	Transactional emails	Limited	Europe
Vonage	Phone numbers, SMS, call routing	Yes	Europe
Meta / WhatsApp	WhatsApp Business messaging	Yes	Europe / Global
Mistral	AI screening, summarization, suggestions	Yes	Europe
ElevenLabs	AI voice agent, call recording & transcription	Yes	Europe / Global
Cloudflare	CDN & security	Potentially	Global
Google Workspace	Internal administration & support	Limited	Europe / Global
Posthog	Logs, analytics, error tracking	Limited	Europe / Global
Mollie	Payment processing	No	Europe

Annex II – Technical and Organisational Measures (TOMs)

The Processor shall implement and maintain reasonable technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed in connection with the Services.

The measures described below reflect the nature, scope, context and purposes of the Processing, the state of the art, implementation costs and the risks associated with the Processing activities conducted under the Agreement and this DPA.

1. Access Control and Authentication

The Processor implements reasonable access control measures intended to limit access to Personal Data to authorized personnel with a legitimate business need to access such data.

Such measures may include:

- role-based access controls;
- least-privilege principles;
- password policies;
- multi-factor authentication for administrative systems where appropriate;
- internal authorization procedures;
- employee confidentiality obligations; and
- access revocation procedures upon termination or role change.

Administrative access to production systems is restricted to authorized personnel.

2. Infrastructure and Hosting Security

The Services are hosted using third-party infrastructure providers selected by the Processor based on commercially reasonable security and operational criteria.

Security measures may include:

- logical separation of customer environments;
- firewall and network protection measures;
- encrypted communications using TLS or equivalent technologies;
- vulnerability management processes;
- infrastructure monitoring;
- system hardening practices where appropriate; and
- redundancy and backup mechanisms.

The Processor may use cloud infrastructure, hosting and content delivery providers located in multiple jurisdictions.

3. Encryption and Data Transmission

The Processor uses commercially reasonable encryption measures designed to protect Personal Data during transmission and storage where appropriate.

Such measures may include:

- TLS encryption for data in transit;
- encrypted storage mechanisms where supported;
- encrypted backups where appropriate; and
- secure credential management practices.

4. Logging and Monitoring

The Processor maintains reasonable logging and monitoring controls appropriate to the nature of the Services and the pilot-stage nature of the platform.

Such controls may include:

- authentication and access logs;
- administrative activity logging;
- deletion and export logs;
- operational event logging;
- API activity monitoring;
- incident investigation logging; and
- security monitoring controls,

where technically available and operationally appropriate.

Log retention periods may vary depending on technical, operational and security requirements.

5. Availability, Backups and Recovery

The Processor maintains commercially reasonable backup and recovery measures intended to support operational resilience and restoration of service availability.

Such measures may include:

- periodic backups;
- disaster recovery procedures;
- infrastructure redundancy;
- incident response processes; and
- service continuity planning.

Backup systems may retain copies of Personal Data for limited periods in accordance with standard operational and security practices.

6. Personnel Security and Confidentiality

Personnel authorized to Process Personal Data are subject to confidentiality obligations and internal access restrictions.

The Processor maintains commercially reasonable internal organizational measures relating to:

- personnel onboarding and offboarding;
- access authorization procedures;
- confidentiality commitments;
- internal security policies; and
- limitation of access to Personal Data.

7. Subprocessors and Third-Party Providers

The Processor may engage third-party providers and Subprocessors in connection with the provision of the Services, including:

- hosting providers;
- telecommunications providers;
- messaging providers;
- AI service providers;
- infrastructure vendors; and
- support providers.

The Processor uses commercially reasonable efforts to impose data protection and security obligations on such providers appropriate to the nature of the Processing activities performed.

The Processor may use enterprise, no-training or equivalent configurations offered by AI providers where commercially and technically available in order to reduce the use of Customer Personal Data for generalized model training or unrelated service improvement purposes.

8. AI-Assisted Functionality and Human Review Support

The Services may include AI-assisted functionality such as:

- conversation summarization;
- transcription;
- translation;
- preliminary candidate categorization; and
- workflow assistance functionality.

Where technically available, the Services may allow Customer users to review underlying candidate responses, transcripts or conversation history associated with AI-assisted outputs in order to support human review and verification of AI-generated information.

AI-generated outputs may be probabilistic in nature and may contain inaccuracies, omissions or incomplete information.

9. Incident Management

The Processor maintains commercially reasonable processes for identifying, investigating and responding to security incidents affecting Personal Data.

Such processes may include:

- internal incident escalation procedures;
- incident investigation workflows;
- remediation procedures; and
- notification procedures consistent with applicable law and the DPA.

10. Data Retention and Deletion

The Processor maintains commercially reasonable procedures relating to deletion, anonymization and retention of Personal Data.

Following termination or expiry of the Services, Personal Data may be:

- returned to the Controller;
- deleted;
- anonymized; or
- retained in backups, logs or archival systems for limited periods,

subject to legal, operational, security and disaster recovery requirements.

The Processor may use commercially reasonable efforts to configure retention settings with applicable Subprocessors where such controls are technically available.

Annex III – Standard Contractual Clauses and International Transfers

1. International Transfers

To the extent that Processing of Personal Data under the Agreement or this DPA involves transfers of Personal Data outside the European Economic Area (“EEA”), the United Kingdom or Switzerland to jurisdictions not recognized as providing an adequate level of data protection under applicable law, the Parties shall implement appropriate safeguards in accordance with applicable data protection laws.

Such safeguards may include:

- adequacy decisions;
- the European Commission Standard Contractual Clauses;
- the UK International Data Transfer Addendum;
- Swiss transfer mechanisms; or
- other lawful transfer mechanisms recognized under applicable law.

2. EU Standard Contractual Clauses

Where required under Article 46 GDPR, the Parties incorporate by reference the Standard Contractual Clauses approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the “EU SCCs”).

The following terms shall apply:

Module

Module Two (Controller to Processor) shall apply where the Customer acts as Controller and the Company acts as Processor.

Where applicable, Module Three (Processor to Processor) may apply in relation to onward transfers involving Subprocessors.

Clause 7 – Docking Clause

The optional docking clause shall apply.

Clause 9 – Use of Subprocessors

Option 2 (general written authorization) shall apply.

The Processor shall maintain and make available an up-to-date list of Subprocessors in accordance with the DPA.

Clause 11 – Redress

The optional language in Clause 11 shall not apply.

Clause 17 – Governing Law

The SCCs shall be governed by the laws of Romania.

Clause 18 – Choice of Forum and Jurisdiction

The courts of Romania shall have jurisdiction.

3. UK Transfers

Where Personal Data originating from the United Kingdom is transferred outside the United Kingdom, the Parties shall rely on:

- the UK International Data Transfer Addendum issued by the UK Information Commissioner's Office; or
- another lawful UK transfer mechanism recognized under applicable law.

The EU SCCs, as modified by the applicable UK Addendum, shall apply to such transfers.

4. Swiss Transfers

Where Personal Data originating from Switzerland is transferred outside Switzerland, the Parties agree that:

- references to the GDPR in the SCCs shall also include the Swiss Federal Act on Data Protection ("FADP") where applicable;
- references to "Member State" shall be interpreted to include Switzerland where required;
- Swiss data subjects may exercise rights under the SCCs in Switzerland where applicable; and
- the SCCs shall be interpreted in accordance with guidance issued by the Swiss Federal Data Protection and Information Commissioner.

5. Supplementary Measures

The Parties acknowledge that the Company may implement supplementary technical and organizational safeguards appropriate to the nature of the Services and the associated transfer risks.

Such safeguards may include:

- encryption in transit;
- access controls;
- contractual safeguards with Subprocessors;
- logical separation of customer environments;
- minimization of access to Personal Data; and
- commercially reasonable security measures described in **Annex II** (Technical and Organisational Measures).

6. Subprocessors and Onward Transfers

The Customer authorizes the Company to engage Subprocessors in accordance with the DPA.

The Company shall use commercially reasonable efforts to ensure that onward transfers involving Subprocessors are subject to contractual safeguards substantially consistent with applicable transfer requirements.

7. Conflicts

In the event of conflict between this Annex and the DPA, this Annex shall govern solely with respect to international transfer requirements to the extent required by applicable law.