

IKON ICT

Data Processing Addendum

Controller-to-Processor terms for Ikon ICT services

Ikon Comms Ltd trading as Ikon ICT | Version 1.0 | Effective from 5 October 2026

Parties and status

This Data Processing Addendum (“DPA”) forms part of the contract between the customer identified in an Order (“Controller”) and Ikon Comms Ltd trading as Ikon ICT, company number 17119071, registered office 20 Wenlock Road, London, England, N1 7GU (“Processor”). It applies only where Ikon ICT processes Personal Data on behalf of the Controller. Each party remains an independent controller for personal data it processes for its own account, including relationship management, billing, legal compliance, security and fraud prevention.

1. Definitions and interpretation

“Applicable Data Protection Law” means the UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003 where applicable, and binding amendments or replacement legislation.

“Controller”, “Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Processing” and “Sub-processor” have the meanings given by Applicable Data Protection Law. “Services” and “Order” have the meanings in the Customer Terms.

If this DPA conflicts with the Customer Terms on data-processing matters, this DPA prevails. The Order and Schedule 1 define the processing. The commercial liability provisions in the Customer Terms apply to this DPA to the fullest extent permitted by law, except where Applicable Data Protection Law requires otherwise.

2. Scope and Controller instructions

The Processor shall process Personal Data only on the Controller’s documented instructions, including the Order, service tickets, authorised emails, approved configurations and this DPA, unless UK law requires other processing. If legally permitted, the Processor shall inform the Controller before carrying out legally required processing. The Processor shall promptly tell the Controller if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law and may pause the affected processing while the parties clarify the instruction.

The Controller is responsible for the lawfulness, fairness, accuracy and transparency of its processing and instructions; selecting lawful bases; issuing notices; responding to Data Subjects; and ensuring that it has authority to disclose Personal Data to the Processor.

3. Confidentiality and personnel

The Processor shall ensure that persons authorised to process Personal Data are subject to appropriate confidentiality obligations, receive data-protection and security guidance appropriate to their duties, and access Personal Data only to the extent required for the Services.

4. Security

Taking account of the state of the art, implementation costs, the nature, scope, context and purposes of processing, and risks to individuals, the Processor shall implement appropriate technical and organisational measures. The baseline measures in Schedule 2 apply where relevant to the ordered Service. No measure guarantees absolute security, and the Controller remains responsible for controls allocated to it in the Order or shared-responsibility model.

5. Personal Data Breaches

The Processor shall notify the Controller without undue delay after becoming aware of a confirmed Personal Data Breach affecting Personal Data processed under this DPA. The notice shall provide information reasonably available about the nature of the breach, affected data and individuals, likely consequences, measures taken or proposed, and a contact point. Information may be supplied in phases. The Processor shall take reasonable steps to contain and remediate the breach and shall not notify regulators or Data Subjects on the Controller’s behalf unless instructed or legally required.

6. Data Subject requests

Taking account of the nature of the processing, the Processor shall provide reasonable assistance through appropriate technical and organisational measures to enable the Controller to respond to requests concerning access, rectification, erasure, restriction, portability, objection or automated decision-making. If the Processor receives a request relating to Controller Personal Data, it shall forward it to the Controller without undue delay and shall not respond substantively unless authorised or legally required.

7. Compliance assistance

Taking account of the nature of processing and information available, the Processor shall provide reasonable assistance with security obligations, breach assessment and notification, data protection impact assessments and prior consultation. Assistance outside the ordinary scope of the Services may be charged at the agreed or standard rate where the need is not caused by the Processor's breach.

8. Sub-processors

The Controller gives general written authorisation for the Processor to use Sub-processors needed to provide the Services. The Processor shall maintain a current Sub-processor list or provide it on request, give reasonable advance notice of a material addition or replacement where practicable, and impose written data-protection obligations that provide materially equivalent protection for the relevant processing. The Processor remains responsible for its Sub-processors' performance of those obligations.

The Controller may object on reasonable data-protection grounds within 10 business days after notice. The parties shall seek a practical alternative. If none is reasonably available, either party may terminate the affected Service, subject to unavoidable disclosed third-party commitments and without affecting accrued rights.

9. International transfers

The Processor shall not make a restricted transfer of Controller Personal Data unless the transfer is based on an applicable adequacy regulation or an appropriate safeguard recognised by UK law, such as the UK International Data Transfer Agreement or UK Addendum, together with any required transfer risk assessment and supplementary measures. The Controller authorises transfers made by approved Sub-processors under such safeguards.

10. Return and deletion

On termination of the relevant Service, the Processor shall, at the Controller's choice and subject to technical capability, return or securely delete Controller Personal Data and delete remaining copies, unless UK law requires retention. Data in routine backups may remain until overwritten under normal cycles, provided it remains protected and is not restored except for continuity or recovery. Reasonable export or migration work may be chargeable unless included in the Order.

11. Information, audits and inspections

The Processor shall make available information reasonably necessary to demonstrate compliance with Article 28 obligations. The Controller shall first use current certifications, independent reports, policies and written responses where these reasonably address its request. If a further audit is reasonably required, it shall normally be conducted no more than once in 12 months, on at least 20 business days' notice, during business hours, without access to other customers' data or material security secrets, and at the Controller's cost. These limits do not apply following a material breach or regulator request. The auditor must be independent and bound by confidentiality.

12. Records, regulator cooperation and contact

The Processor shall maintain records required of processors and cooperate with the Information Commissioner's Office where legally required. Data-protection notices and operational queries should be sent to privacy@ikon-ict.com. Security incidents should be sent to abuse@ikon-ict.com and, for urgent operational support, support@ikon-ict.com.

Schedule 1: Processing details

Field	Default position
Subject matter	Remote and onsite IT support, Microsoft 365 and cloud administration, VoIP and connectivity support, security, backup or other managed services described in the Order.
Duration	For the term of the relevant Service, plus exit, backup-cycle and legal-retention periods described in the Contract.
Nature and purpose	Accessing, hosting where ordered, configuring, transmitting, troubleshooting, securing, backing up, restoring, migrating, deleting and otherwise processing Personal Data solely to provide and support the Services.
Data subjects	Controller staff, workers, volunteers, contractors, customers, service users, suppliers, professional contacts and other individuals whose data is held in systems covered by the Order.
Personal Data	Names, business and personal contact details, account identifiers, user and access data, device and network information, email and document content, service tickets, call and usage metadata, configuration, audit and security logs, and other data visible during authorised support.
Special-category/criminal-offence data	Not intentionally required by default, but may be incidentally present in Controller systems. The Controller must identify higher-risk processing before access so suitable controls can be agreed.
Frequency	Continuous, periodic or ad hoc according to the Service and support requests.
Controller rights and obligations	Determine purposes and lawful bases; issue instructions and privacy information; maintain accurate authority and contacts; configure its use of the Services lawfully; assess risks; and exercise all controller rights under Applicable Data Protection Law.

Order-specific variations

The Order may supplement this Schedule with specific systems, locations, retention, categories of data, categories of individuals, documented instructions, residency requirements or prohibited processing. If special-category data, criminal-offence data, children's data or large-scale monitoring is expected, the parties should document the additional safeguards before processing.

Schedule 2: Baseline technical and organisational measures

- Identity and access management using individual accounts, least privilege and multi-factor authentication where supported and appropriate.
- Confidentiality obligations and access limited to personnel who need it to provide the Services.
- Supported-device, endpoint-protection, patching and vulnerability-management practices proportionate to the Service.
- Encryption in transit using accepted protocols and encryption at rest where supported by the relevant service or platform.
- Logging and monitoring proportionate to service risk, with security logs normally retained for 12 months unless the Order or platform provides otherwise.
- Backup and recovery controls where a managed backup Service is ordered; otherwise backup and restore-testing responsibilities remain with the Controller.
- Incident response, escalation, containment and evidence preservation procedures.
- Supplier and Sub-processor due diligence proportionate to risk and contractual data-protection obligations.
- Secure deletion or sanitisation appropriate to the media and service, subject to backup cycles and legal retention.
- Business-continuity and recovery arrangements appropriate to Ikon ICT's role and the ordered Service.

Schedule 3: Sub-processor categories

Category	Typical purpose
Cloud and productivity platforms	Microsoft 365, identity, email, collaboration and administrative services.
IT distribution and licensing	Provisioning and management of software subscriptions and licences.
Remote support and service desk	Ticketing, remote access, monitoring and support communications.
Hosting, backup and security	Hosting, backup, filtering, endpoint protection, logging and threat response.
Telecoms and connectivity	Voice, SIP, numbering, broadband, carrier and network services.
Billing and accounting	Invoicing, payment administration, accounting and statutory records.
Professional services	Insurers, legal advisers, auditors and incident specialists where necessary.

The specific Sub-processors depend on the Order and current supplier arrangements. Ikon ICT maintains a separate Sub-processor Register containing current supplier names, locations where relevant and processing purposes. The Register is available to the Controller on request and is updated through the notice procedure in clause 8.