

WHARTON GLOBAL PRIVACY POLICY

Date: August 2026

1. Purpose and Scope

Wharton Global Limited is committed to protecting the privacy and personal data of everyone we work with and to handling personal information responsibly, transparently and securely.

As an occupational psychology consultancy, we process personal data in the delivery of assessment, recruitment, coaching, leadership development and organisational consultancy services. We recognise that some of the information entrusted to us is sensitive and that maintaining confidentiality and trust is fundamental to our professional practice.

This policy sets out our approach to data protection, the principles we follow when processing personal data and the responsibilities of those working for or on behalf of Wharton Global.

This policy applies to everyone working for or on behalf of Wharton Global, including employees, directors, contractors, consultants, associates, temporary workers, interns, agents and other third parties acting on our behalf.

This policy should be read alongside our other relevant policies and procedures relating to information security, confidentiality, data retention and the handling of personal information.

2. Data Protection Principles

Wharton Global processes personal data in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We are committed to ensuring that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary for those purposes.
- Accurate and, where necessary, kept up to date.

- Retained for no longer than necessary.
- Protected through appropriate technical and organisational measures.
- Processed in a way that enables us to demonstrate compliance with our responsibilities.

Where our activities are subject to additional applicable data protection requirements, we will take appropriate steps to comply with those requirements.

3. Our Approach

Trust and confidentiality are central to Wharton Global's work.

We are committed to:

- Being clear about why we collect personal data and how it will be used.
- Processing only the personal data reasonably required for a legitimate business or professional purpose.
- Identifying an appropriate lawful basis for processing personal data.
- Applying appropriate additional safeguards where special category personal data is processed.
- Respecting the rights of individuals in relation to their personal data.
- Protecting personal data against unauthorised access, disclosure, loss or misuse.
- Sharing personal data only where there is an appropriate reason to do so.
- Working with reputable third-party providers and applying appropriate contractual and security safeguards.
- Maintaining appropriate retention and deletion arrangements.
- Reviewing and improving our data protection practices as our organisation, services and technology develop.

4. Our Role and Responsibilities

Wharton Global's role under data protection legislation will depend on the nature of the activity or client engagement.

For our own business activities, Wharton Global Limited will generally act as the data controller and determine why and how personal data is processed.

Privacy Policy

Owner: Commercial Director

Date: August 2026

Where we provide assessment, coaching, leadership development or other professional services on behalf of a client organisation, our role will depend on the circumstances of the engagement. In some cases, the client organisation will determine the purposes of the processing and Wharton Global will process personal data on its behalf. In other circumstances, Wharton Global may act as an independent data controller or, where appropriate, a joint controller.

We will establish our responsibilities as part of the relevant engagement and put appropriate contractual arrangements in place where required.

Individuals participating in our professional services will be provided with appropriate information about how their personal data will be processed.

5. Personal Data We Process

The personal data processed by Wharton Global will depend on the nature of our relationship with an individual and the services being provided.

This may include:

- Contact and identification information.
- Client and business contact information.
- Employment and professional information.
- CVs, applications and recruitment information.
- Interview and assessment information.
- Psychometric assessment responses, scores and reports.
- Professional observations and notes.
- Coaching and development information.
- Communications and correspondence.
- Information required to administer client engagements and professional services.
- Information required to meet contractual, legal, regulatory or professional obligations.

We will only collect and process information that is appropriate for the purpose for which it is required.

6. Special Category Personal Data

Some of our professional activities may involve special category personal data, including information relating to health, disability or reasonable adjustments.

Where special category personal data is processed, Wharton Global will ensure that both an appropriate lawful basis under Article 6 UK GDPR and an applicable condition under Article 9 UK GDPR are identified.

We will apply appropriate safeguards to the collection, access, use, sharing, retention and deletion of this information.

We will not assume that all psychometric or assessment information is special category personal data. Where assessment information does contain or reveal special category information, it will be handled accordingly.

7. Assessment and Psychometric Data

Psychometric assessment is an important part of Wharton Global's professional practice, and we recognise the particular responsibility associated with information generated through assessment.

Individuals participating in an assessment will be provided with appropriate information about the processing of their personal data, including the purpose of the assessment, how their information will be used, who may receive the results and how long relevant information will be retained.

Access to assessment information will be restricted to individuals who have a legitimate professional or operational reason to access it.

Assessment results are intended to support professional decision-making and do not replace human judgement.

Where assessment information is used to inform recruitment, selection, development or other decisions, results will be interpreted by appropriately qualified practitioners and considered alongside other relevant information and professional judgement.

8. Lawful Basis for Processing

Wharton Global will ensure that an appropriate lawful basis is identified for each activity involving personal data.

Depending on the circumstances, this may include:

- Consent.

- Performance of a contract or taking steps before entering into a contract.
- Compliance with a legal obligation.
- Legitimate interests, where our interests or those of a third party are not overridden by the rights and freedoms of the individual.
- Other lawful bases where applicable.

Where we rely on legitimate interests, we will consider whether the processing is necessary and proportionate and whether the interests or rights of the individual require additional safeguards.

Where processing relies on consent, that consent must be freely given, specific, informed and capable of being withdrawn.

9. Transparency and Privacy Information

Wharton Global will provide individuals with appropriate information about how their personal data is processed.

The information provided will be proportionate to the nature of the interaction and may form part of an assessment invitation, participant information, client documentation, recruitment process, privacy notice or other relevant communication.

Our website has a separate Website Privacy Notice explaining how personal data is collected and processed through the Wharton Global website, including information submitted through website forms and the use of cookies, analytics and similar technologies.

10. Sharing Personal Data

Personal data will only be shared where there is a legitimate and appropriate reason to do so.

Depending on the circumstances, this may include sharing information with:

- Clients or organisations commissioning our services.
- Assessment platform providers and psychometric publishers.
- Associates, consultants or subcontractors involved in delivering an engagement.
- IT, cloud, software and other service providers processing information on our behalf.
- Professional advisers.
- Regulatory authorities or professional bodies.

- Courts, law enforcement agencies or other authorities where required by law.

We do not sell personal data.

Where a third party processes personal data on our behalf, we will take proportionate steps to assess the provider and ensure that appropriate contractual, confidentiality and security arrangements are in place.

11. International Data Transfers

Some of our clients, professional partners and service providers may operate or store information outside the United Kingdom.

Where personal data is transferred outside the UK, Wharton Global will ensure that the transfer complies with applicable data protection legislation.

Where required, appropriate safeguards may include UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or another legally recognised transfer mechanism.

We will take a proportionate approach to assessing international transfers and the safeguards required.

12. Data Retention

Wharton Global will retain personal data only for as long as there is a legitimate business, professional, contractual or legal reason to do so.

Retention periods will take into account:

- The purpose for which the information was collected.
- The nature of the client engagement or relationship.
- Contractual requirements.
- Legal and regulatory obligations.
- Relevant professional standards.
- The need to establish, exercise or defend legal claims.

Different categories of information may therefore be subject to different retention periods.

Retention arrangements will be documented and reviewed periodically. Personal data that is no longer required will be securely deleted, destroyed or anonymised as appropriate.

13. Data Subject Rights

Wharton Global respects the rights individuals have in relation to their personal data.

Depending on the circumstances, these may include the right to:

- Be informed about how personal data is processed.
- Request access to personal data.
- Request correction of inaccurate or incomplete information.
- Request erasure of personal data in certain circumstances.
- Request restriction of processing.
- Object to certain processing.
- Request data portability where applicable.
- Withdraw consent where processing relies on consent.
- Be protected from certain decisions based solely on automated processing.
- Raise a complaint about the processing of personal data.

Requests relating to personal data should be directed to hello@wharton.global.

We will respond to requests within the timescales required by applicable data protection legislation.

14. Automated Decision-Making

Some of the assessment tools used in our professional services may generate scores, reports, profiles or other outputs through automated processing.

These outputs support professional assessment and decision-making but do not replace professional judgement.

Wharton Global does not make decisions that produce legal or similarly significant effects on an individual based solely on automated processing.

15. Information Security

Privacy Policy

Owner: Commercial Director

Date: August 2026

Wharton Global maintains appropriate technical and organisational measures designed to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, alteration or disclosure.

Measures may include:

- Access controls and permissions based on business need.
- Unique and individually authenticated user accounts.
- Appropriate encryption.
- Secure systems and backups.
- Confidentiality obligations.
- Appropriate physical security.
- Data protection and information security training.
- Security requirements and contractual safeguards for relevant third-party providers.

Our information security arrangements are reviewed periodically and developed in proportion to the nature of the information we hold and the risks associated with its processing.

16. Personal Data Breaches

Everyone working for or on behalf of Wharton Global must report an actual or suspected personal data breach promptly so that appropriate action can be taken.

Wharton Global will assess reported incidents, take appropriate steps to contain and remediate them and maintain appropriate records.

Where a personal data breach meets the relevant legal threshold, we will notify the Information Commissioner's Office within the required timeframe and will notify affected individuals where required.

17. Third-Party Providers

Wharton Global uses a range of professional, assessment and technology providers to support our work.

We will take reasonable and proportionate steps to ensure that providers entrusted with personal data have appropriate data protection and information security arrangements.

Where a provider processes personal data on our behalf, appropriate contractual terms will be put in place as required.

Our use of individual providers may change over time, and we will review relevant arrangements as part of our ongoing data protection and supplier management activities.

18. Training and Awareness

Everyone working for or on behalf of Wharton Global who handles personal data is expected to understand and comply with their data protection responsibilities.

Wharton Global will provide appropriate data protection and information security training and guidance, with additional information where an individual's responsibilities involve sensitive or higher-risk personal data.

19. Responsibility for the Policy

The Directors of Wharton Global have overall responsibility for data protection and privacy.

Day-to-day ownership of this policy sits with Natasha Addis, who is responsible for coordinating data protection compliance, maintaining relevant policies and procedures and supporting the review of Wharton Global's data protection arrangements.

Everyone working for or on behalf of Wharton Global is responsible for complying with this policy and protecting personal data accessed or processed as part of their role.

20. Reporting Concerns

Any actual or suspected breach of this policy, inappropriate handling of personal data or other data protection concern should be reported promptly.

Concerns can be raised with:

- Your line manager.
- The Managing Partner.

Concerns relating to an individual's own personal data can be directed to hello@wharton.global.

Individuals also have the right to raise concerns with the Information Commissioner's Office where applicable.

21. Policy Review

This policy will be reviewed at least annually, and earlier where there is a significant change to our operations, professional services, relevant legislation or the way we process personal data.

Our data protection arrangements will continue to be reviewed and developed as our business, technology and professional practices evolve.

22. Approval

Document Owner	Natasha Addis, Commercial Director
Approved by	Neville Wharton, Managing Partner