Policy title:	**GDPR Compliance Policy**

Summary:	Insight Psychological Assessments Ltd is committed to protecting the privacy, confidentiality, and security of personal data in accordance with the General Data Protection Regulation (GDPR). The policy outlines how the company collects, processes, stores, and safeguards personal information from clients, employees, and third parties.
Target audience:	All Insight Assessments '*team members*', whether employed, contracted or part-time, paid or unpaid, volunteers, students, and contractors.
Authorised by:	Insight Psychological Assessments Ltd Director
Date issued:	1st September 2025
Next review date:	31st August 2026

Version no.	Issue date	Summary of amendments

1. Purpose

This policy outlines how Insight Psychological Assessments Ltd ("the Company", "we", "our", or "us") ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 in the processing of personal and special category data, particularly that of clients undergoing psychological assessment or therapy.

2. Scope

This policy applies to:

- All employees, associates, contractors, and interns of the Company
- All personal data processed in the course of business
- All systems used to process, store, or transmit personal data

It covers data processed in clinical assessments, therapy, administration, research, and communications with service users.

3. Data Protection Principles

We adhere to the following UK GDPR principles:

1. **Lawfulness, Fairness, and Transparency**
2. **Purpose Limitation**
3. **Data Minimisation**
4. **Accuracy**
5. **Storage Limitation**
6. **Integrity and Confidentiality (Security)**
7. **Accountability**

4. Lawful Basis for Processing

We process personal data under the following lawful bases:

Type of Data	Lawful Basis	Description
General Client Data	Contract	Necessary for delivering psychological assessments and services
Special Category Data (e.g. mental health info)	Explicit Consent	Obtained in writing before assessments or therapy begins
Employee Data	Legal Obligation / Contract	For employment and payroll obligations
Marketing (e.g. newsletters)	Consent	Opt-in required, with the option to withdraw

5. Types of Data We Process

- **Personal data**: Names, addresses, dates of birth, contact information
- **Special category data**: Mental health history, psychological test results, medical reports

6. Data Subject Rights

Under the UK GDPR, individuals have the right to:

1. Be informed about data collection and use
2. Access their personal data
3. Rectify inaccurate or incomplete data
4. Erase data (right to be forgotten)
5. Restrict processing
6. Data portability
7. Object to processing
8. Not be subject to automated decision-making without human involvement

Clients and staff may submit a request by emailing: **hello@insightassessments.co.uk**. We will respond within **30 calendar days**.

7. Data Retention

We retain client records and clinical notes for **7 years** from the date of last contact (or until the client reaches age 25, whichever is later), in line with **BPS** and **HCPC** guidance.

Employee data is retained for up to **6 years** after termination of employment.

8. Data Security

We implement appropriate technical and organisational measures, including:

- Encrypted storage (at rest and in transit)
- Access control and role-based permissions
- Secure email systems (e.g., Microsoft 365 with MFA)
- Data breach detection and response procedures
- Device encryption and remote-wipe capabilities

INSIGHT ASSESSMENTS

9. Data Sharing and Third Parties

We do **not sell** personal data.

We may share data with:

- Referring professionals (e.g., GPs, psychiatrists) — with consent
- Legal representatives — upon request and legal obligation
- IT service providers — under strict data processing agreements (DPAs)
- Regulators (e.g., ICO, HCPC) — when legally required

All third-party processors are GDPR-compliant and subject to written agreements.

10. International Transfers

All personal data is stored and processed within the **UK** or countries deemed "adequate" by the UK government. If any transfer outside these regions is necessary, we will ensure that appropriate safeguards (e.g., Standard Contractual Clauses) are in place.

11. Children's Data

When working with children and young people under 16, we obtain **parental or guardian consent** before processing. All information is handled with additional care and confidentiality.

12. Data Protection Officer (DPO)

Where required, we appoint a DPO or internal compliance lead. For all data protection queries, contact:

Data Protection Leadership and Accountability

The company recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. To ensure compliance, clear accountability for data protection is maintained.

- The company director is designated as the Data Protection Lead and holds overall responsibility for ensuring that personal data is processed lawfully, fairly, securely, and in accordance with applicable legislation.

- The Data Protection Lead is responsible for monitoring compliance with data protection policies, ensuring staff and consultants are aware of their obligations, and acting as the point of contact for any data protection queries or concerns.

- To support this role, the company engages external specialists in IT security and data protection to provide technical expertise, undertake audits, and advise on best practice. These specialists do not assume legal accountability, which remains with the company director, but provide assurance that standards are maintained.

- All employees and self-employed consultants are required to co-operate with the Data Protection Lead and to follow company policies and procedures when handling personal data.

- Where the use of external Data Protection Officer services becomes necessary under UK GDPR, the company will formally appoint a qualified provider and notify relevant supervisory authorities as required.

Data Protection Lead
Insight Psychological Assessments Ltd
Email: hannah@insightassessments.co.uk

13. Data Breach Policy

In the event of a data breach:

- The breach will be investigated immediately
- The ICO will be notified within **72 hours** (if risk to data subjects is likely)
- Affected individuals will be informed where there is a high risk to their rights and freedoms
- Breaches will be recorded and reviewed for future prevention

14. Training and Awareness

Responsibilities for Employees and Self-Employed Consultants

The company requires both employees and self-employed consultants to comply with IT security, data protection, and professional standards. The scope of responsibilities differs according to employment status, as set out below.

Employees

Employees are required to:

- Complete GDPR and data protection training during induction and take part in mandatory annual refresher training provided by the company.
- Follow company policies and procedures for IT security, data handling, and confidentiality.
- Use company-approved systems and devices for processing personal and clinical data.
- Report any suspected or actual data breach or IT incident to the Data Protection Lead without delay.
- Participate in company-organised audits, compliance checks, and training sessions as instructed.

Self-Employed Consultants

Self-employed consultants are required to:

- Complete GDPR and data protection training as part of their professional induction into company work, and maintain records of completion.

- Undertake annual refresher training at their own cost and initiative, and provide evidence of this to the company on request.

- Ensure they are familiar with and apply professional guidance for handling clinical and sensitive data, including digital and AI tools where relevant.

- Use secure devices and systems, maintaining up-to-date antivirus protection, firewalls, and strong authentication measures.

- Store and transfer company data only via approved or encrypted methods.

- Immediately report any actual or suspected data breach, loss of data, or IT security incident to the company's Data Protection Lead.

- Co-operate with any investigation into data protection or IT incidents affecting company work.

- Remain accountable for their own compliance and be able to evidence this at any time if requested by the company, clients, or regulators.

15. Policy Review

This policy is reviewed **annually**, or sooner if:

- There are significant changes in the law
- There is a security incident or data breach
- New systems or services are introduced