Data Processing Agreement

Molte

Version 2026-04-29 • Effective date 2026-04-29
Official data processing agreement from Molte

Version:	2026-04-29
Effective date:	2026-04-29
Copy type:	Template copy
Document hash:	1c9ae077d95ac526f711042d32f4b68b22c9383c8f9351682dab87c897566cae
Reference page:	/databehandleravtale

Parties and roles

This Data Processing Agreement is entered into between Molte as processor and the customer organization as controller for personal data processed in Molte.

Scope and purpose

The processor may process personal data only to deliver the recruitment platform, including receiving applications, storing candidate documents, organizing pipelines, generating analytics, and supporting AI-assisted candidate evaluation according to the controller's instructions.

Categories of data and data subjects

- Applicants and candidates, including contact details, CVs, cover letters, assessments, and interview-related notes.
- Customer users such as recruiters, hiring managers, and administrators using the platform.
- Uploaded files, communication records, and metadata related to recruitment processes.
- Evaluation data, ranking outputs, AI-assisted summaries, and workflow activity records.

Processor obligations

- Process personal data solely in accordance with documented instructions from the controller, unless required by EU or national law. If such a legal requirement applies, the processor shall inform the controller before processing, unless prohibited on grounds of important public interest. If the processor considers that an instruction infringes applicable data protection legislation, it shall immediately notify the controller.
- Ensure that persons authorized to process personal data are bound by confidentiality obligations.
- Implement appropriate technical and organizational security measures appropriate to the risk.
- Use subprocessors only under written arrangements imposing equivalent data protection obligations.
- Assist the controller with data subject requests and compliance obligations where required.
- Assist the controller with data protection impact assessments (DPIA) pursuant to GDPR Art. 35, and with prior consultation with the supervisory authority under Art. 36, where the nature of the processing makes the processor's assistance relevant.
- Notify the controller in writing without undue delay, and no later than 24 hours after becoming aware of a personal data breach affecting controller data. The notification shall at a minimum describe: the nature of the breach, the categories and approximate number of affected data subjects and records, the likely consequences, and measures taken or proposed to address the breach. Where complete information is not available within the deadline, information may be provided in stages without further undue delay.
- Delete or return personal data at the end of the customer relationship, unless retention is required by law.

Controller obligations

- Ensure a valid legal basis exists for all personal data processed in the platform.
- Provide documented instructions for processing and remain responsible for the lawfulness of those instructions.
- Provide candidates and other data subjects with required privacy information and notices.
- Review AI-assisted outputs before taking decisions and remain responsible for final recruitment decisions.

Subprocessors

The controller provides general prior authorization for the processor to use subprocessors for infrastructure, email, hosting, analytics, and AI as listed in the processor's current subprocessor list, available in the privacy documentation at Molte.

If the processor wishes to change or add subprocessors, the controller shall be notified in writing at least 14 days in advance. The controller may object to the change within this period if there is a substantive reason related to data protection concerns. If the controller does not object within the deadline, the change is deemed approved.

All subprocessors shall be bound by written agreements imposing the same data protection obligations as those set out in this agreement. The processor is fully responsible to the controller for ensuring that its subprocessors fulfil their obligations.

Transfers and international processing

Where personal data is processed outside the EU/EEA, the processor shall rely on lawful transfer mechanisms such as Standard Contractual Clauses and any supplementary safeguards required under applicable law.

Security and audit support

The processor shall maintain documented security controls, assist the controller with reasonable audit and information requests, and document accepted DPA versions using hashes, timestamps, and PDF snapshots.

Versioning and evidence

Each accepted DPA version is stored with a stable version string, a document hash, acceptance metadata, and a PDF snapshot so the exact accepted text can be reproduced later.

Term and termination

This agreement applies for as long as the processor processes personal data on behalf of the controller in connection with the service and survives for as long as retention, return, deletion, or audit obligations remain applicable.

Governing law and jurisdiction

This agreement is governed by Norwegian law. Disputes arising in connection with this agreement that cannot be resolved amicably shall be brought before Oslo District Court as the legal venue.

Acceptance

This Data Processing Agreement is deemed entered into when the controller accepts it electronically upon establishing a customer relationship, or by written signature from both parties. Electronic acceptance is recorded with the accepting user's identity, timestamp, document hash, and a PDF snapshot.

Manual signature (alternative to electronic acceptance)

- Processor - Molte AS: Name: _____ Title: _____ Date: _____ Signature: _____
- Controller - Customer organization: Name: _____ Title: _____ Date: _____ Signature: _____

Contact

Questions relating to this DPA or privacy compliance may be sent to hello@molte.ai.