

Privacy Policy

Last updated: January 1, 2025

At Avenir Holdings Pte Ltd, we take your privacy seriously. This Privacy Policy explains how we collect, use, and protect your personal data when you use QQ-assessments, our tool for evaluating intangible assets and liabilities.

1. Who We Are

Avenir Holdings Pte Ltd
10 Anson Road #13-11
International Plaza
Singapore 079903

Registered in Singapore

Contact: info@avenirholdings.com

2. What Data We Collect

When you use QQ-assessments, we may collect:

- Identification details (e.g. name, email, organization)
- Assessment inputs (your responses to questions)
- Assessment results (generated reports and insights)
- App usage data (timestamps, device type, interaction patterns)
- Information shared during consultancy or mentoring sessions (e.g., verbal insights, written notes, or supplementary documentation provided by you or your organization in relation to QQ-assessments)

We do not collect sensitive personal data (e.g. racial, religious, biometric) unless explicitly stated and consented.

3. Why We Process Your Data

We use your data based on the following legal bases:

- Contractual necessity – To deliver assessment results to you.
- Legitimate interest – To improve our tools, securely manage the platform, and provide relevant insights.
- Consent – When sharing results with third parties (e.g., coaches or organizational sponsors).

4. How We Use Your Data

Your data helps us to:

- Generate accurate and personalized assessments
- Deliver your results and reports
- Support self-awareness and team development processes
- Maintain and improve the QQ-assessments platform
- Generate anonymized statistics to enhance our tools
- Honor confidentiality of insights shared during consultancy or mentoring interactions, whether recorded digitally or noted manually, in accordance with data protection and professional ethics standards

We do not sell your personal data to third parties.

5. Who Can Access Your Data

- You – Full access and control over your results.
- Authorized professionals (e.g. coaches or internal sponsors) – Only with your explicit consent.
- Our internal team – For support and maintenance purposes under confidentiality.
- Trusted service providers – For secure hosting and analytics, under GDPR-compliant agreements

6. How We Protect Your Data

We use strong security practices, including:

- Encryption (data in transit and at rest)
- Access control and authentication mechanisms
- Secure infrastructure hosted in GDPR-compliant environments

7. Your Rights Under GDPR

You can, at any time:

- Access your data
- Correct inaccurate information
- Delete your data (“right to be forgotten”)
- Restrict or object to processing
- Request a copy of your data (portability)
- Withdraw consent where applicable

Contact us at info@avenirholdings.com to exercise these rights.

8. Data Retention

We retain your data only as long as necessary to fulfill the purpose of the assessment or as legally required. You can request deletion at any time.

9. Confidentiality of Consultancy and Advisory Data

In addition to data collected through the app, we may receive confidential information through direct communication—such as during consultancy, mentoring, or feedback sessions.

This data may include opinions, organizational challenges, leadership dynamics, or strategic observations.

Such information is:

- Treated with strict confidentiality
- Not shared without your consent
- Stored securely if documented
- Processed only to support the purpose of the engagement

We apply the same data protection principles (security, minimization, retention, and access control) to this data as we do to app-based information.

10. Changes to This Policy

We may occasionally update this Privacy Policy. We'll notify you of any significant changes via the app or by email.

11. Contact Us

For privacy questions or to exercise your rights, contact our Data Protection Officer:

Email: info@avenirholdings.com

Mail: Avenir Holdings Pte Ltd, 10 Anson Road #13-11, International Plaza, Singapore 079903

You also have the right to contact your local Data Protection Authority.