Annex D — Data Processing Agreement

Forms part of the Engagement Letter between Alpha IT Solutions Ltd and the client named below. Made under **Article 28 of the UK GDPR** and the Data Protection Act 2018.

Client organisation	
Date	

1. Roles

You are the **controller**. Alpha IT Solutions Ltd is the **processor**.

We process personal data only to carry out the security audit described in the Engagement Letter, and only on your documented instructions.

Alpha IT Solutions Ltd is registered with the Information Commissioner's Office, registration number ZC214066.

2. What we process

Subject matter	Security audit of the computers listed in Form C
Duration	The engagement, plus a 12-month retention period
Nature and purpose	Reading system configuration to identify security weaknesses, and reporting on them
Types of personal data	Windows usernames and account names; computer names; local administrator group membership; account status and last-logon information; user profile folder names; network identifiers such as IP and MAC addresses
Categories of data subject	Your employees, contractors and anyone else holding an account on the computers in scope
Special category data	**None.** We do not seek it and our checks do not read it

We do not read the contents of files, email or documents. Personal data reaches us only as a by-product of reading system configuration.

3. What we will do

3.1 Process personal data only on your documented instructions, unless the law requires otherwise. If it does, we will tell you first unless the law forbids that.

3.2 Make sure everyone who processes the data is under a duty of confidence.

3.3 Apply appropriate technical and organisational security measures (section 4).

3.4 Not engage another processor without your prior written authorisation (section 5).

3.5 Help you respond to requests from individuals exercising their rights, taking account of the nature of the processing.

3.6 Help you with data protection impact assessments and with consulting the ICO, where needed.

3.7 On your written instruction, delete or return all personal data at the end of the retention period, and delete existing copies unless the law requires us to keep them.

3.8 Make available the information you need to demonstrate compliance with Article 28, and allow and contribute to audits by you or an auditor you appoint, on reasonable notice.

4. Security measures

We apply the following:

- Audit results are held encrypted in transit and stored on systems under our sole control
- Access is limited to personnel who need it for the engagement
- Systems used to process the data are patched and run current anti-malware
- Multi-factor authentication is enforced on the accounts used to access the data
- Credentials supplied by you for the audit are held in memory only and never written to disk
- Reports containing findings are shared only through channels agreed with you
- Any sensitive material captured incidentally is redacted before a report leaves us

5. Sub-processors

We use the following sub-processors:

Sub-processor	Purpose	Location
IONOS	Hosting the client portal and report storage	United Kingdom
Anthropic PBC	Optional AI-assisted drafting of the report narrative	USA

The AI-assisted narrative is optional and off unless you agree to it. Where it is used, only finding titles and recommended remediation are sent. **Evidence, credentials, IP addresses, MAC addresses and machine**

names are never sent.

☐ **I agree to the optional AI-assisted report narrative** (initial here: _____)

We will tell you at least **30 days** before adding or replacing any sub-processor, and you may object on reasonable data protection grounds.

6. Where your data is held

Your data stays in the United Kingdom. Working copies are held here, and the client portal and report storage run on UK servers hosted with IONOS.

The single exception is the optional AI-assisted narrative. If you agree to it, the limited data described in section 5 is transferred to the **USA** under the **UK International Data Transfer Addendum** to the EU Standard Contractual Clauses, or another lawful transfer mechanism then in force. Decline it and nothing leaves the UK.

7. Personal data breaches

We will notify you without undue delay, and in any event within 24 hours, of becoming aware of a personal data breach affecting your data.

We will give you the nature of the breach, the categories and approximate number of records affected, the likely consequences, the measures taken, and a contact point.

Reporting to the ICO and to affected individuals is **your** responsibility as controller. We will give you what you need to do it.

8. Retention and deletion

We keep audit results for **12 months** from the date of the report, so a later audit can be compared against it and progress shown.

At the end of that period we delete them. You may ask us in writing to delete them sooner, and we will do so within **30 days**, except where the law requires us to keep something.

Deletion covers working copies, the audit history database, and any copy held in the client portal.

9. Liability

Liability under this Annex is subject to the limits set out in clause 10 of the Engagement Letter.

10. Priority

Where this Annex conflicts with the Engagement Letter on the processing of personal data, **this Annex takes priority**.

Signatures

Controller — the client

Organisation	
Signature	
Name	
Title	
Date	

Processor — Alpha IT Solutions Ltd

Signature	
Name	Laurentiu Robert Niculescu
Title	Director
Date	