# RecruitmentAds.com Data Processing Agreement

*Standard business customer DPA*

Last updated: 22 June 2026

## Parties and application

This Data Processing Agreement (the "DPA") applies between RecruitmentAds.com, sole proprietorship of Niels Geominy, registered with the Dutch Chamber of Commerce under number 80091660, having its business address at Kantonnier 12, 6661MS Elst, the Netherlands (the "Supplier") and the customer entity identified in the applicable order form, subscription agreement, pilot agreement, statement of work, online acceptance flow or other commercial agreement for the Services (the "Customer").

The Supplier provides the RecruitmentAds.com software service, available through studio.recruitmentads.com, and related onboarding, support, content generation, rendering and export services (the "Services").

This DPA forms part of the agreement between the Supplier and the Customer governing the Services (the "Main Agreement"). If there is a conflict between this DPA and the Main Agreement regarding the processing of Customer Data, this DPA prevails.

## 1. Definitions

| Item | Details |
|---|---|
| Applicable Data Protection Law | all applicable laws and regulations relating to privacy and data protection, including the GDPR, the Dutch GDPR Implementation Act, the UK GDPR, the UK Data Protection Act 2018 and any other applicable data protection legislation. |
| Controller | the party that determines the purposes and means of the processing of Personal Data. |
| Customer Data | Personal Data and other data submitted to, uploaded to, generated through or otherwise processed through the Services by or on behalf of the Customer, including vacancy texts, brand assets, uploaded media, generated creatives and project data, to the extent such data contains Personal Data. |
| Data Breach | a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. |
| Data Subject | an identified or identifiable natural person to whom Personal Data relates. |
| GDPR | Regulation (EU) 2016/679. |
| Personal Data | any information relating to an identified or identifiable natural person. |
| Processing | any operation or set of operations performed on Personal Data, including collection, storage, use, disclosure, transmission, erasure or destruction. Process and Processed have corresponding meanings. |
| Processor | the party that processes Personal Data on behalf of a Controller. |
| Subprocessor | a third party engaged by the Supplier to process Customer Data on behalf of the Customer in connection with the Services. |
| UK GDPR | the GDPR as incorporated into the laws of the United Kingdom. |

## 2. Roles and scope

1. For Customer Data, the Customer acts as Controller and the Supplier acts as Processor, unless the Customer itself acts as Processor on behalf of a third-party Controller, in which case the Supplier acts as Subprocessor.
2. The Supplier acts as an independent Controller for Personal Data it processes for its own business purposes, including account administration, billing, sales, support, website analytics, service security, fraud prevention and legal compliance.
3. The Customer determines which vacancy texts, brand assets, images, videos, voice materials, job information or other materials are uploaded to or used in the Services.
4. The Customer remains responsible for the lawfulness, accuracy and appropriateness of Customer Data and for any instructions given to the Supplier.

5. The processing activities covered by this DPA are described in Annex 1.

## 3. Processing instructions

6. The Supplier shall process Customer Data only on documented instructions from the Customer, including instructions given through the Main Agreement, this DPA, the Services, user settings, feature selections, support requests and other written instructions.
7. The Supplier shall inform the Customer if, in the Supplier's opinion, an instruction infringes Applicable Data Protection Law, unless the Supplier is prohibited by law from doing so.
8. The Supplier may process Customer Data where required by law to which the Supplier is subject. In such case, the Supplier shall inform the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.
9. The Supplier shall not sell Customer Data.
10. The Supplier shall not use Customer Data to train its own AI models.
11. Where Customer Data is processed by external AI providers, the Supplier shall use business or paid API configurations where available and shall configure provider settings in a manner intended to prevent Customer Data from being used for third-party model training where such controls are supported by the provider.

## 4. Confidentiality and access

12. The Supplier shall limit access to Customer Data to authorised persons who require access for the purpose of providing, securing, maintaining, improving or supporting the Services.
13. Internal administrative access is used for support, maintenance, troubleshooting, security and operational purposes only.
14. Customer workspaces are logically separated. Customers do not have access to other customers' Customer Data.
15. Where personnel or contractors are engaged by the Supplier, appropriate confidentiality obligations will be applied.

## 5. Security measures

16. The Supplier shall implement and maintain appropriate technical and organisational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
17. The technical and organisational measures in place as of the effective date of this DPA are described in Annex 2.
18. The Supplier may update its technical and organisational measures from time to time, provided that such updates do not materially reduce the overall level of protection for Customer Data.
19. The Customer is responsible for securely managing its own user accounts, credentials, access rights, exported files and publication of generated output outside the Services.

## 6. Subprocessors

20. The Customer grants the Supplier general written authorisation to engage Subprocessors for the processing of Customer Data in connection with the Services.
21. The Supplier shall maintain a current Subprocessor List and make it available to the Customer. The Subprocessor List may be provided as a separate document or webpage.
22. The Supplier shall impose data protection obligations on each Subprocessor that are no less protective in substance than those set out in this DPA, to the extent applicable to the nature of the services provided by that Subprocessor.
23. The Supplier remains responsible to the Customer for the performance of Subprocessors that process Customer Data on behalf of the Supplier.

24. The Supplier shall inform the Customer of intended material changes concerning the addition or replacement of Subprocessors by making an updated Subprocessor List available or by providing notice through email, account notification or another reasonable method.
25. The Customer may object to a new Subprocessor on reasonable data protection grounds within fifteen (15) calendar days of receiving notice. The Parties shall work in good faith to resolve the objection. If the objection cannot be resolved, the Customer may terminate the affected Services unless the Parties agree on another commercially reasonable solution.
26. Third-party platforms to which the Customer independently uploads or publishes exported content, such as LinkedIn, Meta, TikTok, YouTube, job boards, websites or ATS systems, are not Subprocessors of the Supplier unless the Supplier directly processes Customer Data through those platforms on behalf of the Customer.

## 7. International transfers

27. The Supplier uses EU-based infrastructure for its primary platform storage, including AWS eu-west-1 for media and renders, Supabase EU in Frankfurt for authentication and database services, and an EU-based RunCloud-managed VPS for templates and metadata.
28. Certain features may involve processing by Subprocessors or underlying model providers located outside the EEA, the United Kingdom or another jurisdiction recognised as adequate under Applicable Data Protection Law.
29. Where Customer Data is transferred outside the EEA, the United Kingdom or another adequate jurisdiction, the Supplier shall ensure that an appropriate transfer mechanism is in place, such as an adequacy decision, the European Commission Standard Contractual Clauses, the UK International Data Transfer Addendum, the UK International Data Transfer Agreement or another valid transfer mechanism under Applicable Data Protection Law.
30. The Customer authorises the Supplier to enter into appropriate transfer mechanisms with Subprocessors where necessary for the provision of the Services.

## 8. Data Subject rights

31. Taking into account the nature of the processing and the information available to the Supplier, the Supplier shall assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law.
32. If the Supplier receives a request directly from a Data Subject relating to Customer Data, the Supplier shall, where reasonably identifiable as relating to the Customer, forward the request to the Customer or instruct the Data Subject to contact the Customer directly, unless the Supplier is legally required to respond.
33. The Supplier shall not respond substantively to such requests without the Customer's prior written instruction unless required by law.

## 9. Assistance with security, DPIAs and authorities

34. Taking into account the nature of the processing and the information available to the Supplier, the Supplier shall assist the Customer with obligations relating to security of processing, Data Breach notifications, communication of Data Breaches to Data Subjects, data protection impact assessments and prior consultation with supervisory authorities.
35. The Supplier may charge reasonable costs for assistance that goes beyond standard support or requires significant additional work, unless the assistance is required due to the Supplier's breach of this DPA.

## 10. Data Breach notification

36. The Supplier shall notify the Customer without undue delay after becoming aware of a Data Breach affecting Customer Data.

37. The notification shall include, to the extent available, the nature of the Data Breach, the categories and approximate number of Data Subjects concerned, the categories and approximate number of Personal Data records concerned, likely consequences, measures taken or proposed to address the breach, and a contact point for further information.
38. Where information is not available at the time of initial notification, the Supplier shall provide further information in phases without undue further delay.
39. The Supplier shall document Data Breaches affecting Customer Data, including the facts relating to the breach, its effects and remedial action taken.
40. The Supplier shall not notify supervisory authorities or affected Data Subjects on behalf of the Customer unless required by law or instructed by the Customer.

## 11. Deletion and return

41. During the term of the Main Agreement, the Customer may delete certain Customer Data through the functionality of the Services where such functionality is available.
42. Where the Customer deletes Customer Data from the active workspace, the Supplier shall delete or make unavailable such Customer Data from active systems without undue delay and in any event within thirty (30) days, subject to backup rotation, security logs, legal retention obligations and technical limitations.
43. Upon termination or expiry of the Main Agreement, the Customer may export Customer Data for thirty (30) days where export functionality is available.
44. After the export period, or earlier upon the Customer's written instruction, the Supplier shall delete Customer Data from active systems within thirty (30) days unless applicable law requires continued storage.
45. Customer Data stored in backups or logs may remain for up to ninety (90) days and will be deleted through normal backup and log rotation.
46. The Supplier may retain Personal Data to the extent required for legal, accounting, tax, security, fraud prevention or dispute resolution purposes, provided that such data is processed only for such purposes and remains protected.
47. The Customer remains responsible for deleting copies of exported or published content outside the Services, including content downloaded by the Customer or uploaded to third-party platforms.

## 12. Audit and information rights

48. The Supplier shall make available to the Customer information reasonably necessary to demonstrate compliance with Article 28 GDPR, Article 28 UK GDPR where applicable, and this DPA.
49. The Customer may request an audit no more than once per calendar year, unless required by a supervisory authority or following a Data Breach affecting Customer Data.
50. The Customer shall provide at least thirty (30) calendar days' prior written notice of an audit, unless shorter notice is required by a supervisory authority or reasonably necessary following a Data Breach.
51. Audits shall be conducted during normal business hours, with minimal disruption to the Supplier's business, systems and other customers.
52. The Supplier may satisfy an audit request by providing relevant documentation, security information, policies, questionnaires or written responses, unless the Customer can demonstrate a specific and reasonable need for further inspection.
53. The Customer shall ensure that any auditor is bound by confidentiality obligations acceptable to the Supplier.

## 13. Customer responsibilities

54. The Customer is responsible for determining the lawful basis for processing Customer Data, providing privacy notices to Data Subjects where required, obtaining consents, permissions, licences or internal approvals where required, and ensuring that Customer Data uploaded to the Services is lawful, accurate and appropriate.

55. Where the Customer uploads images, videos, voice recordings, names, likenesses or other materials involving identifiable individuals, the Customer represents that it has the necessary rights, permissions and lawful basis to use those materials in the Services and in the intended recruitment marketing output.
56. Where the Customer uses AI-assisted editing, image generation, image-to-video generation, video generation, voice generation or similar features, the Customer is responsible for ensuring that use of such features is permitted under its internal policies and applicable law.
57. The Customer shall not upload special categories of Personal Data, criminal offence data or highly sensitive personal data unless this has been expressly agreed with the Supplier in writing and appropriate safeguards have been put in place.
58. The Customer is responsible for reviewing generated output before publication and for use, publication or distribution of exported content outside the Services.

## 14. AI features and customer materials

59. The Services may include features that use AI providers for text processing, image analysis, image generation, video generation, voice generation, translation, prompt generation, quality control and related functionality.
60. Not every feature uses external AI processing. Storing media in a customer workspace or rendering customer-provided media into a template does not necessarily require sending that media to an external AI model.
61. External AI processing is used where required for the selected feature, such as text generation, image analysis, AI image editing, image generation, image-to-video generation, voice generation or translation.
62. The Supplier shall not reuse Customer Data, uploaded assets or generated output for other customers.
63. The Supplier shall not use Customer Data, uploaded assets or generated output in public marketing, case studies or examples without the Customer's prior permission.
64. The Supplier shall not use Customer Data to train its own AI models.
65. For certain AI video workflows using fal.ai, input and output payloads may be retained by fal.ai under its default payload retention settings, currently expected to be up to approximately thirty (30) days, unless storage is disabled or deletion controls are applied.

## 15. Intellectual property and output

66. As between the Parties, the Customer retains all rights, title and interest in Customer Data, including Customer-provided vacancy texts, images, videos, brand assets and other input materials.
67. As between the Parties, and subject to payment of applicable fees and compliance with the Main Agreement, the Customer may use the output generated through the Services for its own recruitment marketing and employer branding purposes.
68. The Supplier does not claim ownership of Customer-provided input materials.
69. The Supplier may use aggregated, anonymised or statistical information derived from use of the Services for analytics, service improvement, security, operational and business purposes, provided that such information does not identify the Customer, Customer users or Data Subjects.
70. Nothing in this DPA assigns ownership of the Supplier's platform, software, templates, workflows, know-how, pre-existing intellectual property, design systems, code, AI orchestration logic or other proprietary technology to the Customer.

## 16. Liability

71. Each Party shall be liable for damages caused by processing that infringes Applicable Data Protection Law where it is responsible for the event giving rise to the damage.

72. The Supplier shall be liable for damage caused by processing where it has not complied with obligations specifically directed to Processors under Applicable Data Protection Law or where it has acted outside or contrary to the lawful documented instructions of the Customer.
73. The Customer shall be liable for damage caused by processing where the Customer has not complied with obligations applicable to Controllers or where the Customer's instructions, uploaded data, publication decisions or use of the Services cause the damage.
74. The Supplier's aggregate liability under or in connection with this DPA shall be subject to the limitations of liability in the Main Agreement. Where no limitation is specified in the Main Agreement, the Supplier's aggregate liability shall not exceed the fees paid by the Customer for the Services in the six (6) months preceding the event giving rise to liability, except to the extent liability cannot be limited under applicable law.

## 17. Term and termination

75. This DPA becomes effective on the date the Main Agreement becomes effective or the date on which the Supplier first processes Customer Data on behalf of the Customer, whichever occurs first.
76. This DPA remains in effect for as long as the Supplier processes Customer Data on behalf of the Customer.
77. Termination or expiry of the Main Agreement shall automatically terminate this DPA, except for obligations that by their nature should survive termination, including confidentiality, deletion, audit cooperation, liability and provisions relating to retained data.

## 18. Governing law and jurisdiction

78. This DPA is governed by the laws of the Netherlands, unless mandatory Applicable Data Protection Law requires otherwise.
79. Any dispute arising out of or in connection with this DPA shall be submitted to the competent courts of the Netherlands, unless mandatory law requires otherwise.
80. Where Standard Contractual Clauses or UK transfer terms apply, the governing law and jurisdiction for those clauses shall be determined in accordance with the relevant clauses and applicable transfer mechanism.

## 19. General provisions

81. If any provision of this DPA is invalid or unenforceable, the remaining provisions shall remain in effect. The Parties shall replace the invalid or unenforceable provision with a valid provision that most closely reflects the original intention.
82. Amendments to this DPA must be made in writing, except that the Supplier may update the technical and organisational measures, Subprocessor List and feature-based processing descriptions in accordance with this DPA, provided that such updates do not materially reduce the protection of Customer Data.
83. In the event of conflict between this DPA and the Main Agreement, this DPA prevails with respect to the processing of Customer Data.

## Signature

This DPA may be signed by the Parties or incorporated by reference into the Main Agreement, order form, pilot agreement, statement of work or online subscription terms.

| Customer | Supplier |
|---|---|
| Name: | Name: Niels Geominy |
| Title: | Title: Owner |
| Signature and date: | Signature and date: |

# Annex 1 - Description of processing

| Item | Details |
|---|---|
| Subject matter | Provision of the RecruitmentAds.com software service, available through studio.recruitmentads.com, and related onboarding, support, generation, rendering and export services. |
| Duration | The term of the Main Agreement, plus any period required for deletion, export, backup rotation, legal retention, security, accounting or dispute resolution purposes. |
| Nature of processing | Collection, receipt, upload, hosting, storage, structuring, analysis, generation, editing, rendering, export, retrieval, deletion, support, troubleshooting, logging and security monitoring. |
| Purpose of processing | Creating, editing, generating, rendering and exporting recruitment marketing videos, static creatives, social media assets, scripts, captions, translations and related recruitment marketing content. |
| Frequency | Continuous for the duration of the Main Agreement, depending on Customer use of the Services. |
| Supplier contact | privacy@recruitmentads.com for privacy matters, support@recruitmentads.com for support matters. |

## Categories of Data Subjects

- Customer employees, recruiters, HR users, marketing users and administrators.
- Job candidates, applicants, students, interns and other people included in Customer Data.
- Employees, clients, residents, patients or other individuals appearing in customer-provided media, if uploaded by the Customer.

## Categories of Personal Data

- Names, business contact details and user account data.
- Vacancy texts, job titles, employer information and written instructions.
- Brand guidelines, logos, colours, fonts, images, videos and other creative assets.
- Likenesses, faces or voices included in uploaded media where the Customer chooses to upload such materials.
- Generated text, images, videos, audio, scripts, captions, translations, project metadata, usage data and technical logs.

## Special categories of Personal Data

The Services are not intended for the processing of special categories of Personal Data or criminal offence data. The Customer shall not upload such data unless agreed with the Supplier in writing and appropriate safeguards have been put in place. Materials uploaded by the Customer may incidentally reveal sensitive attributes, and the Customer is responsible for ensuring that such processing is lawful.

## Retention period

Customer Data is retained during the term of the Main Agreement or until deleted by the Customer, subject to deletion from active systems within thirty (30) days, a thirty (30) day export period after termination where

applicable, backup and log rotation of up to ninety (90) days, legal retention obligations, security needs and provider-specific retention described in the Subprocessor List.

# Annex 2 - Technical and organisational measures

## Hosting and infrastructure

- AWS eu-west-1 for media and renders.
- Supabase EU, Frankfurt eu-central-1, for authentication and database services.
- EU-based RunCloud-managed VPS for templates, metadata and the job-agent app.
- Cloudflare for DNS, CDN, network security and performance.

## Transmission security

- Use of HTTPS/TLS for transmission of data between users and the platform.
- Secure communication between platform services where technically appropriate.

## Access control

- No customer cross-access. Customer workspaces are logically separated.
- Internal administrative access is limited to support, maintenance, troubleshooting, security and operational purposes.
- Customer MFA is available but not mandatory.

## Data minimisation

- The Customer controls which materials are uploaded and which features are used.
- External AI processing is used only where required by the selected feature.
- Storing or rendering customer-provided media does not necessarily require external AI model processing.

## Logging, backups and deletion

- Technical logs and backups may be retained for up to ninety (90) days.
- Deleted Customer Data is deleted or made unavailable from active systems without undue delay and in any event within thirty (30) days, subject to backup rotation and legal retention obligations.

## Incident response

- The Supplier maintains procedures to identify, assess, contain and respond to suspected security incidents.
- The Customer is notified of Data Breaches affecting Customer Data without undue delay.

## Subprocessor management

- Subprocessors are used for infrastructure, authentication, email, payments, AI processing and other feature-specific purposes.
- The Supplier maintains a Subprocessor List and applies contractual or service terms with Subprocessors where they process Customer Data on behalf of the Supplier.

## Limitations

- The Supplier does not currently maintain ISO 27001 or SOC 2 certification.
- No broad employee NDA programme is currently claimed. Where personnel or contractors are engaged, appropriate confidentiality obligations will be applied.

# Annex 3 - Retention schedule

| Data category | Default retention |
|---|---|
| Account admin data | During the Main Agreement and thereafter as needed for legal, accounting, security or business administration purposes. |
| Vacancy text and project data | During the Main Agreement or until deleted by the Customer. |
| Uploaded brand assets | During the Main Agreement or until deleted by the Customer. |
| Uploaded images and videos | During the Main Agreement or until deleted by the Customer. |
| Generated images, videos, audio and creatives | During the Main Agreement or until deleted by the Customer. |
| After termination | Customer may export Customer Data for thirty (30) days where export functionality is available. Active-system deletion follows within thirty (30) days after the export period or earlier instruction. |
| Technical logs and backups | Up to ninety (90) days, unless longer retention is required for security, legal or operational reasons. |
| Billing and accounting records | Retained for the legally required period. |
| AI provider processing data | Subject to the applicable provider terms and feature-specific settings, as described in the Subprocessor List. |