

Data Processing Agreement

Data Processing Agreement (DPA)

Policy	Data Processing Agreement (DPA)
Version	1.0
Effective date	2 October 2026
Status	Incorporated by clause 16 of the Standard Terms of the Platform Licence Agreement
Address	vhire.com/legal/dpa

Talgrid Tech Private Limited, trading as NextGeek and vHire (**Talgrid**).

Key points

This summary is to help the reader. If it differs from the sections below, the sections below govern.

- For the records the Customer keeps in its own workspace, the Customer is Data Fiduciary and Talgrid is its Data Processor (sections 2.1 and 2.5).
- Talgrid keeps one record for each candidate across all its customers, the Talgrid Candidate Record. Candidate details and documents the Customer supplies are added to that record, and another customer that holds the same candidate sees most of it. Talgrid is Data Fiduciary for that record and limits its own use of it. The Customer accepts this specifically (section 2.6).
- Talgrid erases on written request within thirty days (longer for very large requests) and deletes on exit within the periods in clause 6.6. Talgrid does this by hand. Erasure and exit deletion do not delete the Talgrid Candidate Record, apart from identity documents, payslips and Assessment skill levels (section 11).
- Customer personal data is stored and processed in several countries, mainly in the United States and in Cloudflare's Asia-Pacific region group. Talgrid does not commit to keep it in India (section 8).
- Interviews in a Platform interview room are recorded, transcribed, summarised and scored by AI. The Platform shows participants no recording notice, so the Customer gives one (sections 13.4 and 15.1(g)).
- Reveal, discovery of candidates a customer does not hold, and AI Interviews are not available at the date of this version (sections 2.8 and 13.5).

About this Policy

(a) This is a Policy under clause 16 of the Standard Terms and part of the Agreement (clause 1.1). Terms not defined here have the meaning given in the Standard Terms.

(b) **Ranking.** For personal data this DPA ranks under clause 1.3(b): above the Standard Terms, and below only the latest Order Form or Change Order for what that records. On retention and deletion of personal data it also prevails over the Service Terms (clause 1.3(d)).

(c) **Limits on ranking.** Ranking does not change two things. First, liability: every claim under this DPA is subject to the limits, exclusions and exceptions in clause 12 of the Standard Terms, including the separate limit that clause sets for a personal data breach caused by Talgrid's failure to maintain the Security Measures. Second, how this DPA changes: only under clause 16.2.

(d) This DPA has no governing-law or dispute clause of its own. Clauses 13 and 15 of the Standard Terms apply.

(e) **What this DPA describes.** This DPA describes how the Platform processes personal data on the date this version takes effect. Where a feature is not available on that date, this DPA says so.

1. Definitions

1.1 In this DPA:

Term	Meaning
Data Protection Laws	As defined in clause 1.5(g) of the Standard Terms. In addition, the directions issued by the Indian Computer Emergency Response Team (CERT-In) on 28 April 2022 under section 70B(6) of the Information Technology Act, 2000 continue to form part of the Data Protection Laws after the Digital Personal Data Protection Act, 2023 (the DPDP Act) and the Digital Personal Data Protection Rules, 2025 (the DPDP Rules) apply, to the extent the directions are then in force. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are the SPDI Rules .
Data Fiduciary, Data Processor, Data Principal, personal data, personal data breach and processing	The meanings they have in the DPDP Act (clause 1.5(g)).
Customer personal data	Personal data in Customer Data.
Customer Data	As in clauses 6.1 and 7.1 of the Standard Terms, as section 2 of this DPA applies them. It includes each output Talgrid generates for the Customer, such as a score or ranking, and, once Reveal is available to the Customer (section 2.8), each record delivered to it on a Reveal.

Term	Meaning
Talgrid Candidate Record	The single record Talgrid keeps about an individual for all its customers, described in section 2.3. It includes the record of each individual who is Talgrid's own Data Principal under clause 6.2.
Workspace Records	The Customer Data that the Platform keeps for the Customer's workspace only, listed in section 2.5.
Production Stores	The live databases and storage the Platform runs on: the primary database operated by Neon, the Cloudflare D1 databases, the Cloudflare R2 object storage buckets and the Cloudflare Vectorize search indexes.
Sub-processor	As defined in clause 1.5(h) of the Standard Terms: a third party that Talgrid engages to process Customer personal data on Talgrid's behalf and that is listed in the Third-Party Services Policy. A Third-Party Service the Customer enables under clause 8.1 is not a Sub-processor.
Network Opt-in	A written opt-in to the Network Participation Terms recorded in an Order Form or Change Order (clauses 6.4(d) and 16.1).
Export Period	The thirty (30) days after termination or expiry during which the Customer may export Customer Data (clause 6.6).
Business Day	A day other than a Saturday, a Sunday or a public holiday in Karnataka.

1.2 Commencement. The DPDP Act and DPDP Rules take effect in stages, on the dates the Central Government notifies. Until a provision takes effect, the laws that clause 1.5(g) applies until then, including section 43A of the Information Technology Act, 2000 and the SPDI Rules, govern the processing that provision would cover. This DPA binds the Parties as a contract from the Effective Date and does not wait for a provision to take effect. Where it refers to a requirement of the DPDP Act or DPDP Rules that has not yet taken effect, the reference states the standard the Parties have agreed to work to, and from the date the requirement takes effect it applies as law as well.

2. Roles and the Talgrid Candidate Record

2.1 Customer Data. For Customer Data the Customer is the Data Fiduciary and Talgrid is its Data Processor, acting on the Customer's documented instructions (clause 6.1), except as section 2.6 provides for the Talgrid Candidate Record. This DPA is the contract under which Talgrid processes Customer personal data on the Customer's behalf, including for section 8(2) of the DPDP Act and Rule 6(1)(f) of the DPDP Rules once they take effect. The Customer remains responsible for its duties as Data Fiduciary. Nothing in this DPA transfers a statutory duty from one Party to the other.

2.2 Talgrid's own data principals. Individuals who register with, claim a profile on, or consent to be contacted through NextGeek or vHire are Talgrid's Data Principals. Talgrid is the Data Fiduciary for that relationship (clause 6.2) and this DPA does not govern it. The same is true of the account, sign-in, security and billing records Talgrid keeps about Authorised Users and the Customer's contacts in order to run the Customer's account. Where an Authorised User adds a candidate by hand, or is

recorded as a candidate's owner in the Customer's applicant tracking system, that Authorised User's email address or name becomes part of the Talgrid Candidate Record, and other customers that hold the same candidate can see it (section 2.4(a)).

2.3 The Talgrid Candidate Record.

(a) **What it is.** Talgrid keeps one record for each individual across all its customers. The record holds:

(i) the individual's name and contact details, profile links, current employer, job title and location, work experience, education, skills, compensation and notice period;

(ii) other profile details such as date of birth, gender, nationality and marital status, where they have been supplied;

(iii) the individual's resumes, with the text and parsed content of each, and which of them is the current main resume;

(iv) documents received from an applicant tracking system, such as identity documents (for example scans of a PAN card, Aadhaar card or passport), payslips, offer letters and other HR documents, each with the web address in that system from which it was fetched;

(v) details received from an applicant tracking system about how the individual is handled there: the name or email address of the person recorded as the individual's owner (for an individual an Authorised User adds by hand, that Authorised User), and the individual's profile link, status and comments in that system; and

(vi) skill levels measured in Assessments.

(b) **How a candidate reaches it.** A candidate reaches the Talgrid Candidate Record when the Customer, or the Platform for the Customer:

(i) receives the candidate from an applicant tracking system the Customer connects;

(ii) adds the candidate by hand or by bulk upload;

(iii) receives an application through a careers page or job post that the Platform hosts for the Customer;

(iv) receives the candidate from a vendor (section 2.9);

(v) imports the candidate from a job portal through the Customer's own account; or

(vi) uploads a resume for the candidate.

(c) **Matching.** Talgrid matches the candidate to an existing Talgrid Candidate Record by email address, by LinkedIn or GitHub profile, by an identical resume file, or by phone number together with the same name. If nothing matches, Talgrid creates a new record. Matches Talgrid cannot make with confidence are held for review.

(d) **Updates.** The details and documents supplied update the record. A value supplied replaces the value the record holds, and an empty value leaves it unchanged, except that:

(i) details supplied by any route other than the upload of a resume under paragraph (b)(vi) do not replace a name or current employer that the record already holds;

(ii) entries in lists such as work history, education and skills are added to the entries the record holds, or update a matching entry; and

(iii) an entry the individual has edited is not changed.

(e) **Other updates.** In the same way:

(i) parsing a resume uploaded for the candidate updates the record;

(ii) answers to screening questions that match profile fields, such as compensation, notice period, date of birth, gender, nationality and marital status, update the record;

(iii) where Talgrid has switched on AI call notes for the Customer, applying a suggested update writes the suggested compensation, notice period, employer, job title or location into the record; and

(iv) when an Assessment the Customer commissions is completed and passes Talgrid's integrity checks, Talgrid adds the skill levels it measured to the record.

(f) **No trail by customer.** Talgrid does not keep a complete record of which customer supplied each value or document. Values supplied by different customers, by the individual and by Talgrid cannot be separated one customer at a time.

(g) **No opt-out setting.** The Platform gives the Customer no setting that keeps the details or documents it supplies out of the Talgrid Candidate Record.

2.4 What other customers see.

(a) Another customer that holds the same individual, including one that adds the individual later and is matched to the same record, sees the Talgrid Candidate Record as it currently stands in its candidate list and candidate profile, apart from the status and comments from an applicant tracking system. That includes values the Customer supplied, the owner and profile link from the Customer's applicant tracking system, and the individual's current main resume, which may be a file the Customer uploaded. It also sees the list of documents in section 2.3(a)(iv), and can open those that are not identity documents or payslips. The Platform shows identity documents and payslips to it as restricted and does not let it open them.

(b) It also sees any match report about the individual that the Platform holds without a link to a customer. That can include a match report received from the Customer's applicant tracking system where the Platform could not identify the Customer when it received the report.

(c) Its candidate list also shows the individual's best Assessment score, taken from all the Assessments the individual has taken on the Platform, whichever customer commissioned them.

The candidate quality score and hiring-decision recommendation the Platform gives that customer may also use the individual's results in other customers' Assessments. Other customers cannot open the Customer's Assessment sessions, answers, recordings or reports.

(d) Talgrid keeps two search indexes of candidates for all its customers. One holds, for each individual, an entry built from the individual's skills, summary, work experience, achievements, education, location and work mode, stored with the individual's name, expected compensation, location, experience, notice period and work mode. The other holds entries built from the individual's job titles, summary, skills, experience, location, work mode, notice period and the text of the most recently updated resume. Talgrid limits each customer's results to the individuals that customer holds. When Talgrid matches and ranks candidates for a customer, it uses the Talgrid Candidate Record, including skill levels from Assessments, and resume text (section 13.7).

2.5 Workspace Records. The following Customer Data is kept for the Customer's workspace only:

(a) notes, including notes received from the Customer's applicant tracking system, but not the comments in section 2.3(a)(v);

(b) email and WhatsApp conversations and messages;

(c) calls, call recordings and AI call notes;

(d) applications and the screening answers stored with them, pipeline stages, interviews, offers and placements;

(e) jobs;

(f) candidate profiles forwarded to the Customer's clients;

(g) match reports and scores that Talgrid generates for the Customer, and match reports received from its applicant tracking system, except as section 2.4(b) describes;

(h) edits that Authorised Users make to a candidate's details in the candidate profile;

(i) the Customer's Assessment sessions, answers, scores, recordings, snapshots, identity images, face-matching templates, liveness and anti-spoof results, and reports; and

(j) interview recordings, transcripts, summaries and AI scorecards.

Sections 2.3(e) and 2.4 describe what reaches the Talgrid Candidate Record, or other customers, from some of them. Talgrid separates Workspace Records from other customers' data in application code, by the Customer's identifier, and not by database row-level security (Security Measures, section 3.1).

2.6 Roles for the Talgrid Candidate Record.

(a) Talgrid decides that one record exists for each individual across its customers, how records are matched and updated, and which customers see them. For the Talgrid Candidate Record Talgrid is therefore a Data Fiduciary, and not the Customer's Data Processor.

(b) When the Customer supplies candidate details or documents by any route in section 2.3(b), it instructs Talgrid to match the individual (section 4.1) and authorises Talgrid to add those details and documents to the Talgrid Candidate Record. Once added, they form part of the Talgrid Candidate Record. Adding them does not take away the Customer's rights in what it supplied. It gives Talgrid the right to hold and use them only as this section 2 describes. The Customer's own use of the record, and its Workspace Records, remain Customer Data.

(c) **How this fits with the Standard Terms.** The Customer accepts this section 2 specifically: its Order Form, or the Standard Terms that its Order Form incorporates, records the Customer's acknowledgement of the Talgrid Candidate Record. For personal data this DPA also ranks above the Standard Terms (clause 1.3(b)). Accordingly, for the Talgrid Candidate Record:

(i) clause 6.1 applies to candidate details and documents the Customer supplies as section 2.6(b) provides;

(ii) clauses 6.4(b) and 6.4(c) apply to the Talgrid Candidate Record of each individual the Customer holds as they apply to Customer Data (sections 10.1 and 13.3);

(iii) another customer seeing, or receiving outputs that use, anything section 2.4 describes, including the best Assessment score and any score or recommendation that uses results of the Customer's Assessments, is a further exception to clause 6.4(d), in addition to sharing under the Network Participation Terms;

(iv) deletion under clause 6.6 and section 11 does not delete the items in section 11.4(b);

(v) the first sentence of clause 7.1 describes the basis on which Talgrid makes a record available for Reveal and discovery, and Talgrid holds the Talgrid Candidate Record of an individual who has not given that consent on the basis this section 2 describes;

(vi) adding details and documents to the Talgrid Candidate Record, and what section 2.4 describes, are use for the purposes of this Agreement and a disclosure the Customer authorises, for clause 10.2; and

(vii) Talgrid's own processing of the Talgrid Candidate Record as Data Fiduciary is not processing of Customer Data for clause 12.6.

(d) **Limits on Talgrid's use.** Talgrid uses the Talgrid Candidate Record, including the details and documents the Customer supplied, only:

(i) to provide, secure and support the Platform for the customers that hold the individual;

(ii) to let the individual see and correct their own record;

(iii) to create de-identified data under section 4.4; and

(iv) where the individual is Talgrid's own Data Principal (section 2.2), or Talgrid placed the individual's record in a workspace before the Effective Date (section 2.10), as Data Fiduciary for that relationship.

Talgrid does not let a customer search for, browse or receive on a Reveal the record of an individual that customer does not hold, unless the individual has consented to that through Talgrid's own consent flow.

2.7 Information individuals give Talgrid directly. Information an individual gives Talgrid directly, for example by updating their own vHire profile or consenting through Talgrid's own consent flow, is part of the Talgrid Candidate Record and is not Customer Data. Talgrid may use it as Data Fiduciary.

2.8 Reveal and discovery. Reveal, Profile Refresh and discovery of candidates a customer does not hold (clause 7.1) are not available on the Platform at the date of this version. Where this DPA refers to a Reveal, it applies from the date Talgrid first makes Reveal available to the Customer, which an Order Form or Change Order records. From then, a record delivered on a Reveal becomes Customer Data, and the Customer is Data Fiduciary for its own processing of it (clause 7.1).

2.9 Vendors. Talgrid does not set up a relationship through which another customer submits candidates to the Customer as a vendor, or the Customer submits candidates to another customer, unless an Order Form or Change Order records a Network Opt-in for both. A candidate a vendor submits to the Customer is added for the Customer as section 2.3 describes.

2.10 Records Talgrid placed before the Effective Date. Where the Order Form records that candidate records were in the Customer's workspace before the Effective Date because Talgrid placed them there, those records are Talgrid's own data and not Customer Data, unless the Order Form says otherwise.

3. Scope of processing

Subject matter	Provision of the Platform under the Agreement.
Duration	The Term, plus the Export Period and the deletion periods in clause 6.6 and section 11.
Nature and purpose	Recruitment. Storing and organising candidate records and documents; matching each candidate to the Talgrid Candidate Record and updating it (section 2.3); parsing resumes; matching, scoring and ranking; administering Assessments, including proctoring and identity verification; scheduling, conducting, recording, transcribing, summarising and scoring interviews; calling and messaging candidates; hosting careers pages; and, where the Order Form licenses it and the Third-Party Services Policy lists a Verification Partner, background verification.
Categories of Data Principal	Candidates. The Customer's own personnel, including Authorised Users recorded as a candidate's owner, its interview panellists and, where the Customer is a staffing provider, its clients' personnel, to the extent their data is in Customer Data.

Categories of personal data	Contact details and profile links; employment and education history; skills; compensation and notice period; date of birth, gender, nationality and marital status where supplied; resumes and other attachments; documents received from an applicant tracking system, including identity documents and payslips; the owner, profile link, status and comments from an applicant tracking system; screening answers; Assessment answers and scores; proctoring recordings and snapshots, including face images; where an Assessment uses identity verification, images of identity documents, a live selfie, face-matching templates (biometric descriptors) computed from them, and the results of liveness and anti-spoof checks; interview video and audio recordings, transcripts, summaries and AI scorecards; call recordings and AI call notes where telephony is enabled; email and WhatsApp messages; and notes.
Persons under eighteen	The Platform is not for anyone under eighteen (section 14).

4. Instructions

4.1 Talgrid processes Customer personal data only on the Customer's documented instructions. Those instructions are this DPA, the Standard Terms, the Order Form, the Service Terms, and the Customer's use of the features of the Platform. They include matching each candidate to the Talgrid Candidate Record and adding details and documents to it (section 2.3), and what section 2.4 describes, including outputs given to other customers that use results of the Customer's Assessments.

4.2 If Talgrid considers that an instruction infringes Data Protection Laws, it tells the Customer and may suspend the affected processing until the instruction is withdrawn or changed.

4.3 Enabling a Third-Party Service under clause 8.1 is an instruction to send Customer Data to that provider. The provider acts for the Customer, on the Customer's own account and under the provider's terms, and is not Talgrid's Sub-processor.

4.4 **De-identified data.** The Customer gives the instruction in clause 6.4(f) to create de-identified, aggregated data that identifies no person, customer or candidate. Talgrid creates such data, for example skill names, job titles and match outcomes without identifiers, which it uses to build its skill and role taxonomy. Talgrid does not try to re-identify it. The search indexes in section 2.4(d) are not de-identified data.

4.5 Talgrid processes Customer personal data other than on the Customer's instructions only where the law requires. It then tells the Customer first, unless the law forbids that. This section 4.5 does not affect section 4.4.

5. Confidentiality and personnel

5.1 Talgrid ensures that the personnel it authorises to process Customer personal data are bound by confidentiality obligations.

5.2 Access is limited to personnel who need it to provide or support the Platform.

6. Security

6.1 Talgrid implements and maintains the Security Measures (clause 6.4(a)). They are published at vhire.com/legal/security-measures and describe safeguards Talgrid actually operates.

6.2 The Security Measures state the security safeguards Talgrid maintains for the purposes of the Data Protection Laws. At the date of this version they state no retention period for logs and no backup commitment. Before Rule 6 of the DPDP Rules takes effect, Talgrid will publish a version of the Security Measures that provides for the safeguards that Rule requires, including the retention of logs.

6.3 Talgrid holds no SOC 2 or ISO 27001 certification and represents none.

7. Sub-processors

7.1 **General authorisation.** The Customer authorises Talgrid to engage Sub-processors. The current Sub-processors, with what each does, the data it handles and where, are listed in the Third-Party Services Policy.

7.2 **Notice (clause 6.4).** Talgrid gives at least thirty (30) days' notice before a new or replacement Sub-processor begins to process Customer personal data. The notice goes by email to the Customer's Legal Contact and administrator, and states the Sub-processor's name, service, data categories, location and start date. The change is also recorded in a new version of the Third-Party Services Policy (Part E of that Policy).

7.3 **Objection (clause 9.4).** Within fifteen (15) days of a notice under section 7.2 the Customer may object, in writing to Talgrid's Legal Contact, on reasonable data protection grounds that it states. The Parties discuss the objection in good faith. If it is not resolved within thirty (30) days after the objection, the Customer may, by written notice given within a further fifteen (15) days, terminate the affected service and receive a pro-rata refund of prepaid fees for it (clause 9.4). A Customer that does not object within the fifteen (15) days accepts the Sub-processor.

7.4 **No standstill.** Talgrid may begin to use the new Sub-processor when the thirty (30) days end, even if an objection is still open. The Customer's remedy for an unresolved objection is section 7.3.

7.5 **Emergency replacement.** Talgrid may replace a Sub-processor at once where that is needed to maintain security or continuity of the Platform. It gives notice as soon as practicable. The fifteen (15) days in section 7.3 then run from that notice.

7.6 Sub-processor terms and responsibility. Talgrid uses each Sub-processor under that provider's terms, including its data processing terms where it offers them. For model providers reached through OpenRouter, Talgrid relies on OpenRouter's terms and Talgrid's account settings (section 13.3). Talgrid remains responsible to the Customer for each Sub-processor's processing of Customer personal data. Clause 8.3 does not apply to that processing. Talgrid's liability for it is under clause 12.

7.7 Sub-processor changes are outside clause 16.2. A change of Sub-processor is governed by clauses 6.4 and 9.4 and this section 7. It is not a Policy change under clause 16.2, and the Customer has no right under clause 16.2 to stay on an earlier list.

8. Where Customer personal data is stored and processed

8.1 Locations.

(a) The primary database is operated by Neon on Amazon Web Services in the United States (region us-east-1). It holds candidate records, including the Talgrid Candidate Record and the list of candidate documents, and applications, jobs, messages, notes and most other Workspace Records. Files, recordings, images, and Assessment and interview records are held as paragraph (b) describes.

(b) Edge databases (Cloudflare D1), which hold Assessment and interview records among others, and object storage (Cloudflare R2), which holds resumes, documents, identity documents, payslips, images and recordings, are created with a location hint. Most hints are for Cloudflare's Asia-Pacific region group, and a few are for Eastern North America. Asia-Pacific is a group of countries, not India, and a location hint is not a commitment that data stays in any place.

(c) Search indexes, key-value stores, queues and Durable Objects run on Cloudflare's global network, and Talgrid sets no location for them. Cloudflare may run some services in locations near the primary database in the United States.

(d) To answer repeated requests, Cloudflare may hold copies of database query results for about a minute, and of AI model requests and responses for up to one hour (section 13.6). Talgrid does not keep the content of AI model requests and responses in the logs of Cloudflare's AI Gateway.

(e) Sub-processors process Customer personal data in the countries stated in the Third-Party Services Policy. AI model providers reached through OpenRouter operate in the United States and other countries, and Talgrid does not choose which host serves a request.

(f) Talgrid does not commit to store or process Customer personal data in India or in any particular country.

8.2 Transfers outside India. Until section 16 of the DPDP Act takes effect, Rule 7 of the SPDI Rules governs the transfer of sensitive personal data or information, such as biometric information, outside India. Under it, sensitive personal data or information may be transferred only to a recipient

that ensures the same level of protection, and only where the transfer is necessary for a lawful contract with the individual or the individual has consented. The Customer obtains any consent that Rule requires from it as the party that collects the data through the Platform (section 15.1(b)). From the date section 16 takes effect, the Data Protection Laws permit transfer outside India except to a country or territory the Central Government restricts, subject to Rule 15 of the DPDP Rules and to any requirement that applies to a Significant Data Fiduciary (Rule 13). Talgrid gives notice if a restriction affects the Platform.

8.3 Sectoral rules that require the Customer's own regulated data to stay in India, or in a place, are the Customer's responsibility. The Customer does not upload data covered by such a rule unless the Order Form records an arrangement that meets it.

9. Data Principal rights and grievances

9.1 What the Platform lets the Customer do. The Platform lets Authorised Users view the candidates the Customer holds and its Workspace Records, and delete some items, such as notes, jobs and message templates. It does not let the Customer delete a candidate, a resume, a document, an application, an Assessment record or a recording, and it has no bulk export. Talgrid erases on request under section 11.2 and prepares the exit export under section 11.3.

9.2 If a Data Principal approaches Talgrid about Customer Data, Talgrid refers them to the Customer and notifies the Customer within two (2) Business Days. Talgrid does not respond on the substance except to acknowledge the request and say that it has been passed on.

9.3 Talgrid gives the Customer reasonable assistance, at no charge for a reasonable volume, with a request or complaint the Customer cannot deal with through the Platform. That assistance covers:

- (a) an individual's request for a summary of their personal data (section 11 of the DPDP Act), by extracting what the Platform holds about them for the Customer;
- (b) grievance redress by the Customer (section 8(10) of the DPDP Act);
- (c) a withdrawal of consent, where the Customer instructs Talgrid to stop the processing that depended on it (section 6(6) of the DPDP Act), which Talgrid does by erasure under section 11.2;
- (d) erasure, under section 11.2;
- (e) a correction to the Talgrid Candidate Record that the Customer passes on, which Talgrid makes within thirty (30) days if it is satisfied that the correction is accurate;
- (f) an inquiry by the Data Protection Board of India (the **Board**) about Customer Data; and
- (g) a data protection impact assessment or audit, if the Customer is notified as a Significant Data Fiduciary.

9.4 Revealed candidates (clause 6.5). From the date Reveal is available to the Customer (section 2.8), if a candidate whose record was delivered to the Customer on a Reveal withdraws consent or

asks for deletion, Talgrid passes that to the Customer as a withdrawal notice within two (2) Business Days, through the Platform and by email to the Customer's administrator and Legal Contact. The Customer acts on it as clause 7.1 and the Service Terms provide.

9.5 Talgrid publishes a contact for questions about how it processes personal data, at compliance@vhire.com.

9.6 Requests about the Talgrid Candidate Record. If an individual asks the Customer to correct or erase details held in the Talgrid Candidate Record, the Customer may pass the request to Talgrid under section 9.3 and refer the individual to Talgrid at compliance@vhire.com. Talgrid handles such requests as Data Fiduciary under the Data Protection Laws.

10. Personal data breach

10.1 Notice within 24 hours (clause 6.4). Talgrid notifies the Customer without undue delay, and in any event within twenty-four (24) hours of becoming aware, of a personal data breach affecting Customer Data or the Talgrid Candidate Record of an individual the Customer holds. Notice goes by email to the Customer's Legal Contact and administrator.

10.2 Content. The notice describes, as far as Talgrid then knows:

- (a) the nature of the breach, its extent, and when and where it occurred;
- (b) its cause, if known;
- (c) the categories and approximate number of Data Principals and records affected;
- (d) the likely consequences; and
- (e) the measures taken or proposed to contain it and to reduce harm, and a contact at Talgrid.

Talgrid sends an update at least every twenty-four (24) hours until the breach is closed, and a final report when it is.

10.3 Handling. Talgrid takes reasonable steps to contain, investigate and remedy the breach, and gives the Customer the information and help it reasonably needs to meet its own duties to the Board and to affected Data Principals.

10.4 Who notifies whom. The Customer, as Data Fiduciary, decides whether and how to notify the Board and Data Principals about Customer Data. Talgrid does not notify them about Customer Data unless the law requires it or the Customer instructs it to. Talgrid's own reporting to CERT-In, within six hours where the CERT-In directions apply, and its own notices to the Board and Data Principals for its own data, including the Talgrid Candidate Record, are separate.

11. Retention and deletion

11.1 During the Term. Talgrid keeps Customer Data for the Term and the Export Period, until it is erased under section 11.2 or deleted under section 11.3. Apart from caches, temporary working copies and unused invitations, which the Platform removes on its own, the Platform does not delete Customer Data on a schedule, and Talgrid will not start to do so except under a new version of this DPA. The working copies include copies of inbound emails and of message webhooks, deleted after seven (7) days, copies of inbound WhatsApp messages, deleted after forty-five (45) days, and email delivery events, deleted after thirty (30) days. Where the Service Terms state a different retention period, this DPA prevails (clause 1.3(d)), and the Customer may at any time instruct erasure under section 11.2.

11.2 Erasure on instruction.

(a) **Instruction.** The Customer's administrator or Legal Contact sends a written instruction to compliance@vhire.com that identifies the individuals to be erased, by name and email address or by the identifier the Platform shows, or the records to be erased.

(b) **Timing.** Talgrid acknowledges the instruction within two (2) Business Days. It completes the erasure within thirty (30) days after it receives the instruction. Where the instructions it receives from the Customer in any thirty (30) days together name more than one thousand (1,000) individuals, it completes them within sixty (60) days, and where they name more than ten thousand (10,000) individuals, within ninety (90) days.

(c) **Method.** Talgrid personnel with access to the Production Stores carry out the erasure directly in those stores, using procedures Talgrid has tested. The Platform has no automated function to erase a candidate or the Customer's records about a candidate.

(d) **What is erased.** For each individual named, Talgrid erases from the Production Stores:

(i) the Customer's link to the individual, so the individual no longer appears in the Customer's workspace;

(ii) the Customer's Workspace Records about the individual;

(iii) the Assessment sessions the Customer commissioned for the individual, with their answers, scores, recordings, snapshots, identity images and face-matching templates, and the skill levels Talgrid added to the Talgrid Candidate Record from them;

(iv) recordings, transcripts, summaries and scorecards of the Customer's interviews and calls with the individual;

(v) resume and application files that the Platform stored under the Customer's account for the individual;

(vi) identity documents and payslips received from an applicant tracking system for the individual, and their files. Talgrid cannot tell which customer's system supplied them, so it erases them for every customer that holds the individual; and

(vii) entries in Talgrid's error tracker, and in the issues the error tracker has filed, that contain the individual's email address or phone number, which Talgrid deletes or redacts.

(e) **Provider copies.** Talgrid asks Acefone, Meta and Mailgun in writing to delete the copies they hold of the individual's call recordings, WhatsApp messages and emails sent or received for the Customer, and tells the Customer what each provider confirms.

(f) **Confirmation.** Talgrid confirms in writing when it has finished, listing what it erased, what each provider confirmed, and what remains under section 11.4.

(g) **Backups.** Section 11.5 applies to copies in backups and database history.

11.3 On exit (clause 6.6).

(a) **Export Period.** The Platform has no read-only mode, so Talgrid leaves the Customer's access open for the Export Period, and the Customer uses it only to access and export Customer Data (clause 5.4).

(b) **Export.** The Platform has no bulk export. On written request to compliance@vhire.com made during the Export Period, Talgrid prepares an export and delivers it by a secure method within fifteen (15) Business Days of the request. The export has structured records as CSV files and stored files in their original format. It includes the Customer Data and, for each individual the Customer holds, the Talgrid Candidate Record as it then stands, with the individual's resume files and the documents in section 2.3(a)(iv) other than identity documents and payslips. Once Reveal has been available to the Customer, the export also includes records delivered on a Reveal, notwithstanding clause 7.1.

(c) **Deletion.** Talgrid then deletes Customer Data from the Production Stores within sixty (60) days after the Export Period ends, and from backups within ninety (90) days after it ends (clause 6.6). It does so by the method in section 11.2(c). The deletion covers, for every individual the Customer holds, the items in section 11.2(d), and the Customer's other Customer Data, such as its jobs, templates and settings. Talgrid also makes the requests in section 11.2(e) for the Customer's call recordings, messages and emails.

(d) **Confirmation.** Talgrid confirms the deletion in writing on request.

11.4 What is not deleted (clause 6.6). Sections 11.2 and 11.3 do not require deletion of:

(a) what clause 6.6 itself excludes: de-identified, aggregated data created under section 4.4; data Talgrid must keep by law, including logs and the personal data in them that Talgrid keeps because the Data Protection Laws require it (including under Rules 6(1)(e) and 8(3) of the DPDP Rules once they take effect), to which access is limited to security and legal purposes; Platform Records, executed Order Forms and Change Orders, Certificates of Execution, invoices, and records of licences, Authorised Users and Usage Units, for the periods in clauses 3.6(f) and 11 of the Standard Terms; and the data of Talgrid's own Data Principals; and

(b) the following further items, which the Customer accepts under section 2.6(c)(iv):

- (i) the Talgrid Candidate Record, apart from the skill levels and documents erased under section 11.2(d)(iii) and (vi). It includes the details the Customer supplied that became part of it (section 2.6); the text and parsed content of each resume the Customer supplied, which stay after the resume file is erased; documents received from the Customer's applicant tracking system other than identity documents and payslips; the owner, profile link, status and comments from that system; and the entries in the search indexes built from the record. The record stays after the Customer's link is removed, including where no other customer holds the individual;
- (ii) Talgrid's audit log of privileged actions, which Talgrid keeps for security;
- (iii) Assessment session state held in Cloudflare Durable Objects, namely the candidate's identifier, the session's timings and status, the proctoring score, recorded violations and the ability estimate, which the Platform has no means to delete for one session at the date of this version;
- (iv) copies in Cloudflare key-value stores and queues, which the Platform uses for caches and work in progress. Cloudflare deletes a queue message once it is processed or its retention period ends, and some caches expire on their own. Talgrid does not search those stores for an individual's data;
- (v) entries in Talgrid's error tracker, and in the issues it has filed, that contain fragments of personal data other than those removed under section 11.2(d)(vii); and
- (vi) copies that providers keep under their own terms: Cloudflare's interview service keeps recordings and transcripts for seven (7) days; Cloudflare's AI Gateway keeps cached model requests and responses for up to one hour; model providers reached through OpenRouter keep requests as their terms and Talgrid's account settings allow (section 13.3); and Acefone, Meta and Mailgun keep copies until they act on a request under section 11.2(e) or as their own terms provide.

11.5 Backups, database history and logs. Copies of deleted data remain in the point-in-time history of the primary database and of the D1 databases until they age out, and in any other copy of a Production Store that Talgrid has made until Talgrid deletes it. Talgrid ensures those copies are gone within ninety (90) days after an erasure under section 11.2, and on exit within the period in section 11.3(c). Cloudflare deletes the Platform's request logs after about seven (7) days.

12. Audit and information

12.1 Talgrid makes available the information reasonably necessary to show that it complies with this DPA.

12.2 The Customer may audit Talgrid's processing of Customer personal data once in any twelve (12) month period, on thirty (30) days' notice, during business hours, remotely unless the Parties agree otherwise, without disrupting the Platform, and under confidentiality (clause 10.2). Each Party bears its own costs of an audit.

12.3 The Customer may make one further audit after a personal data breach affecting Customer Data, or where the Board or another regulator requires it.

12.4 Talgrid holds no third-party audit report. It may satisfy an audit by providing a completed security questionnaire and the supporting evidence, and by answering the Customer's reasonable follow-up questions.

12.5 Audit of records showing that invoices correspond to the Order Form is under clause 11 of the Standard Terms and not this section.

13. Assessments, interviews, proctoring and automated processing

13.1 Proctored Assessments. Before a proctored Assessment starts, the Platform shows the candidate a data-processing notice that Talgrid has written, on the Customer's behalf and as its Data Processor, and records the candidate's consent to camera access, screen monitoring and recording of the session. During the Assessment the Platform captures camera snapshots, recording segments and events such as switching tabs. Where the Assessment uses identity verification, the candidate's browser computes face-matching templates (biometric descriptors) from an image of an identity document and a live selfie, and the Platform stores the images, the templates, the results of liveness and anti-spoof checks, and the match decision. Talgrid is responsible for the accuracy of what that notice says about the Platform's processing. The Customer, as Data Fiduciary, gives the candidate any further notice its law requires, including notice that the Customer is the Data Fiduciary.

13.2 Human review (clause 7.2). Resume parsing, matching, scoring, screening, interview scorecards and other automated outputs support the Customer's decisions and do not make them. The Customer keeps meaningful human review of every output before acting on it. No output is the sole basis for rejecting a candidate.

13.3 No training. Talgrid does not use Customer Data, the Talgrid Candidate Record or candidate responses to train foundation models, and does not permit its Sub-processors to (clause 6.4(c)). Talgrid itself does not train or fine-tune any language model or other foundation model.

13.4 Interview rooms. The Platform records every interview held in a Platform interview room, from the start, in two ways. Each participant's browser records the interview (the candidate's video and audio, and the interviewer's audio) and uploads the recording directly to Talgrid's storage. Cloudflare's interview service also records the meeting, and Talgrid copies that recording to its own storage. Talgrid transcribes the recording on Cloudflare Workers AI. Cloudflare's interview service also produces a transcript and an AI-generated summary, which Talgrid copies to its own storage. The Platform then automatically produces an AI-generated scorecard that scores the candidate's answers. Section 13.2 applies to the summary and the scorecard. The Platform does not show participants a recording notice. Before using an interview room, the Customer tells the participants that the interview will be recorded, transcribed, summarised and scored by AI, and obtains any consent its law requires (section 15.1(g)).

13.5 AI Interviews. AI Interviews are not available on the Platform at the date of this version. Clause 7.2 applies to them when they are.

13.6 AI models.

(a) The Platform uses AI models to parse resumes and job descriptions; to match, score and rank candidates; to summarise and classify messages, interviews and calls; to transcribe and score interviews; to generate Assessment content; to transcribe calls where AI call notes are switched on; and to classify skill names and job titles for its taxonomy (section 4.4).

(b) Some models run on Cloudflare Workers AI, inside Cloudflare's service. Others are reached through OpenRouter, by way of Cloudflare's AI Gateway, and are served by the model providers OpenRouter routes to.

(c) Requests to those models can include resume text and scanned resume files, candidate profile details, screening answers, messages from candidates, interview transcripts, and interview and Assessment context.

(d) Cloudflare's AI Gateway may keep a request and its response for up to one hour, so that an identical request can be answered from that copy. Talgrid does not keep the content of requests and responses in the AI Gateway's logs.

(e) OpenRouter decides which host serves a request. For search re-ranking, Talgrid allows any model in OpenRouter's catalogue up to a price ceiling. The model providers and where they operate are in the Third-Party Services Policy.

13.7 Characteristics the law protects. Talgrid's search indexes and candidate ranking do not read the date of birth, gender, nationality or marital status held in the Talgrid Candidate Record, but they use resume text, which may contain such details. The Platform's screening asks every applicant a standard set of questions, which can include date of birth, gender, nationality and marital status. When the Platform generates a match report after a screening, the AI model receives every screening answer, including those. The Customer's duties in section 13.2 and clause 7.2 apply to that report.

14. Persons under eighteen

14.1 The Platform is not for anyone under eighteen. The Customer does not upload personal data of anyone under eighteen, and does not enable proctoring, recording or other monitoring of anyone under eighteen.

14.2 Talgrid may reject a record, invitation or capture for someone it has reason to think is under eighteen. This reflects section 9 of the DPDP Act.

15. The Customer's responsibilities

15.1 The Customer:

- (a) gives Talgrid only lawful instructions, and has a lawful ground under the Data Protection Laws for all Customer Data it uploads or instructs Talgrid to process, and for its own processing of each record it receives on a Reveal (clause 6.3);
- (b) gives Data Principals the notices, and obtains the consents, that its law requires from it as Data Fiduciary, except where this DPA or the Service Terms say that Talgrid presents a notice on its behalf;
- (c) provides its own channel for Data Principals' requests and grievances, and publishes the contact for it;
- (d) tells Talgrid promptly of a request, complaint or notice it receives that affects Talgrid's processing;
- (e) is responsible for the accuracy of what it uploads;
- (f) tells candidates, in the notices its law requires it to give, that it uses a platform that keeps a shared record of each candidate across the platform's customers, as section 2 describes. Talgrid's own processing of the Talgrid Candidate Record as Data Fiduciary is not processing of Customer Data for clause 12.6 (section 2.6(c)(vii)); and
- (g) tells interview participants that interviews in a Platform interview room are recorded, transcribed, summarised and scored by AI, and obtains any consent its law requires, before the interview (section 13.4).

16. Cooperation and records

16.1 Talgrid gives the Customer the information it reasonably needs about Talgrid's processing of Customer personal data to keep its own records.

16.2 If the Central Government designates the Customer or Talgrid a Significant Data Fiduciary (section 10 of the DPDP Act), each Party gives the other the cooperation it reasonably needs to meet the resulting duties, including a data protection impact assessment and an independent audit under Rule 13.

17. Changes and term

17.1 This DPA changes under clause 16.2, except that a change the law requires takes effect at once, and Talgrid gives notice as soon as practicable.

17.2 This DPA applies for as long as Talgrid processes Customer personal data, including through the Export Period and the deletion periods in section 11. Sections 2.6, 10, 11.4 and 17.3 survive.

17.3 Liability under this DPA is subject to clause 12 of the Standard Terms.