Schedule 1 — Data Processing Addendum

1. Scope of This Addendum

This Data Processing Addendum ("DPA") applies where DPIAS processes Personal Data **on behalf of the Customer**, including during the provision of:

- DPIA/ROPA consulting
- Security posture reviews
- Cyber Security Reviews
- Systems analysis, configuration assessment, and compliance auditing

All processing will be carried out solely for the purposes described below and strictly in accordance with Customer instructions.

2. Subject Matter, Nature & Purpose of Processing

2.1 Subject Matter

Processing of Personal Data contained within documents, systems, logs, permissions records, and security-related datasets accessed solely for the purpose of delivering the Services.

2.2 Nature of Processing

Processing activities may include:

- Accessing and reviewing datasets
- Analysing system configurations and permissions
- Reviewing audit logs, authentication logs, and user access activity
- Evaluating security controls
- Producing security findings and recommendations
- Document review, report writing, and secure communication of results

2.3 Purpose

Personal Data will only be processed for:

- Creating DPIAs, ROPAs, assessments or compliance documents
- Conducting Cyber Security Review work
- Identifying vulnerabilities and misconfigurations
- Validating access controls and authentication practices
- Supporting Customer compliance with UK GDPR Article 32 security obligations
- Producing advisory recommendations

Processing will **never** be used for Supplier's own purposes.

3. Categories of Personal Data

The following Personal Data may be processed:

- Staff identifiers (name, email, role, username)
- Access permissions and group memberships
- Device or system activity logs
- Authentication logs (successful/failed sign-ins, MFA events)
- IP addresses and session metadata
- Security incident data
- Misconfiguration or vulnerability data that may indirectly relate to individuals
- Any personal data contained in files supplied by the Customer

Special Category Data:

Not typically required for Cyber Security Review work but may be encountered in:

- HR systems
- SEND/safeguarding records
- Email/document repositories

If Special Category Data is in scope, Customer must inform Supplier in advance.

4. Categories of Data Subjects

- Customer employees
- Contractors
- System users
- Administrators and privileged accounts
- Any identifiable individuals appearing within audit logs or datasets

5. Data Location & Storage

- All processing and storage will occur **within the United Kingdom**.
- Supplier uses UK-based Microsoft 365 infrastructure for communications, document storage and collaboration.
- No Personal Data will be transferred outside the UK unless explicitly authorised by the Customer and protected by appropriate safeguards (e.g., UK IDTA).

6. Access and Sub-Processors

6.1 Supplier Personnel

Access to Customer Personal Data is restricted to DPIAS personnel who:

- Require access to fulfil the Services
- Are bound by written confidentiality obligations
- Have received training in data protection and cyber security

6.2 Sub-Processors

Supplier may use specialist UK-based cyber security sub-processors **only with Customer approval**.

- Sub-processors will be bound by written data processing agreements meeting UK GDPR Article 28 requirements.
- Supplier must notify Customer of intended new sub-processors, giving Customer the right to object.

7. Security Measures (Article 32)

Supplier will implement appropriate technical and organisational measures including:

- UK-hosted Microsoft 365 tenancy
- MFA and secure authentication for all accounts
- Encryption in transit and at rest
- Role-based access controls
- Logging and audit trails
- Secure transfer protocols
- Device hardening and endpoint protection
- Document classification and secure workspace separation
- Principle of least privilege
- Regular review of cyber security posture

These measures align with NCSC guidance and Article 32 UK GDPR.

8. Customer Responsibilities

Customer must:

- Provide accurate data and appropriate access
- Ensure lawful basis and transparency for all shared data
- Implement any recommended controls internally
- Ensure security of Customer systems outside of DPIAS scope

9. Breach Notification

Supplier will notify Customer:

- **Without undue delay**, and
- **In any event within 48 hours**,

after becoming aware of a Personal Data Breach affecting Customer data.

Supplier will provide all reasonably necessary information to support investigation and reporting.

10. Data Sharing & Disclosure

Except as directed by Customer or required by law, Supplier will **not** disclose Personal Data to third parties.

Disclosure for cyber security review purposes will **only occur**:

- With Customer instruction
- To approved UK-based cyber specialists
- Under binding confidentiality and data protection terms

No other disclosure is permitted.

11. Retention & Deletion

Upon completion of the Services, Supplier will:

- Retain Personal Data only for the minimum period required (normally up to 90 days unless contractual or legal retention applies)
- Securely delete or return all Customer Personal Data upon written instruction

Supplier may retain non-personal aggregates, metrics, or derived insight that contains **no personal data**.

12. Audit Rights

Customer may request evidence of Supplier's compliance with this DPA.
Formal audit access will be granted where required by law or contract.

13. Liability

Liability under this DPA is governed by the main Terms of Business.
Supplier is not liable for cyber incidents occurring within Customer systems unless directly caused by Supplier's negligence.