Talent Recognition Limited

Biometric Data & Privacy Policy

Version 1.0 | Effective date: March 2026

1 INTRODUCTION

Talent Recognition Limited ("TRL", "we", "us") is committed to protecting the privacy and biometric data of every individual who interacts with our platform. This policy explains specifically how we collect, process, store, and delete biometric data in connection with our PoPSY personality assessment technology.

This policy applies to all users of the Talent Recognition and ProMind Insight platforms and supplements our main Privacy Policy. Where this policy conflicts with the main Privacy Policy on matters of biometric data, this policy takes precedence.

2 WHAT BIOMETRIC DATA WE COLLECT

When you use our personality assessment feature, our platform captures a short series of facial images via your device's camera. From these images, PoPSY — our proprietary Portrait-oriented Personality Scoring System — analyses your facial morphology (the geometric structure, proportions, and spatial relationships of facial features) to generate a personality profile.

The biometric data we collect comprises:

- Facial images: a small number of photographs captured during the assessment session
- Facial geometry: spatial measurements and proportions derived from those images during processing

We do not collect fingerprints, retinal scans, voiceprints, or any other category of biometric identifier.

3 PURPOSE OF COLLECTION

We collect and process biometric data for one purpose only: to generate your OCEAN Big Five personality profile. The OCEAN model measures Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism — five scientifically validated dimensions of personality.

Your biometric data is not used for:

- Identity verification or authentication
- Marketing, advertising, or profiling for commercial purposes
- Any purpose other than personality score generation as described above

4 HOW POPSY PROCESSES YOUR DATA

PoPSY is our own proprietary AI microservice. It operates as follows:

- Your facial images are captured by your device and transmitted securely (encrypted in transit via TLS) to the PoPSY processing engine.
- PoPSY analyses the facial geometry within those images and computes your personality scores.
- Your facial images and facial geometry data are deleted immediately upon completion of the analysis. This deletion is automatic and permanent.
- The resulting OCEAN personality scores — five numerical values representing personality dimensions — are retained as your assessment results. These scores do not constitute biometric data; they are derived personality metrics that cannot be used to identify you or reconstruct your facial images.

Key point: We do not store your facial images. We do not store facial geometry data.

Biometric data is deleted automatically the moment processing is complete.

What is retained is your personality profile (OCEAN scores) — not your biometrics.

5 RETENTION AND DESTRUCTION SCHEDULE

Our retention periods for biometric data are as follows:

Data Type	Retention Period	Destruction Method
Facial images	Deleted immediately after processing (seconds)	Automatic permanent deletion on processing completion
Facial geometry (intermediate)	Deleted immediately after processing (seconds)	Automatic permanent deletion on processing completion
OCEAN personality scores (non-biometric)	Duration of your account or as agreed with your organisation	Account deletion or on written request

This retention schedule meets or exceeds the requirements of the Illinois Biometric Information Privacy Act (BIPA), which mandates destruction of biometric data no later than three years after collection or when the purpose is satisfied (whichever occurs first). Our immediate deletion policy satisfies this requirement at the point of collection.

6 THIRD-PARTY DISCLOSURE

Your facial images are transmitted to PoPSY, Talent Recognition Limited's own proprietary processing microservice, for the sole purpose of generating your personality scores. PoPSY operates within our secure cloud infrastructure hosted on Amazon Web Services (AWS).

We do not sell, lease, trade, or otherwise profit from your biometric data. We do not disclose your biometric data to any third party except:

- AWS, as our cloud infrastructure provider, who process data on our behalf under appropriate data processing agreements
- As required by law or valid legal process

No other third-party disclosure of biometric data occurs.

7 SECURITY MEASURES

We apply a standard of care consistent with how we protect our own confidential information. Specifically:

- All data transmission is encrypted in transit using TLS
- Our platform is hosted on AWS, which maintains ISO 27001 certification and SOC 2 compliance
- Access to biometric processing systems is restricted to authorised personnel only
- We maintain comprehensive audit logs of all data processing events

8 CONSENT

Before any facial image is captured, you are presented with a clear consent notice at the point of collection. Your assessment will not proceed without your explicit agreement. You may withdraw consent at any time prior to the assessment commencing.

For users in Illinois or other US states with biometric privacy legislation, the consent mechanism at the point of capture constitutes the written informed consent required under applicable state law.

9 YOUR RIGHTS

Depending on your jurisdiction, you may have the following rights in relation to your data:

- Right to be informed: you have the right to know what data we hold about you
- Right of access: you may request a copy of your personal data
- Right to erasure: you may request deletion of your account and associated personality scores
- Right to object: you may object to processing of your data
- Right to complain: UK and EU residents may complain to the Information Commissioner's Office (ICO) or their local supervisory authority

As your facial images and biometric geometry are deleted immediately upon processing, there is no biometric data to access, correct, or delete after the assessment completes.

10 REGULATORY COMPLIANCE

Talent Recognition Limited is registered with the Information Commissioner's Office (ICO) as a data controller under UK GDPR. Our processing of biometric data is conducted in accordance with UK GDPR Article 9 (special category data), relying on explicit consent as the lawful basis.

Our compliance position across key frameworks:

Framework	Status
UK GDPR (ICO registered)	☑ Compliant — explicit consent, immediate deletion, ICO registered
EU GDPR	☑ Compliant — aligned to UK GDPR standards
Illinois BIPA	☑ Compliant — written consent, immediate deletion exceeds 3yr requirement, no sale of biometric data, public policy published
POPIA (South Africa)	☑ Ready — consent-driven, purpose-limited, AWS infrastructure
CCPA/CPRA (California)	☑ Addressed — no sale of personal data, deletion rights honoured

11 CONTACT AND DATA CONTROLLER DETAILS

If you have any questions about this policy or wish to exercise your rights, please contact:

Data Controller: Talent Recognition Limited

Company No.: 12128657

Registered Office: Brockley Place, Bury St. Edmunds, IP29 4AG, United Kingdom

Data Protection Officer: Anthony Silver

Email: privacy@talent-recognition.com

ICO Registration: Registered Data Controller

12 UPDATES TO THIS POLICY

We may update this policy from time to time to reflect changes in our technology, legal obligations, or best practice. The effective date at the top of this document will be updated accordingly. We will notify registered users of material changes via the platform or by email.