

Data Processing Agreement

System Force I.T. Limited – processor terms under UK GDPR Article 28 and the Data Protection Act 2018

Version: 1.0

Effective date: 14 October 2026

Last updated: 14 October 2026

Revision history: v1.0, 14 October 2026 – first published version.

This Data Processing Agreement ("DPA") forms part of, and is incorporated into, the master services agreement, engagement terms or statement of work between the Client and System Force I.T. Limited (the "Principal Agreement"). It sets out the terms on which System Force I.T. Limited processes personal data on behalf of the Client in connection with the services. Where there is any conflict between this DPA and the Principal Agreement in relation to the processing of personal data, this DPA prevails.

1. The parties and their roles

Processor: System Force I.T. Limited, a company registered in England and Wales (company number 05750412), whose registered office is at Unit C1, Brearley Place, Waterwells Business Park, Baird Road, Quedgeley, Gloucester, GL2 2GB, and whose operational address is Units C1 & C2, Brearley Place, Waterwells Business Park, Baird Road, Quedgeley, Gloucester, GL2 2GB ("SFIT", "we", "us").

Controller: the Client identified in the Principal Agreement (the "Client", "you").

For the purposes of this DPA, and in respect of personal data processed in connection with the services, the Client is the controller and SFIT is the processor. Where the Client is itself a processor acting on behalf of a third-party controller, SFIT acts as a sub-processor, and the Client's instructions to SFIT must be consistent with that third-party controller's instructions.

2. Definitions

Unless otherwise defined, the following terms have the meanings given in UK data protection law:

- **UK GDPR** means the UK General Data Protection Regulation as defined in the Data Protection Act 2018.
 - **Data Protection Laws** means the UK GDPR, the Data Protection Act 2018, and all other laws relating to the processing of personal data and privacy that apply in the United Kingdom.
 - **controller, processor, personal data, processing, personal data breach, data subject, and special category data** have the meanings given in the UK GDPR.
 - **sub-processor** means any third party engaged by SFIT to process personal data on the Client's behalf in connection with the services.
 - **services** means the services provided by SFIT to the Client under the Principal Agreement.
 - **ICO** means the UK Information Commissioner's Office.
-

3. Scope, subject-matter, duration, nature and purpose

SFIT processes personal data on behalf of the Client only to the extent necessary to provide the services. The subject-matter, duration, nature and purpose of the processing, the types of personal data, and the categories of data subjects are set out in Schedule 1 (Details of Processing), which the Client completes and

keeps up to date. In the absence of a completed Schedule 1, the processing is as reasonably necessary to deliver the services described in the Principal Agreement.

The duration of processing is the term of the Principal Agreement, together with any period during which SFIT is required to retain personal data under clause 11 or by law.

4. Processing on documented instructions

SFIT processes the Client's personal data only on the Client's documented instructions, including with regard to international transfers, unless required to do otherwise by law to which SFIT is subject. The Principal Agreement, this DPA, and the Client's ordinary use of the services constitute the Client's initial documented instructions. If SFIT is required by law to process personal data otherwise than on the Client's instructions, it will, where legally permitted, inform the Client of that legal requirement before processing. SFIT will promptly inform the Client if, in its opinion, an instruction infringes the Data Protection Laws (without being obliged to provide legal advice).

5. Confidentiality

SFIT ensures that all personnel authorised to process the Client's personal data are bound by appropriate obligations of confidentiality (whether contractual or statutory), are informed of the confidential nature of the personal data, and process it only as necessary to perform their duties in connection with the services.

6. Security of processing (Article 32)

Taking account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risks to data subjects, SFIT implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk. SFIT holds UKAS-accredited certification to ISO/IEC 27001:2022 and operates an information security management system (ISMS) certified to that standard. The measures are described in general terms in Annex A and include: encryption of personal data in transit and at rest; enforced multi-factor authentication; role-based access control on a least-privilege basis; centralised logging and security monitoring (SIEM); backup with periodic recovery testing; vulnerability management and patching; and a documented incident response process. SFIT may update these measures from time to time, provided the level of security is not materially reduced.

7. Sub-processors

The Client gives SFIT general written authorisation to engage sub-processors to process the Client's personal data in connection with the services. A current list of sub-processors is set out in Annex B. SFIT imposes on each sub-processor, by written contract, data protection obligations that are substantially the same as those set out in this DPA, and SFIT remains fully liable to the Client for the performance of each sub-processor's obligations.

SFIT will give the Client reasonable prior notice of any intended addition or replacement of a sub-processor that handles the Client's personal data. The Client may object to such a change on reasonable data protection grounds within 14 days of that notice. If the parties cannot resolve the objection, the Client may terminate the affected services in accordance with the Principal Agreement. SFIT maintains the authoritative, current sub-processor list in its ISMS Approved Supplier Register, which is available to the Client on request.

8. International transfers

Where the provision of the services involves a transfer of personal data to, or access from, a country outside the United Kingdom, SFIT ensures that an appropriate transfer mechanism is in place, such as UK adequacy regulations, the UK International Data Transfer Agreement (IDTA), or the UK Addendum to the European Commission's Standard Contractual Clauses, together with a transfer risk assessment and any supplementary measures required to ensure an adequate level of protection. Details of relevant sub-processor locations and safeguards are maintained in SFIT's ISMS Approved Supplier Register (see Annex B).

9. Assistance to the Client

Taking into account the nature of the processing and the information available to SFIT, SFIT provides the Client with reasonable assistance:

- by appropriate technical and organisational measures, insofar as possible, to help the Client respond to requests from data subjects exercising their rights under the Data Protection Laws; and
- in ensuring compliance with the Client's obligations under Articles 32 to 36 of the UK GDPR (security of processing, personal data breach notification and communication, data protection impact assessments, and prior consultation with the ICO).

Where a data subject sends a request directly to SFIT in relation to the Client's personal data, SFIT will, unless legally prohibited, promptly forward it to the Client and will not respond to it itself except on the Client's documented instructions. SFIT may charge a reasonable fee for assistance that goes beyond the standard functionality of the services, as set out in the Principal Agreement.

10. Personal data breach notification

SFIT notifies the Client without undue delay after becoming aware of a personal data breach affecting the Client's personal data. The notification will, to the extent known, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address it. SFIT will cooperate with the Client and take reasonable steps to mitigate and remediate the breach. SFIT will not notify the ICO or data subjects on the Client's behalf unless instructed to do so in writing.

11. Return or deletion of personal data

On termination or expiry of the services, or earlier on the Client's written request, SFIT will, at the Client's choice, return the Client's personal data and/or delete it and delete existing copies, unless SFIT is required to retain a copy by law. Where deletion is chosen, SFIT will delete the personal data within a reasonable period and, on request, certify that deletion. Personal data held in routine backups is deleted in accordance with SFIT's backup retention cycle and remains protected by the measures in Annex A until deleted.

12. Audit and information rights

SFIT makes available to the Client the information reasonably necessary to demonstrate compliance with Article 28 of the UK GDPR and this DPA, and allows for and contributes to audits, including inspections, conducted by the Client or an auditor it mandates. The Client agrees that SFIT's UKAS-accredited ISO/IEC 27001:2022 certification, and the associated Statement of Applicability and audit reports (to the extent disclosable), may be provided to satisfy audit and information requests in the first instance. Any on-site audit

will be on reasonable prior notice, during normal business hours, no more than once per year (except where required by a supervisory authority or following a personal data breach), conducted so as to minimise disruption to SFIT's operations, and subject to confidentiality.

13. Liability and indemnity

The liability of each party under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement. Nothing in this DPA limits or excludes liability to the extent it cannot be limited or excluded by law.

14. Governing law and jurisdiction

This DPA is governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales, consistent with the Principal Agreement.

15. Acceptance

This DPA is accepted and incorporated into the Principal Agreement when the Client accepts it online through System Force's ClearSignal platform, or signs or accepts the Principal Agreement (or a document that references this DPA).

16. Data protection contact

Questions about this DPA, or about how SFIT processes personal data, may be sent to dpa@systemforce.co.uk, or by post to the operational address given in clause 1.

Schedule 1 – Details of processing (to be completed by the Client)

This Schedule records the specifics of the processing SFIT carries out for the Client. The Client is responsible for completing and maintaining it.

- **Subject-matter of processing:** to be completed – for example, provision of managed IT, cyber security, cloud, backup and telephony services.
- **Duration:** the term of the Principal Agreement, plus any lawful retention period.
- **Nature and purpose:** to be completed – for example, hosting, storage, backup, monitoring, support, administration and security of the Client's systems and data.
- **Types of personal data:** to be completed – for example, names, contact details, job roles, account credentials, email content, device and usage data, and any personal data contained within the Client's systems and files.
- **Categories of data subjects:** to be completed – for example, the Client's staff, contractors, customers, suppliers and other individuals whose data is held in the Client's systems.
- **Special category or criminal offence data:** to be completed – state whether any special category or criminal offence data is processed, and if so, which.

Annex A – Technical and organisational measures (Article 32)

SFIT operates an ISO/IEC 27001:2022-certified ISMS. In general terms, the measures include:

- **Encryption:** encryption of personal data in transit and at rest.
- **Access control:** enforced multi-factor authentication, and role-based access control on a least-privilege basis.
- **Logging and monitoring:** centralised logging and security monitoring (SIEM).
- **Resilience and backup:** backup of data with periodic recovery testing.
- **Vulnerability management:** vulnerability management and timely patching.
- **Incident response:** a documented incident response process.
- **Organisational measures:** staff confidentiality obligations, security awareness, supplier management via an Approved Supplier Register, and policies maintained within the ISMS.

These measures are maintained under the ISMS and may be updated, provided the level of security is not materially reduced.

Annex B – Sub-processors

The following sub-processors may process the Client's personal data in connection with the services. The processing locations shown are indicative; SFIT maintains the authoritative, current list (including processing locations and transfer safeguards) in its ISMS Approved Supplier Register, which is available on request.

Current sub-processors

Sub-processor	Purpose	Processing location
Microsoft (Microsoft 365 / Azure)	Productivity, email, identity and cloud hosting	United Kingdom / EU
Axcient	Cloud backup and disaster recovery	United Kingdom / EU
Atera	Remote monitoring and management (RMM)	EU / US
Cynet	Endpoint detection and response (EDR)	EU / US
Cisco Duo	Multi-factor authentication	US / EU
Cloudflare	DNS, content delivery and web security	Global edge network (UK / EU / US)
3CX	Business telephony (VoIP)	United Kingdom / EU
Exclaimer	Email signature management	United Kingdom / EU
RoboShadow	Vulnerability and attack-surface scanning	United Kingdom

Where any sub-processor processes personal data outside the UK, those transfers are protected as described in clause 8.

See also our [Privacy Policy](#) and [Terms of Use](#).