

FRONTLINE CRM PRIVACY POLICY

Last Updated: 13 October 2026

1. Introduction

This Privacy Policy ("Privacy Policy") explains how Frontline CRM GmbH ("Frontline", "we", "our" or "us") collects, uses, discloses and otherwise processes personal data in connection with the Frontline CRM platform, websites, applications, AI-assisted functionality and related services (collectively, the "Services").

This Privacy Policy applies to:

- visitors of our website;
- individuals creating or using Accounts;
- representatives of our Customers;
- Candidates whose personal data may be processed through the Services; and
- other individuals interacting with us in connection with the Services.

This Privacy Policy is intended to provide transparency regarding our processing activities and supplements, but does not replace, recruitment privacy notices provided by employers, recruitment agencies, staffing providers or other organizations using the Services ("Customers").

Where a Customer uses Frontline for recruitment activities, the Customer remains the primary Controller of Candidate Data and is responsible for providing Candidate-facing privacy notices.

Your use of the Services is also subject to our Terms of Service and Data Processing Addendum ("DPA"), both of which are incorporated by reference.

2. Who We Are

Frontline CRM GmbH is a technology company that provides software-as-a-service (SaaS) solutions supporting recruitment and candidate relationship management activities.

Frontline primarily acts as a Processor processing Personal Data on behalf of its Customers in connection with the Services.

Frontline may also act as an independent Controller with respect to limited categories of Personal Data necessary to operate, secure and administer the Services, including website administration, account management, subscription management, billing, customer support, security monitoring and compliance with legal obligations.

Frontline CRM GmbH

Hagenholzstrasse 90

8050 Zurich

Switzerland

Email: privacy@frontline-crm.com

Website: <https://frontline-crm.com>

If you have any questions regarding this Privacy Policy or our data processing practices, you may contact us using the details above.

3. Scope of this Privacy Policy

This Privacy Policy applies to personal data processed in connection with:

- use of our website;
- account registration;
- subscription management;
- customer support;
- communications with Frontline;
- operation and security of the Services;
- AI-assisted functionality;
- WhatsApp and SMS functionality;
- AI voice functionality;
- call recording and transcription functionality; and
- Candidate Data processed through the Services.

This Privacy Policy does not apply to:

- third-party websites;
- third-party services integrated by Customers;
- personal data processed independently by Customers outside the Services; or
- processing activities performed by Customers as independent Controllers.

Customers may have their own privacy notices governing their recruitment activities.

Candidates should review the applicable Customer's privacy notice for additional information.

4. Our Roles Under Data Protection Laws

Our role depends on the type of information being processed.

4.1 Frontline as Processor

Frontline primarily acts as a Processor processing personal data on behalf of Customers.

In particular, Frontline processes Candidate Data solely to provide the Services and in accordance with Customer instructions.

Frontline does not determine:

- recruitment purposes;
- hiring objectives;
- candidate evaluation criteria;
- retention periods;
- recruitment decisions; or
- employment decisions.

All such decisions remain solely under the Customer's control.

Customers remain responsible for:

- recruitment and hiring decisions;

- defining recruitment purposes and criteria;
- candidate communications;
- determining legal bases for processing;
- compliance with employment and recruitment laws;
- providing Candidate-facing privacy notices;
- obtaining legally required consents; and
- responding to data subject requests.

4.2 Frontline as Independent Controller

Frontline may independently process limited personal data where necessary to:

- operate the Services;
- provide customer support;
- maintain service reliability;
- administer subscriptions and billing;
- secure the platform;
- detect abuse, spam or security incidents;
- comply with legal obligations; and
- improve platform stability, security and operational performance.

In these situations, Frontline acts as an independent Controller.

5. Categories of Personal Data We Process

The categories of personal data we process depend on how you interact with the Services.

5.1 Website Visitors

We may process:

- IP address;
- browser type;
- device information;
- operating system;
- language preferences;
- website usage information;
- pages visited;
- referral URLs;
- session information; and
- cookie identifiers.

5.2 Account Users and Customer Representatives

We may process:

- name;
- business email address;
- company name;
- job title;
- telephone number;
- account credentials;
- authentication information;
- subscription information;
- billing information;
- communications with Frontline;

- support requests; and
- activity logs.

5.3 Candidate Data

Customers may upload or process Candidate Data through the Services, including:

- name;
- contact information;
- CVs and resumes;
- employment history;
- education history;
- skills and qualifications;
- communications;
- application responses;
- interview notes;
- AI-generated summaries;
- transcripts; and
- other recruitment-related information.

Customers determine which Candidate Data is processed through the Services.

5.4 AI Voice, Call Recording and Transcription Data

Where enabled by a Customer, we may process:

- voice recordings;
- call transcripts;
- AI-generated summaries;
- call metadata;
- timestamps; and
- communication logs.

Such functionality is enabled and controlled by Customers.

Customers remain responsible for providing all legally required notices and obtaining all legally required consents.

5.5 Technical and Security Information

We may process:

- access logs;
- authentication logs;
- device identifiers;
- system events;
- error logs;
- API logs;
- security events;
- performance metrics; and
- other operational information necessary to operate and secure the Services.

6. How We Use Personal Data

We process personal data only to the extent necessary to operate, provide, maintain, secure and improve the Services.

Depending on your interaction with the Services, we may process personal data to:

- provide and administer Accounts;
- provide access to the Services;
- manage subscriptions and billing;
- provide customer support and troubleshooting;
- operate and secure the platform;
- monitor performance and reliability;
- detect, prevent and investigate security incidents, abuse or fraud;
- provide AI-assisted functionality;
- facilitate communications through the Services;
- generate analytics and operational insights;
- comply with legal and regulatory obligations; and
- improve the stability, security and functionality of the Services.

Where Frontline acts as a Processor, we process personal data solely on behalf of Customers and in accordance with their documented instructions.

Where Frontline acts as an independent Controller, we process only the minimum amount of personal data reasonably necessary to operate and administer the Services.

We do not sell personal data. We do not use Candidate Data to train our own general-purpose artificial intelligence models.

7. Candidate Data Processing

Customers use the Services to manage recruitment and candidate relationship management activities.

For recruitment-related activities conducted through the Services:

- the Customer is the Controller of Candidate Data; and
- Frontline acts as a Processor processing Candidate Data on behalf of the Customer.

Customers remain solely responsible for:

- recruitment and hiring decisions;
- defining recruitment purposes and criteria;
- candidate communications;
- determining legal bases for processing;
- compliance with employment and recruitment laws;
- providing Candidate-facing privacy notices;
- obtaining legally required consents;
- determining retention periods; and
- responding to data subject requests.

Frontline does not independently decide:

- whom to recruit;
- whom to contact;
- whom to interview;
- whom to hire;
- how long Candidate Data should be retained; or
- how Candidate Data should be evaluated.

Frontline processes Candidate Data solely to provide the Services and in accordance with Customer instructions.

If you are a Candidate and wish to exercise your privacy rights (including requests for access, correction, deletion, restriction, objection or portability), we strongly recommend that you contact the relevant hiring company, employer, recruitment agency or staffing provider that collected your information.

Where appropriate, Frontline will assist Customers in responding to such requests in accordance with applicable law and the Data Processing Addendum.

8. AI-Assisted Functionality

The Services may include AI-Assisted Functionality designed to support recruitment and administrative workflows.

Depending on the enabled functionality, AI-Assisted Functionality may include:

- AI-generated summaries;
- AI-assisted communication workflows;
- AI voice interactions;
- preliminary candidate categorizations;
- suggested responses;
- transcription services;
- candidate insights; and
- other assistive tools.

AI-Assisted Functionality is intended solely to assist human users and administrative processes.

AI-generated outputs:

- are informational only;
- may be inaccurate, incomplete or inconclusive;
- may contain errors, omissions or biases;
- may not reflect all relevant Candidate information; and
- must not be relied upon as the sole basis for any decision.

The Services do not automatically:

- reject Candidates;
- rank Candidates;
- prioritize Candidates;
- shortlist Candidates;
- advance Candidates;
- exclude Candidates;
- select Candidates; or
- make hiring or employment-related decisions.

Customers remain solely responsible for exercising independent judgment and implementing appropriate human oversight.

Customers are responsible for informing Candidates when AI-Assisted Functionality is used, where required by applicable law.

We do not use Candidate Data to train our own general-purpose AI models.

Customers shall not use the Services for:

- candidate ranking;

- suitability scoring;
- hiring prediction;
- personality profiling;
- emotion recognition;
- behavioral profiling; or
- other prohibited uses under applicable law.

9. Voice Calls, Call Recording and AI Voice Functionality

Where enabled by a Customer, the Services may include AI-assisted voice functionality provided through third-party providers, including ElevenLabs.

Such functionality may involve:

- AI voice interactions;
- call recording;
- transcription;
- AI-generated summaries;
- telecommunications services; and
- international data transfers.

Candidates will be informed at the beginning of such calls that:

- they are interacting with an AI assistant; and
- the call may be recorded and transcribed,

to the extent required by applicable law.

Customers remain solely responsible for:

- determining whether such functionality may lawfully be used;
- obtaining all legally required notices, disclosures and consents;
- complying with telecommunications laws;
- complying with employment laws;
- complying with privacy laws; and
- complying with applicable international transfer requirements.

Where required by applicable law, Customers shall provide Candidates with an alternative non-recorded communication channel.

Frontline does not determine:

- whether call recording requires consent;
- which lawful basis applies to a call;
- which retention period applies to voice recordings; or
- which disclosures must be provided under local law.

These decisions remain solely the responsibility of the Customer.

Voice recordings, transcripts and AI-generated summaries may be processed by third-party providers located outside the EEA or Switzerland, including ElevenLabs in the United States.

Additional information regarding international transfers is available below and in our Data Processing Addendum.

10. WhatsApp and SMS Communications

The Services may enable Customers to communicate with Candidates using:

- WhatsApp Business;
- SMS messaging; and
- other supported communications channels.

Such functionality may involve:

- sending messages;
- receiving messages;
- storing communication history;
- AI-assisted responses;
- AI-assisted summarization; and
- communication analytics.

Customers remain solely responsible for:

- determining whether such communications may lawfully be used;
- obtaining all legally required notices and consents;
- complying with telecommunications laws;
- complying with marketing and anti-spam laws;
- maintaining opt-out mechanisms where required by law; and
- complying with applicable privacy laws.

Customers are responsible for ensuring that Candidates are appropriately informed when AI-assisted messaging functionality is used.

Certain communications functionality depends on third-party providers, including Meta/WhatsApp and Vonage.

Frontline does not control the availability, functionality or policies of such providers and shall not be liable for outages, interruptions or changes introduced by them.

11. International Data Transfers

The Services may involve the transfer of personal data outside the European Economic Area ("EEA"), Switzerland or the United Kingdom.

In particular, certain Third-Party Providers used by Frontline may process personal data in jurisdictions outside the EEA or Switzerland, including the United States.

Most notably, AI voice functionality may involve the use of ElevenLabs, a provider located in the United States.

Depending on the enabled functionality, international transfers may occur in connection with:

- AI voice interactions;
- call recordings;
- transcription services;
- AI-generated summaries;
- cloud infrastructure;
- customer support; and
- operational services.

Where required by applicable law, Frontline implements appropriate safeguards for such transfers, including:

- EU Standard Contractual Clauses (SCCs);
- supplementary technical and organizational measures; and
- contractual obligations imposed on subprocessors.

Additional information regarding international transfers is available in our Data Processing Addendum or upon request.

Customers remain responsible for providing any disclosures required under applicable law regarding international transfers affecting their Candidates.

12. Subprocessors and Service Providers

Frontline may engage Third-Party Providers and subprocessors to support the operation, delivery and security of the Services.

Such providers may include, without limitation:

- OVH;
- Scaleway;
- Cloudflare;
- Vonage;
- Meta / WhatsApp;
- ElevenLabs;
- Mistral AI;
- Google Workspace;
- Posthog; and
- other operational service providers.

These providers may be engaged in connection with:

- cloud hosting and infrastructure;
- telecommunications;
- messaging services;
- AI-assisted functionality;
- analytics and monitoring;
- customer support;
- security operations; and
- business continuity.

Frontline uses commercially reasonable efforts to require appropriate privacy, confidentiality and security commitments from such providers.

The list of subprocessors may be updated from time to time.

The most current list of subprocessors is available in the Data Processing Addendum or upon request.

13. Data Retention

We retain personal data only for as long as reasonably necessary to:

- provide the Services;
- fulfill contractual obligations;

- comply with legal obligations;
- resolve disputes;
- enforce our agreements;
- maintain security; and
- protect our legitimate interests.

Retention periods vary depending on the type of information involved.

Customers remain solely responsible for determining retention periods applicable to Candidate Data processed through the Services.

Where Frontline acts as a Processor, Candidate Data will be retained in accordance with:

- Customer instructions;
- applicable law; and
- the Data Processing Addendum.

Voice recordings, transcripts and AI-generated summaries shall be retained only for as long as reasonably necessary for the purposes for which they were collected, unless otherwise required by law or instructed by the Customer.

Upon termination of the Services, Customer Data will be handled in accordance with applicable contractual terms, Customer instructions and the Data Processing Addendum.

14. Data Subject Rights

Depending on your jurisdiction and applicable law, you may have certain rights regarding your personal data, including the right to:

- access your personal data;
- correct inaccurate information;
- request deletion;
- request restriction of processing;
- object to processing;
- request data portability; and
- withdraw consent where processing is based on consent.

If you are a Candidate whose information was collected by an employer, recruitment agency, staffing provider or other Customer, we strongly recommend that you direct your request to that Customer in the first instance.

This is because the relevant Customer is the primary Controller of your personal data for recruitment purposes.

Where appropriate, Frontline will assist Customers in responding to such requests in accordance with applicable law and the Data Processing Addendum.

We may request additional information to verify your identity before responding to a request.

Certain rights may be limited by applicable law.

15. Security Measures

Frontline implements reasonable technical, organizational and administrative measures designed to protect personal data against unauthorized access, disclosure, alteration, loss or destruction.

Such measures may include:

- role-based access controls;
- multi-factor authentication;
- encryption in transit;
- encryption at rest, where applicable;
- logging and monitoring;
- backup procedures;
- incident response procedures;
- vulnerability management;
- vendor management controls; and
- personnel access restrictions.

No internet-based service can be guaranteed to be completely secure.

Accordingly, while we implement reasonable safeguards, we cannot guarantee absolute security.

If we become aware of a Personal Data Breach, we will act in accordance with applicable law and our contractual obligations.

16. Cookies and Similar Technologies

Our website may use cookies and similar technologies to:

- operate the website;
- remember preferences;
- maintain security;
- analyze website usage;
- improve performance; and
- enhance user experience.

Cookies may be classified as:

- strictly necessary cookies;
- functional cookies;
- analytics cookies; and
- other cookies described in our Cookie Policy.

Where required by applicable law, we will obtain consent before placing non-essential cookies on your device.

You may configure your browser settings to reject certain cookies, although doing so may affect website functionality.

Additional information may be provided in a separate Cookie Policy.

17. Changes to this Privacy Policy

We may update this Privacy Policy from time to time.

Material changes will be communicated through:

- our website;
- the Services;
- email notifications; or

- account notifications.

Unless otherwise stated, updated versions become effective upon publication.

Your continued use of the Services following the effective date constitutes acknowledgement of the updated Privacy Policy.

18. Contact Information

If you have any questions regarding this Privacy Policy or our data processing practices, please contact us at privacy@frontline-crm.com.