Genius Within C.I.C.

Data Processing Addendum (DPA)

Last Updated: 23 July 2026

URL: https://geniuswithin.org/dpa

Table of Contents

DPA Terms 1

Appendix 1 - Details of Processing 5

Appendix 2 - Technical and Organisational Measures 6

Appendix 3 - Subprocessor List 7

Appendix 4 - Retention and Deletion 8

DPA Terms

1. Scope and Application

- This Data Processing Addendum ("DPA") applies where GENIUS WITHIN C.I.C. ("Licensor", "Supplier", "we", or "us") processes Licensee Data as a Processor on behalf of the customer or organisation ("Licensee", "Organisation", or "you") in connection with Digital Services (including Genius Finder Pro® platform hosting, account administration, dashboard generation, eLearning platforms, and digital support) under the Genius Within Master Services Agreement or Standard Terms and Conditions.
- This DPA does not apply to activities for which Genius Within acts as an Independent Controller (such as individual workplace coaching, workplace needs assessments, diagnostic/psychological assessments, or clinical reports where Genius Within staff exercise independent professional judgment).

2. Recitals and Roles

- **Controller / Processor Roles:** The Licensee, acting as Controller, determines the purposes and means of processing Licensee Data. Genius Within, acting as Processor, processes Licensee Data for the purpose of providing the Digital Services and otherwise on the documented instructions of the Licensee.

- **Compliance**: Both parties agree to this DPA to document their respective obligations for Licensee Data in compliance with Applicable Data Protection Legislation

(including the UK GDPR, Data Protection Act 2018, PECR, and the Data (Use and Access) Act 2025).

3. Definitions

In this DPA, the terms Applicable Data Protection Legislation, Licensee Data, Personal Data, Controller, Processor, Processing, Data Subject, Subprocessor, Special Category Data, and Technical and Organisational Measures (TOMs) have the meanings given in Applicable Data Protection Legislation or the main Agreement.

- **Data Breach:** Any event that results or may result in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Licensee Data transmitted, stored or otherwise processed.

4. Processor Obligations

Genius Within shall:

- Process Licensee Data only in compliance with Applicable Data Protection Legislation and this DPA;
- Process Licensee Data only on the documented instructions of the Licensee, including with regard to transfers outside the UK, unless required by UK law to which Genius Within is subject;
- Inform the Licensee if, in Genius Within's opinion, an instruction infringes Applicable Data Protection Legislation, without providing legal advice;
- Ensure that personnel authorised to process Licensee Data are subject to appropriate confidentiality obligations;
- Implement and maintain appropriate TOMs to protect Licensee Data in accordance with Article 32 UK GDPR and Appendix 2;
- Maintain records of processing activities where required by Applicable Data Protection Legislation; and
- Not sell Licensee Data or use it for purposes unrelated to providing, securing, supporting or lawfully improving the Digital Services, except for truly anonymised data.

5. Special Category Data

The Licensee acknowledges that Digital Services may process Special Category Data where users provide information relating to neurodivergence, disability, health, mental health, assessment outcomes or adjustment needs. The Licensee, as Controller, is responsible for identifying and documenting the Article 6 lawful basis, Article 9 condition, any DPA 2018 Schedule 1 condition, and any Appropriate Policy Document (APD) required for such

processing. Genius Within shall process such data only as Processor under this DPA unless otherwise stated in the Agreement or applicable privacy notice.

6. **Data Subject Rights & Assistance**

Genius Within shall assist the Licensee, taking into account the nature of the processing and the information available to Genius Within, by appropriate TOMs and reasonable cooperation to fulfil the Licensee's obligations to respond to Data Subject rights requests. Genius Within shall promptly notify the Licensee if it receives a request relating to Licensee Data, unless prohibited by law.

7. **Security, DPIAs and Regulatory Cooperation**

Genius Within shall provide reasonable assistance to enable the Licensee to comply with obligations relating to security, breach notification, Data Protection Impact Assessments (DPIAs), and prior consultation with the ICO where required, taking into account the nature of processing and information available. Reasonable assistance outside standard support may be chargeable at Genius Within's then-current rates unless required because of Genius Within's breach.

8. **International transfers**

Genius Within shall not transfer Licensee Data outside the UK unless the Licensee has been notified in advance and an appropriate UK GDPR transfer mechanism is in place, such as adequacy regulations, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (SCCs), or another lawful transfer mechanism. Remote access from outside the UK is treated as a transfer for these purposes where required by law.

9. **Appointment of Subprocessors**

The Licensee gives Genius Within general written authorisation to appoint Subprocessors for the provision of the Digital Services, subject to this clause and Appendix 3. Genius Within shall inform the Licensee of intended changes concerning the addition or replacement of Subprocessors, thereby giving the Licensee the opportunity to object on reasonable data protection grounds before the change takes effect.

Genius Within shall enter into a written agreement with each Subprocessor imposing data protection obligations equivalent to those required by Article 28(3) UK GDPR and this DPA. Genius Within remains fully liable to the Licensee for the performance of each Subprocessor's data protection obligations.

If the Licensee reasonably objects to a new or replacement Subprocessor on data protection grounds, the parties shall work in good faith to resolve the objection. If no reasonable resolution is available, the Licensee may terminate the affected Digital Services on written

notice, subject to payment for Services provided up to termination and non-cancellable costs.

10. **Audit Rights**

Genius Within shall provide information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits or inspections by the Licensee or an auditor mandated by the Licensee, on reasonable prior notice, no more than once per year unless required by the ICO, another regulator, a Data Breach, or a material suspected breach. Audits shall be conducted during Business Days, subject to confidentiality, security, and health and safety requirements, and without material disruption to Genius Within's business.

Genius Within may redact confidential, commercially sensitive, or third-party information from audit materials where the redaction does not prevent the Licensee from verifying compliance. The parties shall prefer provision of independent audit reports, security summaries, certifications, policies, or completed questionnaires where these reasonably satisfy the audit objective.

11. **Data Breach Notification**

Genius Within shall notify the Licensee without undue delay and, where practicable, within twenty-four (24) hours after becoming aware of a Data Breach affecting Licensee Data. The notice shall include reasonable details then available, including the nature of the breach, categories and approximate number of affected Data Subjects and records where known, likely consequences, measures taken or proposed, and a contact point for further information.

Genius Within shall provide regular updates as information becomes available, maintain a log of Data Breaches including facts, effects, and remedial action, and provide reasonable assistance to enable the Licensee to comply with Articles 33 and 34 UK GDPR and equivalent requirements.

12. **Return and Deletion of Data**

On expiry or termination of the relevant processing, Genius Within shall, at the Licensee's choice, delete or return Licensee Data and delete existing copies unless UK law requires storage or retention is otherwise permitted by the Agreement. Practical deletion from backups may occur on the next scheduled backup deletion/destruction cycle, provided the data is put beyond ordinary use and protected until deletion.

The Licensee shall request return/export of Licensee Data within thirty (30) days after termination unless another period is stated in the Order. After the export window, Genius Within may delete Licensee Data in accordance with Appendix 4.

13. **Anonymised Data**

Genius Within may retain aggregated and anonymised data that does not identify the Licensee, any Client, or any individual, for benchmarking, service improvement, research,

product development, and analytics. Genius Within shall apply safeguards against re-identification, including aggregation thresholds and suppression where appropriate. Pseudonymised data is not anonymised data and remains subject to this DPA where it is Licensee Data.

14. **Governing law and Jurisdiction**

This DPA shall be governed by and construed in accordance with the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction over any claim or matter arising out of or in connection with this DPA.

Appendix 1 - Details of Processing

Subject matter	Processing of Licensee Data in connection with the provision, administration, support, security and improvement of Digital Services under the Agreement, including Genius Finder Pro® where ordered.
Duration	The Subscription Term and any post-termination export/deletion period. Unless otherwise agreed, the Licensee may request export for 30 days after termination and deletion will occur in accordance with Appendix 4.
Nature of processing	Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, analysis, aggregation, anonymisation, disclosure by transmission, restriction, deletion and destruction.
Purpose of processing	To provide user accounts, platform access, individual strategy outputs, suggested adjustments, dashboards, analytics, reports, support, troubleshooting, security monitoring, audit logging, account administration and lawful service improvement.
Categories of Data Subjects	Employees, workers, contractors, applicants/candidates, managers, administrators, HR users, referrers, broker/customer staff and other individuals authorised or referred by the Licensee.
Types of Personal Data	Name, work email, role, department, team, organisation, line manager/referrer details, account identifiers, authentication metadata, access logs, IP address/device/browser metadata, support ticket content, questionnaire responses, self-reported workplace challenges, strengths, adjustment preferences, report/results data, usage data, dashboard data and audit logs.
Special Category Data	Where supplied by or about a user: data concerning health, disability, neurodivergence, mental health, diagnostic information, assessment outcomes, reasonable adjustment needs, workplace support needs and related free-text information.

Sensitive non-special-category data	Employment context, performance support needs, workplace difficulties, role/team data, manager/referrer information and free-text responses that may be sensitive in context.
Processing locations	Primarily United Kingdom, including AWS London (currently eu-west-2) where applicable. Any additional location or remote access arrangement must be documented in Appendix 3, the Order or a written subprocessor notice.
Subprocessors	See Appendix 3.
Aggregation / anonymisation	Organisation dashboards and analytics shall use aggregation, anonymisation or pseudonymisation appropriate to the use case. Unless otherwise agreed, small groups below 10 individuals or rare combinations that risk re-identification shall be suppressed.
Retention	See Appendix 4. Retention periods are to be confirmed before signature if the Organisation requires specific periods.
TOMs	See Appendix 2.

Appendix 2 - Technical and Organisational Measures

Measure	Description
Access control	Role-based access controls, least privilege, unique user accounts, access approval/removal procedures and periodic access review for systems processing Licensee Data.
Authentication	Password controls for users and administrators. Multi-factor authentication for privileged/admin access where available and appropriate.
Encryption	Encryption in transit using TLS/HTTPS where supported. Encryption at rest for hosted platform databases/storage where supported by the hosting provider.
Logging and monitoring	Administrative access logs, system/security logs and monitoring proportionate to the Digital Services, with investigation of suspicious activity.
Segregation	Logical segregation of customer data within hosted systems where applicable and controls to prevent unauthorised cross-customer access.
Backups and resilience	Commercially reasonable backup and restoration arrangements. Specific backup frequency, RTO/RPO and restore testing commitments must be stated in the Statement of Work if required.
Vulnerability and patch management	Reasonable processes for applying security patches, addressing vulnerabilities and maintaining supported infrastructure and software components.
Secure development/change control	Change control for material platform changes, review/testing before release where appropriate, and assessment of security/data protection impacts for significant changes.

Measure	Description
Incident response	Incident identification, escalation, containment, investigation and remediation processes, including Data Breach notification in accordance with Section 11 of this DPA.
Staff confidentiality and training	Personnel with access to Licensee Data are subject to confidentiality obligations and receive appropriate data protection/security awareness training.
Physical security	Physical security is provided by office controls and hosting provider data centre controls, as applicable.
Supplier management	Subprocessor due diligence and written Article 28-equivalent contractual obligations for Subprocessors processing Licensee Data.
Data minimisation	Processing limited to data reasonably necessary to provide and support the Digital Services and comply with legal obligations.
Deletion and disposal	Secure deletion or return of Licensee Data in accordance with Section 12 and Appendix 4 of this DPA. Backups overwritten on scheduled cycles.
Business continuity	Commercially reasonable continuity arrangements proportionate to the Digital Services. Enhanced commitments must be specified in a separate Statement of Work.

Appendix 3 - Subprocessor List

Subprocessor	Service provided	Location	Processing purpose	Safeguards / transfer mechanism
Amazon Web Services (AWS)	Cloud hosting/infrastructure for Digital Services and secure storage	United Kingdom - London region (eu-west-2) unless otherwise notified	Hosting, storage, compute, backup and security services	AWS data processing terms and applicable UK transfer mechanisms where needed
Microsoft Ireland Operations Limited (and affiliates)	Email support desk. Cloud email infrastructure, productivity suite, and enterprise communication services	United Kingdom / European Economic Area (EEA) data centres	Processing, routing, and storing client support emails, inbound notifications, and internal communications	Microsoft Products and Services Data Protection Addendum (DPA) and UK GDPR compliant standard

Subprocessor	Service provided	Location	Processing purpose	Safeguards / transfer mechanism
			regarding Digital Services.	contractual clauses / UK Addendum where applicable.
Atlassian Pty Ltd (and Atlassian US, Inc.)	Jira Service Management / customer support ticketing platform	United Kingdom	Logging, tracking, investigating, and resolving technical support tickets, platform bugs, and user account queries containing Licensee Data.	Atlassian Data Processing Addendum, incorporating EU Standard Contractual Clauses (SCCs) alongside the UK International Data Transfer Addendum.

Appendix 4 - Retention and Deletion

Data / record type	Default retention period	Deletion / return approach
Digital Services account data and user profile data	Subscription Term plus 30-day export period unless otherwise agreed	Deleted or anonymised after export period, subject to backup cycles and legal retention.
Questionnaire responses, report/results data and dashboard source data processed as processor	Subscription Term plus 30-day export period unless otherwise instructed	Returned/exported on request, then deleted or anonymised in accordance with this DPA.
Support tickets and service desk communications containing Licensee Data	For the period required to support the issue and maintain service records, normally up to 24 months unless otherwise agreed	Deleted, anonymised or retained as business records where lawful and necessary.
Security logs, audit logs and access logs	Normally 6-24 months depending on system/security needs unless a longer period is required for investigation or legal compliance	Deleted on scheduled log retention cycles.

Data / record type	Default retention period	Deletion / return approach
Backups	Overwritten or deleted on the next scheduled backup cycle, normally within 180 days unless otherwise agreed	Backups are put beyond ordinary use after termination and protected until deletion.
Aggregated/anonymised data	May be retained indefinitely where no individual or Licensee is identifiable	Not subject to UK GDPR if truly anonymised; re-identification prohibited.
Financial, contractual and compliance records	Up to 6 years after the end of the relevant financial year or longer if required by law/dispute	Retained by Genius Within as independent controller for legal/accounting purposes.