Data Processing Agreement

Caliber Global Limited (NZBN 9429051112615), Auckland, New Zealand

Party details

	Caliber (Provider)	Customer
Legal name	Caliber Global Limited	_____
Company number	NZBN 9429051112615	_____
Address	Auckland, New Zealand	_____
Contact for notices	support@caliberjobs.com	_____

What this document is. This Data Processing Agreement sets out how Caliber handles personal information on your behalf when you use, test, or evaluate the Caliber product. It covers what we may do with your data, how we protect it, who else touches it, what happens when something goes wrong, and how you get your data back or have it deleted. It applies whether or not you have a paid subscription yet, so it can be signed before a migration or sync test begins. This box is a plain-English summary only and does not form part of the operative terms.

1. Definitions and interpretation

1.1 In this Data Processing Agreement (this **"DPA"**):

"Agreement" means the Caliber Terms of Service available at caliberjobs.com/terms (the **"Terms"**) together with any **Order** (an order form, online sign-up, or other document setting out Customer's subscription). During any Pre-Contract Period, "Agreement" means this DPA together with any non-disclosure or confidentiality agreement in force between the parties (the **"NDA"**).

"Caliber" and **"Customer"** mean the parties identified in the party details table above.

"Customer Data" means information Customer or its users upload to, or generate inside, the Service, or provide to Caliber for migration, import, sync testing, or evaluation, including candidate and contact records, CVs, notes, messages, pipeline data, and files. Once an Order is in effect, "Customer Data" has the meaning given in the Terms and includes data provided during any Pre-Contract Period.

"Customer Personal Information" means personal information contained in Customer Data, that is, information about an identifiable individual that Customer or its users provide to, or generate inside, the Service, or provide to Caliber for migration, import, sync testing, or evaluation. It includes the categories described in Annex 1.

"Notifiable Privacy Breach" means a Privacy Breach that is notifiable under applicable Privacy Laws (for the Privacy Act, a privacy breach that it is reasonable to believe has caused, or is likely to cause, serious harm to an affected individual).

"Pre-Contract Period" means any period during which Caliber processes Customer Personal Information before an Order is in effect, including for migration, import, sync testing, or evaluation under clause 3.

"Privacy Breach" means unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, Customer Personal Information, or an action that prevents access to it (within the meaning of section 112 of the Privacy Act), and includes a personal data breach under the GDPR or UK GDPR.

"Privacy Laws" means the New Zealand Privacy Act 2020 (the **"Privacy Act"**), including its Information Privacy Principles (**"IPPs"**), and, to the extent applicable to the processing in question, the Australian Privacy Act 1988, the United Kingdom General Data Protection Regulation (the **"UK GDPR"**), Regulation (EU) 2016/679 (the **"GDPR"**), and any other privacy or data protection law that applies to a party.

"Service" means the Caliber product, including the ATS, CRM, Chat, Scout, the built-in phone system, contact enrichment, and document signing.

"Sub-processor" means a third party engaged by Caliber to process Customer Personal Information on Caliber's behalf.

1.2 **Roles and vocabulary.** For Customer Personal Information, Customer is the **controller** (under the Privacy Act, the agency that collected and holds the information) and Caliber is the **processor** (under the Privacy Act, an agent processing information on Customer's behalf). Under section 11 of the Privacy Act, information Caliber holds solely as Customer's agent is treated as held by Customer, and Customer remains responsible for it under the IPPs. This DPA is intended to satisfy the requirements of Article 28(3) of the GDPR and UK GDPR where those regimes apply. "Processing", "data subject", and similar terms have the meanings given in applicable Privacy Laws.

1.3 **Precedence.** If this DPA conflicts with the Terms, this DPA prevails for the subject matter of the conflict. An Order prevails over this DPA only where the conflicting term expressly refers to this DPA and is agreed in a writing signed by both parties; standard online sign-up terms do not override this DPA. This otherwise matches the order of precedence stated in the Terms: Order, then DPA, then Terms.

2. Scope and duration

2.1 This DPA applies to all processing of Customer Personal Information by Caliber on Customer's behalf, whether during a subscription under an Order or during a Pre-Contract Period.

2.2 This DPA takes effect on the Effective Date stated above the signature blocks (or, if none is stated, the date of last signature) and continues for as long as Caliber processes Customer Personal Information.

2.3 If the parties later enter an Order, this DPA automatically forms part of the Agreement for that Order without needing to be re-signed, and continues to govern all Customer Personal Information, including data provided during the Pre-Contract Period.

3. Pre-contract migration, testing, and evaluation

3.1 The parties may agree that Caliber will process Customer Personal Information before any Order is in effect, for example to migrate or import data from Customer's existing systems, to run sync tests against a

source system, or to let Customer evaluate the Service using its own data. All such processing is covered by this DPA and, where in force, the NDA.

3.2 During a Pre-Contract Period, Caliber will:

(a) except for interim migration copies handled under clause 3.2(d), hold Customer Personal Information in the same production environment used for subscriber data (described in clause 8.1 and Annex 3), and apply the same technical and organisational measures set out in Annex 2;

(b) limit access to those Caliber personnel who need it to perform the migration, testing, or evaluation, in accordance with clause 5;

(c) process the data only as needed for the agreed migration, import, sync testing, or evaluation, and for no other purpose;

(d) accept migration source files (for example, a CSV export from Customer's existing CRM) only through a secure, access-controlled transfer channel nominated or approved by Caliber; hold any interim copies in encrypted, company-managed storage (never on personal devices), accessible only to the personnel performing the migration; and delete those interim copies within 14 days of a confirmed import, or within 14 days of the migration being abandoned or the Pre-Contract Period ending, whichever comes first. Where migration or sync runs through a direct connection to Customer's source system instead, no source files change hands: the connection runs over TLS, is authorised by Customer through the source system's own sign-in, can be revoked by Customer there at any time, and is used only for the agreed migration, import, or sync activities (including any write-back Customer enables, such as AI call summaries saved to Customer's own CRM).

3.3 If the parties do not enter an Order, Caliber will delete Customer Personal Information provided during the Pre-Contract Period from its production systems:

(a) within 30 days of Customer's written request; and

(b) in any event, no later than 6 months after the agreed migration, testing, or evaluation activities end (or a later date the parties agree in writing),

whichever comes first, and from backups on a rolling basis within a further 6 months. Backup copies are not restored to production except for disaster recovery and remain protected under this DPA until deleted. Residual log and trace data expires as described in clause 12.2. Before deletion is completed, Customer may request a full export of the Customer Personal Information provided during the Pre-Contract Period in a commonly used machine-readable format, and Caliber will provide it within 14 days at no charge. These obligations apply except to the extent Caliber is required by law to retain the information. On request, Caliber will confirm deletion in writing.

3.4 If the parties do enter an Order, data provided during the Pre-Contract Period becomes Customer Data under the Agreement and the retention and deletion terms in clause 12 apply instead of clause 3.3.

4. Processing on instructions

4.1 Caliber will process Customer Personal Information only on Customer's documented instructions. Customer's instructions are: the Agreement (including this DPA), the settings and features Customer configures or uses in the Service, and any other written instructions Customer gives that are consistent with

the Agreement. Migration, import, sync testing, and evaluation activities the parties agree in writing (including by email) are documented instructions.

4.2 Caliber may process Customer Personal Information other than on Customer's instructions only where required by law. In that case Caliber will inform Customer of the legal requirement before processing, unless the law prohibits it.

4.3 If Caliber considers that an instruction breaches, or is likely to breach, Privacy Laws, Caliber will inform Customer immediately (and in any event without undue delay) and may pause the affected processing until the instruction is confirmed or changed. Caliber is not obliged to conduct a legal review of Customer's instructions.

4.4 Customer is responsible for the lawfulness of the Customer Personal Information it provides, including having the right (and, where required, the authorisation of individuals) to disclose it to Caliber for processing under this DPA.

5. Personnel

5.1 Caliber will ensure that every person it authorises to process Customer Personal Information is bound by a contractual or statutory duty of confidentiality, and that access is limited to personnel who need it to perform Caliber's obligations.

6. Security

6.1 Caliber will implement and maintain the technical and organisational measures set out in Annex 2, and will not materially reduce the overall level of protection during the term of this DPA. Caliber may update the measures as technology and threats evolve, provided the updated measures provide at least an equivalent level of protection.

6.2 Annex 2 states Caliber's current certification status plainly, and Customer acknowledges that status. The measures in Annex 2 are the agreed contractual standard of security for the purposes of this DPA. Nothing in this clause limits or determines either party's obligations under applicable Privacy Laws, including IPP 5 of the Privacy Act and Article 32 of the GDPR.

7. Sub-processors

7.1 **General authorisation.** Customer authorises Caliber to engage the Sub-processors listed in Annex 3, and to engage new or replacement Sub-processors under this clause 7. Caliber remains responsible to Customer for each Sub-processor's performance.

7.2 **Flow-down.** Caliber will impose on each Sub-processor written data protection obligations that are materially equivalent to those in this DPA, to the extent relevant to the services the Sub-processor performs.

7.3 **Notice of changes.** Caliber will give Customer at least 30 days' written notice before a new Sub-processor begins processing Customer Personal Information, and will update Annex 3 to reflect any change that takes effect under this clause 7.

7.4 **Objection.** Customer may object to a new Sub-processor within the notice period on reasonable data protection grounds. The parties will then discuss the objection in good faith, including whether the affected processing can be configured to avoid the new Sub-processor. If no resolution is reached within 30 days of the

objection, Customer may terminate the affected processing (or, where the Sub-processor is integral to the Service, its subscription) on written notice, and Caliber will refund any pre-paid fees for the unused period.

8. Cross-border transfers

8.1 Caliber is a New Zealand company. The Service's backend systems, databases, and file storage are hosted on Amazon Web Services in the United States (us-east-1), and the web application frontend is served by Render, also in the United States. Most of Caliber's Sub-processors operate in the United States, as set out in Annex 3. Customer Personal Information will therefore be stored and processed outside New Zealand, principally in the United States.

8.2 Caliber's Sub-processors hold Customer Personal Information solely as agents for processing. Under section 11 of the Privacy Act the information remains held by Customer, so engaging an overseas Sub-processor is not a disclosure governed by IPP 12. As part of its security safeguards under IPP 5, Caliber's agreements with overseas Sub-processors include data protection terms addressing cross-border transfers, including standard contractual clauses or equivalent frameworks where appropriate. Where the GDPR or UK GDPR applies to a transfer, Caliber will ensure a valid transfer mechanism is in place.

8.3 Details of the mechanism relied on for a specific Sub-processor are available on written request to support@caliberjobs.com.

8.4 Customer authorises, and this DPA constitutes Customer's documented instruction for, the transfers of Customer Personal Information described in this clause 8 and Annex 3, subject to Caliber's compliance with this clause 8.

9. Assistance with individuals' requests

9.1 If an individual contacts Caliber directly about personal information that Caliber processes on Customer's behalf (for example, an access or correction request under IPP 6 or IPP 7 of the Privacy Act, or a rights request under the GDPR or UK GDPR), Caliber will not respond substantively except to direct the individual to Customer, unless required by law.

9.2 Taking into account the nature of the processing, Caliber will provide reasonable assistance to help Customer respond to such requests, including retrieving, exporting, correcting, or deleting specific records where Customer cannot fully self-serve in the product. Caliber will act on such assistance requests promptly, recognising Customer's statutory deadlines.

9.3 Assistance under this clause 9 is included in the Service, except that Customer will bear Caliber's reasonable costs of assistance with requests that are manifestly excessive or unusually voluminous, agreed in advance where practicable.

9.4 Caliber will also provide reasonable assistance with Customer's privacy impact assessments and consultations with regulators, to the extent they relate to the processing under this DPA and the information is available to Caliber.

10. Privacy breach notification

10.1 If Caliber becomes aware of a Privacy Breach, Caliber will notify Customer without undue delay, and in any event within 72 hours of becoming aware. As between the parties, Customer determines whether the

breach is a Notifiable Privacy Breach (including the serious-harm assessment under the Privacy Act), and Caliber will provide the information Customer reasonably needs to make that assessment.

10.2 The notification will include, to the extent then known: the nature of the breach, the categories and approximate number of individuals and records affected, the likely consequences, the measures taken or proposed to address the breach and mitigate harm, and a contact point at Caliber. Caliber may provide information in phases as the investigation progresses.

10.3 Caliber will take reasonable steps to contain and remediate the breach, and will provide reasonable assistance to Customer in meeting Customer's own notification obligations to the Office of the Privacy Commissioner, other regulators, and affected individuals.

10.4 As between the parties, Customer decides whether and how to notify regulators and individuals about a breach affecting Customer Personal Information. Caliber will not make such notifications on Customer's behalf unless the parties agree in writing or Caliber is required to do so by law.

11. No use for AI training

11.1 Caliber will not use Customer Personal Information or Customer Data to train public or third-party foundation AI models, and Caliber's agreements with the AI Sub-processors it engages (for example, OpenAI) contractually prohibit them from doing so. Zoom's call transcription runs in Customer's own Zoom account and is governed by Customer's own agreement with Zoom (see Annex 3). AI features in the Service operate on Customer's data only to return outputs to Customer's users and to systems Customer connects, as described in Annex 1.

12. Return and deletion

12.1 During the subscription term and for 30 days after it ends, Customer may request a full export of Customer Data in a commonly used machine-readable format, prepared and delivered by Caliber's support team within 14 days of the request.

12.2 After that 30-day window (and completion of any export requested within it), Caliber will delete Customer Personal Information from its production systems within 90 days, and from backups on a rolling basis within a further 6 months. Log and trace data containing Customer Personal Information expires on the 365-day retention schedule stated in Annex 3, or earlier on written request where reasonably practicable, and remains protected under this DPA until deleted.

12.3 Caliber may retain Customer Personal Information to the extent required by applicable law (for example, tax and accounting records), and will continue to protect it under this DPA and delete it when the legal requirement ends.

12.4 On written request, Caliber will confirm in writing that deletion under this clause 12 (or clause 3.3) has been completed.

13. Audit and information rights

13.1 On written request no more than once in any 12-month period, Caliber will respond to Customer's reasonable written security questionnaires, provide available documentation describing its technical and

organisational measures, and make available the further information reasonably necessary to demonstrate compliance with this DPA, within a reasonable period.

13.2 An on-site or remote audit of Caliber's processing is available: (a) where a regulator with authority over Customer requires it; (b) following a Notifiable Privacy Breach affecting Customer Personal Information; or (c) where the information provided under clause 13.1 is reasonably insufficient to demonstrate Caliber's compliance with this DPA, in which case Customer may audit no more than once in any 12-month period. Any such audit will be at Customer's cost, on at least 30 days' written notice, during business hours, subject to Caliber's confidentiality and security requirements, and must not give Customer or its auditor access to any other customer's data.

13.3 This clause 13 is the parties' agreed mechanism for the audit and inspection rights contemplated by Article 28(3)(h) of the GDPR and UK GDPR.

14. Liability

14.1 Each party's liability arising out of or in connection with this DPA is subject to the exclusions and limitations of liability in the Agreement, except that: (a) any exclusion of liability for loss or corruption of data in the Agreement does not apply to Customer Personal Information lost or corrupted as a result of Caliber's breach of this DPA; and (b) Customer's reasonable costs of investigating, notifying, and remediating a Privacy Breach caused by Caliber's breach of this DPA are treated as direct losses. Liability under this clause 14.1 remains subject to the applicable liability cap.

14.2 For processing during a Pre-Contract Period (when no Order-based fee cap exists), each party's total aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), or otherwise, will not exceed NZD 100,000. This cap does not apply to liability that cannot be limited or excluded under applicable law, or to fraud or wilful misconduct.

15. General

15.1 **Governing law.** This DPA is governed by the laws of New Zealand, and the parties submit to the exclusive jurisdiction of the New Zealand courts.

15.2 **Notices.** Notices under this DPA go to the contacts in the party details table, by email, and are treated as given when sent, provided no bounce is received.

15.3 **Variation.** This DPA can be varied only in writing signed by both parties, except that changes to the Sub-processors listed in Annex 3 take effect as provided in clause 7. No update to the Terms reduces Caliber's obligations, or Customer's rights or remedies, under this DPA; for clause 14.1, the exclusions and limitations applied are those in the Terms as at the effective date of the applicable Order.

15.4 **Severability.** If any part of this DPA is held unenforceable, the rest remains in effect.

15.5 **Counterparts.** This DPA may be signed in counterparts, including electronically, each of which is an original.

15.6 **No third-party rights.** This DPA does not confer a benefit on, and is not enforceable by, anyone other than the parties. Subpart 1 of Part 2 of the Contract and Commercial Law Act 2017 does not apply to this DPA.

Signatures

Effective Date: _____ (if left blank, the date of last signature; see clause 2.2)

Signed for and on behalf of Caliber Global Limited

Signature	_____
Name	_____
Title	_____
Date	_____

Signed for and on behalf of the Customer

Signature	_____
Name	_____
Title	_____
Date	_____

Annex 1: Processing details

Subject matter. Customer Personal Information provided to, or generated in, the Service, including data provided for pre-contract migration, import, sync testing, or evaluation.

Duration. The term of this DPA under clause 2.2, including any Pre-Contract Period, until deletion under clause 3.3 or clause 12.

Nature and purpose of processing. Hosting, storage, transmission, display, backup, and retrieval of Customer Personal Information to provide the Service; migration and import of data from Customer's existing systems; sync testing against source systems; search, matching, and pipeline management operated by Customer's users; contact-detail enrichment run by Customer's users; email, chat, and phone communications initiated by Customer's users; document signing initiated by Customer's users; AI features (for example, record summarisation, and automatic transcription and summarisation of calls and meetings Customer's users choose to record), as operated on Customer's instruction; writing AI call summaries back to source systems Customer connects (for example, Customer's own CRM); support and troubleshooting; deletion and export.

Categories of data subjects. Candidates; client and company contacts; referees; Customer's own users and staff.

Categories of personal information. Identity and contact details; CVs, work history, and qualifications; notes and communications (including emails and chat messages); files and attachments; pipeline, tag, and activity data; call and meeting recordings, transcripts, AI summaries, call metadata, and voicemail data where Customer uses the built-in phone or recording features.

Special or sensitive categories. Recruitment data may incidentally include sensitive information (for example, information about health, ethnicity, or union membership appearing in a CV or note). Customer instructs Caliber to process such information only as needed to provide the Service and only to the extent Customer's collection and use of it is lawful. The Service is not designed for the systematic processing of special-category data.

Annex 2: Technical and organisational measures

Caliber maintains the following measures for the production environment that hosts Customer Personal Information (including during any Pre-Contract Period):

1. **Encryption in transit.** Data in transit between the user's browser or device and the Service is encrypted using TLS.

2. **Encryption at rest.** Databases and file storage are encrypted at rest with AWS-managed encryption (database-level and S3 server-side encryption); integration credentials such as OAuth tokens are additionally encrypted at the application level.

3. **Tenant separation.** Customer data is segregated by workspace within the application, and user access is scoped to the customer's own workspace. Pre-contract migration and test data is loaded into a workspace created for that customer alone.

4. **Access control.** Role-based access controls within the Service. Caliber staff access to customer data is limited to what is needed to operate and support the Service.

5. **Authentication.** Password-based sign-in with individual named user accounts; shared logins are not permitted.

6. **Logging and monitoring.** Application-level request logging and tracing (retained for 365 days) used to operate, debug, and investigate incidents. A customer-facing audit log is on the product roadmap.

7. **Vulnerability management.** Application dependencies and infrastructure are kept up to date as part of active, ongoing development.

8. **Backups and recovery.** Production data is backed up regularly; backups are retained and deleted on the rolling schedules in clause 12.2 (or clause 3.3 during a Pre-Contract Period) and are used to restore availability and access to Customer Personal Information after an incident.

9. **Migration handling.** Migration source files are accepted only through a secure, access-controlled transfer channel; interim copies are held encrypted in company-managed storage, restricted to the personnel performing the migration, and deleted within 14 days of a confirmed import or of the migration ending (see clause 3.2(d)).

10. **Incident response.** Privacy breach notification procedures aligned with the NZ Privacy Act 2020 and, where applicable, the GDPR, as set out in clause 10.

11. **Review.** Caliber reviews these measures periodically and after any significant incident or change to the Service.

Certification status. Caliber is not currently SOC 2 or ISO 27001 certified. Formal certification is on the roadmap. Caliber will update the Security section of its published Privacy Policy when an audit is in progress or complete.

Annex 3: Approved Sub-processors

Each Sub-processor receives only the Customer Personal Information described below, and several receive nothing unless Customer uses the feature they power:

Sub-processor	What it receives, and when	Location
Amazon Web Services, Inc.	Hosts the Service's backend, databases, and file storage, and delivers transactional email. Acts solely as Caliber's infrastructure provider.	United States (us-east-1, Northern Virginia)
Render Services, Inc.	Serves the web application frontend. Customer data passes through it, encrypted in transit, whenever the app is used; databases and file storage remain in AWS.	United States
People Data Labs, Inc.	Supplies the licensed public-profile index behind Scout search. Receives only the search query when a user runs a search; profile data flows from the index into Caliber, and Customer workspace data is never added to it.	United States
FullEnrich	Finds work contact details (phone numbers and email addresses) when a user runs enrichment on a candidate. Receives the candidate's name, LinkedIn URL, and company for that lookup only, and queries its own network of data providers to find matches. Enrichment is optional; nothing is sent unless a user chooses to run it.	France

Sub-processor	What it receives, and when	Location
Vonq B.V.	Distributes job ads Customer chooses to publish to third-party job boards, and returns the applications boards send back; applicant details (name, CV, contact information) pass through Vonq on their way into Caliber.	Netherlands
Google LLC	Email sync where a user connects a Gmail inbox (the mailbox itself stays in the user's own Google account), and delivery of mobile push notifications through Firebase Cloud Messaging (relayed to Apple's push service for iOS devices); notification content includes the sender's name, the chat name, and the message text.	United States
Microsoft Corporation	Email sync via Microsoft Graph where a user connects an Outlook inbox; the mailbox itself stays in the user's own Microsoft account. Receives nothing unless that integration is connected.	United States
Unipile	Powers the Gmail inbox sync; connected mailbox content and metadata pass through it. Receives nothing unless a Gmail inbox is connected.	France
OpenAI, L.L.C.	Processes the content an AI feature runs on, for example summarising a candidate record or transcribing a recorded in-person meeting. Phone-call transcription is done by Zoom; call audio never reaches OpenAI. Contractually prohibited from training models on Customer Data.	United States
Zoom Communications, Inc.	Carries calls for the built-in phone system through the customer's own Zoom account; call recordings, voicemail, and Zoom's own call transcription live in that Zoom account per its retention settings. Where Customer opts in to contact sync, contact names, numbers, and email addresses are pushed to that Zoom account as well. Zoom acts as a Sub-processor only for connecting calls placed through the Service; data stored in Customer's own Zoom account is held under Customer's direct agreement with Zoom. Receives nothing if calling is not used.	United States
SignWell	Handles documents a user sends out for electronic signature (for example, offers or client agreements) and signer names and email addresses. Receives nothing unless document signing is used.	United States
Intercom, Inc.	Powers the in-app support chat. Receives the user's name, work email, and the messages they send Caliber's team.	United States
Axiom, Inc.	Receives application logs and traces (OpenTelemetry) used to operate and debug the Service, retained for 365 days. Traces are technical diagnostic data; error records can occasionally capture personal information from a failing request.	United States

The following vendors support Caliber's business but do not process Customer Personal Information under this DPA, and are listed for transparency only: Vercel, Inc. (hosting of the caliberjobs.com marketing website), Xero Limited (Caliber's own invoicing and billing records), Unsplash Inc. (stock image search for workspace branding).