SCHEDULE 6
DATA PROCESSING INFORMATION

This Schedule 6 forms part of the Agreement between **Talent Recognition Limited** (the "Provider") and the Customer identified in the Services Order Form. It sets out the information required under Article 28(3) of the UK GDPR and, where applicable, the EU GDPR, in connection with the Provider's processing of Customer Personal Data on behalf of the Customer.

1. Categories of Data Subjects

1.1 The Customer Personal Data processed under the Agreement relates to the following categories of data subject:

Category	Description
Assessment subjects	Employees, workers, candidates, contractors and other individuals employed by or engaged with the Customer or its clients, whose images of facial morphology are submitted to the Platform for psychometric assessment.
Platform users	Employees, HR personnel, managers and administrators of the Customer who hold User Accounts on the Platform and access the Hosted Services on behalf of the Customer.
Prospects and leads	Individuals whose contact details and limited personal data are submitted by the Customer to the Prospects module of the Platform for the purposes of outreach, team invitation or pipeline management.

2. Types of Personal Data Processed

2.1 The Provider processes the following types of personal data on behalf of the Customer:

Data type	Detail	Special category?
Images of facial morphology	Images captured via webcam and submitted to the Platform's image processing API for transient processing. Deleted immediately upon generation of the derived data matrix. Not retained.	**Yes** — Biometric Data under Article 9 UK/EU GDPR
Derived numerical matrix	A 195-value numerical matrix generated from each image of facial morphology. Constitutes derived biometric data. Processed to generate OCEAN Scores.	**Yes** — derived from Biometric Data

OCEAN Scores and fit percentages	Big Five personality profile scores (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism) and role fit percentage scores derived from the numerical matrix.	Potentially — derived from biometric processing; treated as special category by the Provider.
Names and contact details	First name, last name, email address of assessment subjects and Platform users.	No
Consent records	Timestamp, subject identifier, and consent status logged by the Platform at the point of image capture where the Platform's native consent flow is used.	No
Access and activity logs	User login activity, session tokens, page access records and API call logs maintained for security, audit and support purposes.	No
Psychometric report content	Generated report text and profile narratives presented to the Customer via the Hosted Services, derived from OCEAN Scores.	Potentially — treated as special category by the Provider.

3. Purposes of Processing

3.1 The Provider processes Customer Personal Data solely for the following purposes, in each case on the documented instructions of the Customer:

(a) Generating OCEAN Scores and fit percentages from images of facial morphology submitted to the Platform.

(b) Storing and presenting psychometric assessment results, reports and derived data to the Customer and its authorised Platform users via the Hosted Services.

(c) Providing, operating, maintaining and supporting the Hosted Services in accordance with the Agreement.

(d) Managing the Customer's account, user access credentials and subscriber configuration.

(e) Logging consent at the point of image capture where the Platform's native consent workflow is used.

(f) Sending automated communications to subjects and Platform users as directed by the Customer, including assessment invitations and team notifications (where the Prospects module is activated).

(g) Maintaining security audit logs and activity records for the purposes of information security, fraud prevention and platform integrity.

(h) Complying with applicable legal obligations, including in response to lawful requests from regulators or courts.

4. Technical and Organisational Security Measures

4.1 The Provider has implemented the following technical and organisational measures to ensure a level of security appropriate to the risk of processing, in accordance with Article 32 UK GDPR:

Access control and authentication

- Multi-factor access credential system with cross-subdomain session token bridge (SessionToken and TR_Session cookies) providing authenticated access to the Platform.
- Password hashing using PBKDF2-SHA512 with 600,000 iterations and per-user salts, implemented via ASP.NET Core Identity services.
- Role-based access control enforcing separation between Customer administrator, user and subject access levels.
- JWT (JSON Web Token) authentication for API access with token expiry and revocation controls.

Data minimisation and transient processing

- Images of facial morphology are processed transiently via the image processing API. Each image is permanently deleted immediately upon generation of the derived numerical matrix. No image is retained on the Platform or by the Provider following that processing step.
- The 195-value numerical matrix is processed in memory for the generation of OCEAN Scores and is not independently stored as a separate data set.

Network and application security

- All data transmitted between users and the Platform is encrypted in transit using TLS 1.2 or above (HTTPS enforced across all subdomains).
- Centralised authentication and authorisation controls applied across all platform pages via PageInit.asp, preventing unauthenticated access to any operational page.
- CSRF (Cross-Site Request Forgery) protection tokens implemented across all state-modifying operations.
- Parameterised SQL queries throughout the Platform codebase, preventing SQL injection.
- IDOR (Insecure Direct Object Reference) validation applied to all data access operations.
- Input sanitisation and HTMLEncode applied to all user-supplied data prior to rendering.

Hosting infrastructure

- Platform hosted on managed infrastructure provided by Web Wiz Ltd (Poole, Dorset, UK), with physical security, network firewalling and DDoS mitigation controls. Web Wiz holds annual Cyber Essentials certification in accordance with NCSC requirements.

- SQL Server database hosted within the Web Wiz managed environment with restricted access credentials and connection string protection.
- PoPSY microservice infrastructure (AI scoring component) deployed on Amazon Web Services (AWS) in isolated EC2 instances within us-east-1, with separate AWS account for clean isolation.

Backup and recovery

- Daily automated backups of Customer Data maintained in accordance with Clause 12.5 of the Agreement.
- Backup restoration capability within 1 Business Day of a Customer request, in accordance with Clause 12.6 of the Agreement.

Organisational measures

- Data Protection Officer appointed: A J Silver, dpo@talent-recognition.com.
- Registered with the Information Commissioner's Office (ICO) under the UK GDPR.
- Company registration number: 12128657 (England and Wales).
- Personnel with access to Customer Personal Data are subject to confidentiality obligations as a condition of engagement.
- Security remediation programme maintained, with periodic penetration testing conducted by independent third parties.
- Privacy impact assessments conducted for high-risk processing activities.

5. Third Party Sub-Processors and Transfer Jurisdictions

5.1 The Provider is hereby authorised by the Customer to engage the following sub-processors in connection with the processing of Customer Personal Data. The Provider shall ensure that each sub-processor is subject to data processing obligations equivalent to those set out in Clause 25 of the Agreement.

Sub-processor	Role	Data processed	Jurisdiction
Web Wiz Ltd	Managed hosting provider for the Platform, database infrastructure and web server environment. Data centre located in Poole, Dorset, UK (designated Critical National Infrastructure). Company No. 05977755, registered in England & Wales.	All Customer Personal Data stored on the Platform, including OCEAN Scores, user account data and activity logs.	United Kingdom. No international transfer — UK-to-UK hosting. No transfer mechanism required.

HPPM API	Third-party webcam capture and image processing API used for the Platform's Psychometric Response Technology (PRT) image capture workflow.	Images of facial morphology at point of capture only. Images are processed transiently and not retained by the sub-processor following processing.	United Kingdom
Amazon Web Services (AWS)	Cloud infrastructure provider for the PoPSY AI scoring microservice (Portrait-oriented Personality Scoring System).	Images of facial morphology and derived numerical matrix during the scoring computation only. No personal data is retained following generation of OCEAN Scores.	United States (us-east-1). Transfers protected by the AWS Global Data Processing Addendum and UK GDPR Addendum, both automatically incorporated into the AWS Service Terms and applicable to all AWS customers processing personal data. EU SCCs (Commission Implementing Decision 2021/914) and UK IDTA apply automatically. No separate acceptance required. Current DPA: aws.amazon.com/service-terms
Brevo (formerly Sendinblue)	Email automation and transactional communications platform used for sending assessment invitations, team notifications and system emails on behalf of the Customer.	Names and email addresses of assessment subjects and Platform users to whom communications are sent.	European Union / France (Sendinblue SAS, Paris). Transfers from the UK are covered by the UK adequacy decision for EEA countries. Brevo DPA automatically incorporated into their General Conditions of Use upon account acceptance. No separate form required. Current DPA: brevo.com/legal/termsofuse

5.2 The Provider shall notify the Customer in advance of any intended addition to or replacement of a sub-processor listed in this Section 5, giving the Customer a reasonable opportunity to object to such change. Objections must be raised in writing within 10 Business Days of receipt of such notification. The parties shall cooperate in good faith to resolve any reasonable objection.

6. Processing Duration

6.1 The Provider shall process Customer Personal Data for the duration of the Agreement and, following expiry or termination of the Agreement, for a period of not more than 30 days, after which the Provider shall delete or return all Customer Personal Data in accordance with Clause 25.18 of the Agreement, subject to the anonymisation provisions in Clause 25.22(c) and to any legal obligation requiring continued retention.

6.2 Notwithstanding Clause 6.1, images of facial morphology are not subject to this retention period as they are deleted immediately upon generation of the derived data matrix in accordance with Clauses 25.21(b) and 25.22(a) of the Agreement.

6.3 Where the Customer requests anonymisation of OCEAN Scores or derived data in accordance with Clause 25.22(c) of the Agreement, anonymised data that has ceased to constitute personal data may be retained by the Provider indefinitely for statistical, research or service improvement purposes.

7. Contact and DPO Details

7.1 **Provider Data Protection Officer:** A J Silver

7.2 **DPO email:** dpo@talent-recognition.com

7.3 **ICO registration:** Talent Recognition Limited is registered with the Information Commissioner's Office.

7.4 **Company number:** 12128657 (incorporated in England and Wales)

7.5 **Data subject rights requests:** To be directed to the Customer in the first instance in accordance with Clause 25.14 of the Agreement. The Customer shall forward to dpo@talent-recognition.com any request requiring action by the Provider as data processor.

7.6 **Personal data breach reporting:** The Provider shall notify the Customer of any personal data breach affecting Customer Personal Data without undue delay and in any case within 72 hours of becoming aware of the breach, in accordance with Clause 25.16 of the Agreement. Notifications to be sent to the Customer Representative identified in Section 6 of the Services Order Form.

IN FORCE FROM March 2026

This Schedule 6 should be read alongside and forms part of the Agreement between the parties.