

DATA PROCESSING TERMS

These Data Processing Terms are issued by Leap IT Ltd (05317506) whose registered office is at Unit 16, Hockley Court, Solihull, West Midlands, B94 6NW ("Leap IT", "Processor" or "Data Processor"). These Data Processing Terms form part of the agreement under which Leap IT Ltd provides Services to the Customer. They apply whenever Leap IT Ltd Processes Customer Personal Data on behalf of the Customer. By ordering, receiving or continuing to use the Services, the Customer agrees that these Data Processing Terms are incorporated into the Principal Agreement.

BACKGROUND

(A) The Customer is a Controller in respect of the Customer Personal Data.

(B) The Customer wishes to engage the Data Processor to provide the Services, which involve the Processing of Customer Personal Data by the Data Processor on the Customer's behalf.

(C) The Customer and Data Processor adopt these Data Processing Terms in order to satisfy the requirements of Article 28 of the UK GDPR and to set out the terms on which the Data Processor Processes Customer Personal Data.

1. Definitions and Interpretation

1.1 In these Data Processing Terms, the following terms have the following meanings:

"Applicable Laws" means the laws of England and Wales and any other laws or regulations to which the Customer and Data Processor are subject;

"Customer Personal Data" means any Personal Data Processed by the Data Processor on behalf of the Customer pursuant to or in connection with the Principal Agreement;

"Data Processing Terms" means these data processing terms, including their Schedules;

"Data Protection Laws" means the UK GDPR, the Data Protection Act 2018 and all other Applicable Laws relating to the Processing of Personal Data and privacy that are in force in the United Kingdom from time to time;

"Data Transfer" means a transfer of Customer Personal Data by the Data Processor to a country or international organisation outside the United Kingdom, or an onward transfer of Customer Personal Data by a Sub-processor, in each case where such transfer is restricted by Data Protection Laws;

"Principal Agreement" means the agreement or agreements between the Customer and Data Processor under which the Data Processor provides the Services to the Customer;

"Processor" or "Data Processor" means Leap IT Ltd;

"Services" means the services provided by the Data Processor to the Customer under the Principal Agreement, as further described in Schedule 1;

"Sub-processor" means any person appointed by or on behalf of the Data Processor to Process Personal Data on behalf of the Customer in connection with these Data Processing Terms; and

"UK GDPR" has the meaning given to it in section 3(10) of the Data Protection Act 2018 (as supplemented by section 205(4) of that Act).

1.2 The terms "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing", "Processor" and "Supervisory Authority" have the meanings given to them in the UK GDPR, and their cognate terms are construed accordingly.

1.3 References in these Data Processing Terms to Articles are references to Articles of the UK GDPR.

2. Processing of Customer Personal Data

2.1 The Data Processor shall comply with all Data Protection Laws applicable to it in its Processing of Customer Personal Data.

2.2 The Data Processor shall Process Customer Personal Data only on the Customer's documented instructions, including with regard to Data Transfers, unless required to Process Customer Personal Data otherwise by

Applicable Laws. Where the Data Processor is so required, it shall inform the Customer of that legal requirement before Processing, unless Applicable Laws prohibit it from doing so on important grounds of public interest.

2.3 The Data Processor shall immediately inform the Customer if, in its opinion, an instruction given by the Customer infringes Data Protection Laws. The Data Processor shall not be obliged to act on any such instruction pending resolution of the matter between the Customer and Data Processor.

2.4 The Customer's initial documented instructions, together with the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, the categories of Data Subjects and the Customer's obligations and rights, are set out in Schedule 1. The Customer may issue further instructions in writing (including by email) from time to time.

2.5 The Customer warrants that it has all necessary rights, consents and lawful bases to disclose Customer Personal Data to the Data Processor and that its instructions comply with Data Protection Laws.

2.6 Where the Customer subscribes to WorkPulse under a separate WorkPulse Agreement with the Data Processor, Schedules 3, 4 and 5 apply in addition to Schedule 1 for so long as that subscription continues. The Sub-processors identified in Schedule 2 as applying only to WorkPulse apply solely in respect of that subscription and not to the Customer's other Services.

3. Data Processor Personnel

3.1 The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent, contractor or Sub-processor who may have access to Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Customer Personal Data for the purposes of the Principal Agreement.

3.2 The Data Processor shall ensure that all such individuals are subject to confidentiality undertakings, or are under an appropriate professional or statutory obligation of confidentiality, in respect of Customer Personal Data.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including as appropriate the measures referred to in Article 32(1).

4.2 In assessing the appropriate level of security, the Data Processor shall take account in particular of the risks presented by the Processing, and in particular from a Personal Data Breach.

4.3 In discharging its obligations under this clause 4, the Data Processor shall as a minimum give due consideration to the following categories of security measure: information security management systems; physical security; access control; security and privacy enhancing technologies; awareness, training and security checks in relation to personnel; incident response management and business continuity; and audit controls and due diligence.

4.4 Taking into account the nature of the Processing and the information available to it, the Data Processor shall assist the Customer in ensuring compliance with the Customer's obligations under Articles 32 to 36, including obligations relating to the security of Processing, the notification of Personal Data Breaches to the Supervisory Authority and to Data Subjects, the carrying out of data protection impact assessments and prior consultation with the Supervisory Authority.

5. Sub-processing

5.1 The Customer gives the Data Processor general written authorisation to appoint the Sub-processors listed in Schedule 2. Any addition to, or replacement of, those Sub-processors shall be made in accordance with clause 5.2, and the Data Processor shall not disclose any Customer Personal Data to a Sub-processor otherwise than as permitted by this clause 5.

5.2 Where the Data Processor intends to add or replace a Sub-processor, it shall give the Customer not less than thirty (30) days' written notice of the intended change, and the Customer shall have a reasonable opportunity to object to the change during that period. Where the Customer objects on reasonable data protection grounds, the Customer and Data Processor shall discuss in good faith an alternative arrangement.

5.3 Where the Data Processor appoints a Sub-processor, it shall do so by way of a written contract which imposes on the Sub-processor data protection obligations offering a level of protection for Customer Personal Data

equivalent to that provided under these Data Processing Terms, including an obligation to provide sufficient guarantees to implement appropriate technical and organisational measures.

5.4 The Data Processor shall remain fully liable to the Customer for the performance of each Sub-processor's data protection obligations. Any such liability shall be subject to clause 12 of these Data Processing Terms.

5.5 For the avoidance of doubt, any third party with which the Customer contracts directly, and any third party whose services the Data Processor administers on the Customer's behalf pursuant to a contract between the Customer and that third party, is not a Sub-processor for the purposes of these Data Processing Terms.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Data Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests from Data Subjects seeking to exercise their rights under Data Protection Laws.

6.2 The Data Processor shall promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data.

6.3 The Data Processor shall not respond to any such request except on the Customer's documented instructions or as required by Applicable Laws. Where the Data Processor is required by Applicable Laws to respond, it shall, to the extent permitted by those laws, inform the Customer of that legal requirement before responding.

7. Personal Data Breach

7.1 The Data Processor shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, upon becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 Such notification shall provide the Customer with sufficient information to allow the Customer to meet any obligation to report the Personal Data Breach to the Supervisory Authority or to inform Data Subjects under Data Protection Laws, including, to the extent known, 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.

7.3 The Data Processor shall co-operate with the Customer and take such reasonable steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessments and Prior Consultation

8.1 The Data Processor shall provide reasonable assistance to the Customer with any data protection impact assessment, and with any prior consultation with the Supervisory Authority, which the Customer reasonably considers to be required by Article 35 or Article 36, in each case solely in relation to the Processing of Customer Personal Data by the Data Processor and taking into account the nature of the Processing and the information available to the Data Processor.

9. Deletion or Return of Customer Personal Data

9.1 On the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), the Data Processor shall, at the Customer's choice, delete or return to the Customer all Customer Personal Data then in its possession or control.

9.2 The Data Processor shall give effect to the Customer's choice in respect of live and actively accessible Customer Personal Data within ten (10) business days of the Cessation Date, or within such longer period as the Customer and Data Processor may agree in writing.

9.3 Where Customer Personal Data is held within backup or archive media from which immediate deletion is not technically practicable, the Data Processor shall place that Customer Personal Data beyond use with effect from the Cessation Date and shall securely delete it on the expiry of the applicable backup retention cycle. The Data Processor shall on request confirm to the Customer the applicable retention period.

9.4 Clauses 9.1 to 9.3 do not apply to the extent that Applicable Laws require the Data Processor to store Customer Personal Data, in which case the Data Processor shall inform the Customer of that requirement and shall continue to protect that Customer Personal Data in accordance with these Data Processing Terms for so long as it is retained.

10. Audits and Inspections

10.1 The Data Processor shall make available to the Customer on request all information necessary to demonstrate compliance with the obligations set out in Article 28 and these Data Processing Terms.

10.2 The Data Processor shall allow for, and contribute to, audits and inspections of its Processing of Customer Personal Data conducted by the Customer or by an auditor mandated by the Customer, subject to clause 10.3.

10.3 Any audit under clause 10.2 shall be conducted no more than once in any twelve (12) month period, on not less than thirty (30) days' written notice, during normal business hours, in a manner that does not unreasonably disrupt the Data Processor's business, and subject to the auditor entering into reasonable confidentiality undertakings. This limitation does not apply where an audit is required by a Supervisory Authority or is carried out following a Personal Data Breach affecting Customer Personal Data.

10.4 The Data Processor may satisfy its obligations under clauses 10.1 and 10.2 by providing the Customer with its current certifications, audit reports or summary findings under the standards to which it is certified, where these reasonably address the scope of the Customer's request.

11. Data Transfers

11.1 The Data Processor shall not transfer, or authorise the transfer of, Customer Personal Data to any country outside the United Kingdom without the Customer's prior written consent, and shall not do so except in accordance with Data Protection Laws. The Customer's consent to the transfers identified in Schedule 2 is given in that Schedule.

11.2 Where a Data Transfer requires appropriate safeguards under Data Protection Laws, the Customer and Data Processor shall ensure that a lawful transfer mechanism is in place. Such mechanisms may include a relevant adequacy decision or adequacy regulations, the International Data Transfer Agreement issued by the Information Commissioner, the International Data Transfer Addendum to the EU Standard Contractual Clauses, or any other transfer mechanism recognised under Data Protection Laws.

12. Liability

12.1 The liability of the Customer and Data Processor under or in connection with the Data Processing Terms, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the exclusions and limitations of liability set out in the Principal Agreement, and all claims arising under these Data Processing Terms shall count towards the aggregate financial cap on liability set out in the Principal Agreement under which the relevant Service giving rise to the claim was provided.

12.2 Nothing in these Data Processing Terms limits or excludes the Customer's and Data Processor's liability to the extent that such liability cannot be limited or excluded under Applicable Laws, and nothing in these Data Processing Terms affects the rights of Data Subjects under Data Protection Laws or the liability of either Customer or Data Processor to a Supervisory Authority.

13. General

13.1 The Customer and Data Processor shall keep confidential the terms of these Data Processing Terms and any information received from the other party in connection with them, and shall not use or disclose such information without either the Customer's or Data Processor's prior written consent, except to the extent that disclosure is required by Applicable Laws or the information is already in the public domain other than through breach of this clause.

13.2 All notices given under these Data Processing Terms shall be in writing and shall be delivered personally, sent by pre-paid post or sent by email to the contact details specified in the relevant Principal Agreement, the Customer's account records maintained by the Data Processor, or to such other address as either party notifies.

13.3 These Data Processing Terms constitute the entire terms between the Customer and Data Processor in respect of the Processing of Customer Personal Data. In the event of any conflict between these Data Processing Terms and the Principal Agreement in relation to the Processing of Customer Personal Data, these Data Processing Terms prevail, save that the exclusions and limitations of liability set out in the Principal Agreement continue to apply as provided in clause 12.1.

13.4 The Data Processor may amend these Data Processing Terms from time to time to reflect changes in Applicable Laws, regulatory requirements, services, processing activities or business operations. The Data Processor shall provide not less than thirty (30) days' written notice of any material amendment. Where the Customer reasonably objects to a material amendment on data protection grounds, the parties shall discuss in

good faith an alternative arrangement. Continued use of the Services following the effective date of the amendment constitutes acceptance of the amended Data Processing Terms.

13.5 Third party rights. A person who is not the Customer or Data Processor has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of these Data Processing Terms.

13.6 These Data Processing Terms may be executed in counterparts, each of which when executed constitutes an original and all of which together constitute one agreement. Execution by electronic signature is valid and binding.

14. Governing Law and Jurisdiction

14.1 These Data Processing Terms and any dispute or claim arising out of or in connection with them are governed by and construed in accordance with the law of England and Wales.

14.2 The Customer and Data Processor irrevocably submit to the exclusive jurisdiction of the courts of England and Wales.

Schedule 1 — Details of the Processing

This Schedule sets out the information required by Article 28(3).

Item	Details
Subject matter of the Processing	The provision of IT support, managed services, cloud services, cyber security services, Microsoft 365 administration, backup, monitoring, helpdesk and related technical services by the Data Processor to the Customer under the Principal Agreement.
Duration of the Processing	For the term of the Principal Agreement, and thereafter for any further period required to give effect to clause 9 (including backup retention cycles), to complete documented transition activities, or to comply with a retention obligation under Applicable Laws.
Nature of the Processing	Accessing, viewing, storing, hosting, transmitting, retrieving, organising, backing up, restoring, maintaining, securing and deleting Customer Personal Data, and such other operations as are required to provide the Services.
Purpose of the Processing	To deliver the Services, being the support of users, maintenance of systems, administration of accounts and licensing, security monitoring, resolution of technical issues, incident response, management of backups, and the carrying out of other technical activities instructed by the Customer.
Type of Personal Data	Names, business contact details, email addresses, telephone numbers, job titles, usernames and user identifiers, device identifiers, IP addresses, system and access logs, the content of business communications and files held within supported systems, support ticket content, and any other Personal Data made accessible to the Data Processor through the Customer's systems in the course of providing the Services.
Categories of Data Subject	The Customer's employees, workers, contractors, consultants and directors; and the Customer's clients, customers, suppliers, end users and other individuals whose Personal Data is held within systems supported by the Data Processor.
Special category data	The Data Processor is not instructed to Process special category data or criminal offence data as a distinct activity. Where such data is held within systems supported by the Data Processor, it may be incidentally accessible in the course of providing the Services and shall be treated as Customer Personal Data under these Data Processing Terms.
Obligations and rights of the Customer	The Customer determines the purposes and means of the Processing and remains responsible for: establishing a lawful basis for the Processing; issuing documented instructions to the Data Processor; providing information to Data Subjects and responding to the exercise of their rights; assessing whether a data protection impact assessment is required; notifying Personal Data Breaches to the Supervisory Authority and, where required, to Data Subjects; and

	determining, on the Cessation Date, whether Customer Personal Data is to be deleted or returned. The Customer has the rights set out in these Data Processing Terms, including the rights of audit and inspection under clause 10 and the right to object to a Sub-processor under clause 5.2.
--	--

Schedule 2 — Authorised Sub-processors

The Customer gives general written authorisation under clause 5.1 to the appointment of the Sub-processors listed below. Changes are subject to the notice and objection procedure in clause 5.2.

Sub-processor	Purpose / Service and location of Processing
NinjaONE LLC	Remote monitoring and management, endpoint monitoring, device management and remote support. Location: EU.
Bitdefender SRL	Endpoint security and threat protection. Location: EU.
Acronis International GmbH	Backup, recovery and business continuity services, and advanced email security. Location: United Kingdom and EU.
RocketCyber (Kaseya)	Security monitoring, managed detection and response, and threat protection. Location: United States. Transfers are made under the UK Extension to the EU-US Data Privacy Framework, with the UK International Data Transfer Addendum applying as an alternative mechanism, in each case as provided in the Kaseya Data Processing Addendum.
Accelo Inc.	CRM, service desk, ticketing, contracts and project management. Location: EU (AWS hosted).
Microsoft	Microsoft 365 cloud productivity, email, storage and collaboration services, provided under the Microsoft Customer Agreement and administered by the Data Processor on the Customer's behalf under the Data Processor's CSP reseller relationship (via Arrow, a CSP distributor). Location: United Kingdom / EU (Microsoft 365 UK Data Boundary).
Supabase (WorkPulse only)	WorkPulse application and/or database hosting. Location: EU. Applies only where the Customer subscribes to WorkPulse — see clause 2.6.
Lovable (WorkPulse only)	WorkPulse customer frontend interface. Location: EU. Applies only where the Customer subscribes to WorkPulse — see clause 2.6.

By entering into these Data Processing Terms the Customer gives its prior written consent under clause 11.1 to transfers of Customer Personal Data to the locations set out in this Schedule, subject to the safeguards required by clause 11.2.

Third parties with which the Customer contracts directly are not Sub-processors for the purposes of these Data Processing Terms, and are not listed above. See clause 5.5.

Schedule 3 — WorkPulse-Specific Processing Details

Applies only where the Customer subscribes to WorkPulse. This Schedule supplements, and does not replace, Schedule 1 — see clause 2.6.

Article 28 information	WorkPulse details
Subject matter	Provision of the WorkPulse workforce and device-visibility Service.
Duration	For the Term, together with the retention and deletion periods stated in Schedule 4 and these Data Processing Terms.
Nature and purpose	Collection, retrieval, organisation, storage, analysis and presentation of endpoint telemetry to produce dashboards, reports and operational summaries for the Customer.
Data subjects	Customer employees, workers and contractors whose devices are enrolled in WorkPulse.

Personal data	Names or employee identifiers associated with devices; login, lock and logoff timestamps; inferred location category; software and application names; active-window or tab titles; configured application time; device health metrics; and roll-call presence records where enabled.
Special category data	Not intentionally collected. It may be incidentally revealed in active-window or browser-tab titles.
Customer instructions	The configuration and use of the subscribed WorkPulse features, subject to these Data Processing Terms.

Schedule 4 — WorkPulse-Specific Retention, Return and Deletion

Applies only where the Customer subscribes to WorkPulse. This Schedule supplements clause 9, which continues to govern retention at cessation of the Customer's WorkPulse subscription.

Data category	Retention period
Working-hours and productivity records	Up to 90 days.
Device activity and location history	Up to 30 days.
Dashboard display window	The interface may display a shorter period than the underlying retention period.
Customer-exported reports	Controlled by the Customer once exported from WorkPulse.

On termination, the Customer may choose return or deletion in accordance with clause 9. Live and actively accessible Customer Personal Data shall be dealt with within the period specified in that clause. Data held in backup or archive media shall be placed beyond use and securely deleted on expiry of the applicable backup-retention cycle.

Schedule 5 — WorkPulse-Specific Technical and Organisational Measures

Applies only where the Customer subscribes to WorkPulse. This Schedule supplements clause 4, setting out specific measures in addition to the general standard required by that clause.

Control area	Measure	Confirmed
Tenant segregation	Per-organisation row-level security to prevent one Customer from accessing another Customer's data.	Yes
Access control	Role-based access control for Authorised Users.	Yes
Encryption in transit	Industry-standard encrypted transport for network communications.	Yes
Encryption at rest	Encryption of hosted data and backups at rest.	Yes
Privileged access	MFA and least-privilege controls for privileged access.	Yes
Logging and review	Administrative access logging and periodic review.	Yes
Vulnerability management	Patch, dependency and vulnerability-management processes.	Yes
Backup and recovery	Documented backup, recovery and resilience arrangements.	Yes
Incident management	Documented security incident and personal-data-breach procedures.	Yes

Personnel security	Confidentiality, training and prompt access removal for leavers.	Yes
--------------------	--	-----