TETRABYTE

Data Processing Agreement

UK GDPR Article 28 terms for managed IT, cloud, communications, security, hosting and backup services

This Data Processing Agreement (DPA) forms part of the agreement between Tetrabyte Limited (company number 05546220, Portland Place, Hastings, East Sussex, TN34 1QN) (Tetrabyte) and the client named in the Contract (the Client). It applies whenever Tetrabyte processes personal data on the Client's behalf in providing the Services.

1. Definitions

1.1 In this DPA:

Applicable Data Protection Law: the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and any other UK law about personal data, each as amended or replaced from time to time.

Client Personal Data: personal data that Tetrabyte processes on the Client's behalf in providing the Services, including data about the Client's staff, customers, suppliers, website visitors and callers.

Contract: the agreement between the Client and Tetrabyte for the Services, including the Terms and Conditions, quotation, service-specific terms and this DPA.

Services: the managed IT, cloud, communications, security, hosting, backup and related services Tetrabyte provides under the Contract.

Sub-processor: a supplier or subcontractor that Tetrabyte engages and that processes Client Personal Data. The Sub-processors in use are listed in Annex 3.

Restricted Transfer: a transfer of Client Personal Data to a country or organisation outside the UK to which Chapter V of the UK GDPR applies.

Personal Data Breach, controller, processor, personal data, processing, data subject: have the meanings given in the UK GDPR.

2. Roles

2.1 **Client as controller.** For Client Personal Data, the Client is the controller (or, where it processes the data for another organisation, a processor) and Tetrabyte is the Client's processor.

2.2 **Tetrabyte's own data.** Tetrabyte is a controller of personal data it holds for its own business purposes, such as contact, billing, sales, account management and fraud-prevention records. That data is governed by Tetrabyte's privacy notice and not by this DPA.

2.3 **Client responsibilities.** The Client is responsible for having a lawful basis to process Client Personal Data and to instruct Tetrabyte, for giving complete and lawful instructions, for telling its staff and customers that their data may be managed by Tetrabyte, and for maintaining accurate user and access lists.

3. Details of the processing

3.1 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 Annex 1.

4. Instructions

4.1 Tetrabyte will process Client Personal Data only on the Client's documented instructions, including with regard to Restricted Transfers, unless UK law requires otherwise. In that case Tetrabyte will tell the Client before processing unless the law prohibits it.

4.2 The Contract, this DPA, approved quotations, support tickets and other retained written requests from authorised Client contacts are the Client's documented instructions. Verbal instructions may be acted on where the Contract allows, and Tetrabyte will record them in the ticket.

4.3 Account-wide, security-sensitive, access-control, export, deletion or disclosure decisions must come from a Client Decision Maker or authorised contact. If authority is unclear, Tetrabyte will pause the processing unless immediate action is reasonably needed to contain a security incident and the Contract allows it.

4.4 Tetrabyte will tell the Client if, in its opinion, an instruction infringes Applicable Data Protection Law, and is not required to carry out an instruction that it believes is unlawful.

4.5 Disclosure. Tetrabyte may disclose Client Personal Data where the law requires it and, as set out in the Terms and Conditions, may tell the appropriate authorities and the Client's senior team if it finds unlawful activity while providing the Services.

5. Confidentiality

5.1 Tetrabyte will ensure that everyone it authorises to process Client Personal Data is bound by a duty of confidentiality and has access only where needed for their task.

6. Security

6.1 Tetrabyte will apply technical and organisational measures appropriate to the risk, as required by Article 32 UK GDPR. The measures in force at the date of this DPA are summarised in Annex 2. Tetrabyte may update them if the level of protection is not reduced.

7. Sub-processors

7.1 General authorisation. The Client authorises Tetrabyte to engage the Sub-processors listed in Annex 3 for the Services the Client takes. A Sub-processor is relevant to the Client only where the Client's Services use it. Where the Contract requires specific authorisation for a named Sub-processor, the Contract applies.

7.2 Changes. Tetrabyte will tell the Client with reasonable advance notice before a new or replacement Sub-processor starts to process Client Personal Data, by email to the Client's authorised contact and by updating Annex 3. The Client may object on reasonable data protection grounds within the notice period. Tetrabyte will then discuss the concern in good faith and, where practicable, not use the new Sub-processor for the Client's data. If that is not possible, the Client may end the affected Service without penalty for that Service. Where an urgent change is needed for security or continuity, Tetrabyte will notify the Client as soon as practicable and follow the objection process afterwards.

7.3 Flow-down and liability. Tetrabyte will take reasonable steps to bind each Sub-processor to data protection obligations that give materially equivalent protection, using the Sub-processor's data processing terms where it will only offer its standard terms. Tetrabyte remains liable to the Client for each Sub-processor's performance of its data protection obligations.

7.4 Independent recipients and Client-owned suppliers. Some organisations, such as couriers, network operators, hardware distributors, manufacturer warranty portals and regulators, receive limited data and use it for their own purposes under their own terms. They are not Sub-processors and are described in Annex 4. Where the Client holds the contract with a supplier and Tetrabyte sets up or administers the service on the Client's instruction, that supplier is the Client's own supplier and not Tetrabyte's Sub-processor.

7.5 Suppliers brought in by a Sub-processor. Some Sub-processors provide a Service by engaging their own suppliers, for example a marketplace or wholesaler engaging the vendor of the product. Where Annex 3 names that supplier, or where the Sub-processor publishes a list of its own sub-processors and gives notice of changes under its terms, the Client authorises their use for the Services the Client takes. Tetrabyte will seek written confirmation that its Sub-processors bind

their own sub-processors to data protection obligations in line with Article 28(4) of the UK GDPR, and will give the Client a link to the relevant published list on request.

8. International transfers

8.1 Tetrabyte will take reasonable steps to ensure that a Restricted Transfer of Client Personal Data (including by allowing remote access from outside the UK) is made only where the Contract allows it and a lawful transfer mechanism applies to the Sub-processor concerned. Accepted mechanisms are UK adequacy regulations (including the UK extension to the EU-US Data Privacy Framework where the recipient is certified), the UK International Data Transfer Agreement, and the UK Addendum to the EU standard contractual clauses.

8.2 Tetrabyte does not promise UK-only or EU-only processing, hosting or support for any Service unless the supplier has confirmed it in writing or Tetrabyte has checked the Client's own configuration. On request Tetrabyte will tell the Client the hosting and support locations and the transfer mechanism recorded for any Sub-processor that handles its data.

9. Assistance to the Client

9.1 **Data subject requests.** Taking account of the nature of the processing, Tetrabyte will help the Client respond to requests from individuals. If Tetrabyte receives a request about Client Personal Data directly, it will not respond itself unless the law requires, and will pass it to the Client without undue delay.

9.2 **Security, breaches and impact assessments.** Tetrabyte will help the Client meet its obligations under Articles 32 to 36 UK GDPR (security, breach notification, data protection impact assessments and prior consultation), taking account of the information available to Tetrabyte. Assistance outside the scope of the Services may be chargeable, but charges will not be used to delay the Client meeting a legal deadline.

10. Personal Data Breaches

10.1 Tetrabyte will notify the Client without undue delay after becoming aware of a Personal Data Breach affecting Client Personal Data. Tetrabyte becomes aware when it has a reasonable degree of certainty that a breach affecting Client Personal Data has occurred; for a breach at a Sub-processor, that is when the Sub-processor notifies Tetrabyte or Tetrabyte otherwise has that certainty. The notice will give the information then available (what happened, the data and Services affected, likely consequences, and the measures taken or proposed) and further information in phases as the investigation develops. Tetrabyte will give reasonable help to the Client to assess the risk and decide whether to notify the ICO or individuals.

10.2 As controller, the Client decides whether to notify the ICO or individuals. Tetrabyte will not notify them on the Client's behalf unless the Client authorises it or the law requires it.

11. Return and deletion

11.1 When the Services end, Tetrabyte will, at the Client's choice, return or delete Client Personal Data and delete existing copies within a reasonable period after the Client's written instruction, unless UK law requires the data to be kept. Retention periods that apply to particular Services (for example backup retention and support records kept for transition) are in the service-specific terms and the Client's written instruction overrides a default retention period where the Contract allows.

11.2 Where data sits in protected backup cycles and cannot be deleted immediately, Tetrabyte will isolate it from normal use, keep it only for the remaining cycle and delete or overwrite it under the applicable schedule. On request Tetrabyte will confirm in writing that deletion is complete.

12. Information and audits

12.1 Tetrabyte will make available the information reasonably necessary to show that it complies with Article 28 UK GDPR and will allow and contribute to audits and inspections by the Client or its

auditor, no more than once in any 12 months unless a Personal Data Breach or a regulator requires otherwise, on reasonable written notice, in working hours, subject to confidentiality and to reasonable arrangements on scope, timing and cost. Tetrabyte may meet a request using existing independent reports, certifications, policies, questionnaires or remote evidence where they give suitable assurance. An audit must not compromise the security or confidentiality of other clients, Tetrabyte systems, staff data or supplier confidential information.

13. Liability, term and precedence

13.1 Liability. Tetrabyte's liability to the Client under or in connection with this DPA is subject to the limits and exclusions in the Contract, including those in the Terms and Conditions on indirect and consequential loss and on the total amount payable. It counts towards, and does not add to, the total limit in the Contract. Nothing in this DPA limits liability that cannot lawfully be limited, or a data subject's rights against either party.

13.2 This DPA starts when Tetrabyte first processes Client Personal Data under the Contract and continues until all Client Personal Data has been returned or deleted under clause 11. If this DPA conflicts with the rest of the Contract on a data protection matter, this DPA prevails.

13.3 Tetrabyte may update this DPA and its Annexes to reflect changes in law, guidance or the Services, giving the Client reasonable written notice of any change that reduces the Client's protection. The Annex 3 process in clause 7.2 applies to Sub-processor changes. This DPA is governed by the law of England and Wales.

13.4 Contact. Tetrabyte's contact for this DPA, including requests and notices under it, is James Cuthbert, Company Director, who can be reached at support@tbyte.com. Tetrabyte may change its contact by telling the Client.

Annex 1: Details of the processing

Item	Details
Subject matter	Tetrabyte's provision of the Services described in the Contract.
Duration	The term of the Contract, plus the return and deletion period in clause 11.
Nature of the processing	Access, viewing, collection, storage, transmission, backup, restoration, alteration, deletion and destruction, as needed to deliver the Services.
Purpose	To provide, support, secure, host, back up, migrate and bill for the Services the Client has ordered, and to follow the Client's documented instructions.
Categories of data subjects	The Client's staff and contractors; the Client's customers and suppliers; callers and call recipients; website visitors and form submitters; guests on managed Wi-Fi; other individuals whose data is held in systems Tetrabyte administers.
Special category data	Tetrabyte does not seek special category or criminal offence data. Such data may be held in the Client's systems (for example HR, health or safeguarding records) and may be incidentally encountered during support. The Client is responsible for telling Tetrabyte where such data is held and for any extra safeguards it needs.

Types of personal data by service area (the Services actually used are those in the Client's Contract):

Service area	Likely personal data
Managed IT support and on-site support	Device and user identity, user names, business files, emails, logs, screen contents and information seen during remote or on-site troubleshooting; support session data, chat logs, call recordings and satisfaction survey responses.
Remote access and monitoring	Device name, user, operating system, IP and network data, connection status, installed software and configuration, screenshots, inventory, health telemetry, remote session content, and login logs on Tetrabyte-hosted and Client systems. The software may stay installed to help with future support until removed.
Microsoft 365, Entra, Exchange, SharePoint, OneDrive, Intune; Azure, Windows 365, Azure Virtual Desktop	User identities, mailboxes, messages, files, groups, sign-in and device management information; hosted server and desktop data, user profiles, logs and backups.
Hosted voice and telephony	Names, addresses, telephone numbers, call records, voicemail and call recordings.
Mobile telephony and connectivity	Subscriber and contact data, telephone numbers, service address, usage and billing records, fault information.
Backup (server and Microsoft 365)	Server files, mailboxes, OneDrive and SharePoint data, backup metadata and restored copies, as the Client selects.
Website hosting and domains	Website account data, form submissions, databases, logs, domain registrant contacts and backups where included.
Security tooling (antivirus, MDR, vulnerability scanning, Cyber Essentials)	Device and user identity, detections, suspicious files or metadata, IP addresses, telemetry, device inventories and configuration evidence.
Security awareness training, phishing simulation, dark-web monitoring	Employee names and work emails, training and test results, exposed email addresses and credentials.
Email signature and email security services	Names, roles, contact details, directory attributes, email content and routing metadata.
Mobile device and network management	Device serials, owner names and emails, installed apps, location where enabled, network client lists and MAC addresses, guest Wi-Fi sign-in data.
Customer-owned tools that Tetrabyte sets up or administers (for example staff-activity monitoring, VPN networks, software licences)	User names, work emails and account or licence details. Where the Client uses a staff-activity monitoring tool that Tetrabyte administers on the Client's instruction, also the activity and application-use data (and screenshots, if the Client switches them on) that the tool records about the Client's staff. The Client decides whether to monitor, tells its staff and is responsible for its own lawful basis; Tetrabyte only sets up and administers the tool.
Courier, equipment return and data destruction	Contact name, collection or delivery address, telephone and email, device identifiers and data held on storage media.
Project and IT Director services	As set out in the agreed scope: system inventories, user and access information, reports and project records.

Annex 2: Security measures (summary)

- Identity controls: unique named accounts, multi-factor authentication, privileged access restriction and prompt removal of leaver access.
- Endpoint protection, supported software, security updates, secure configuration and malware controls on systems used to deliver the Services.
- Encryption in transit and, where supported and appropriate, at rest.
- Network security, tenant separation and controlled remote access.
- Logging and monitoring proportionate to privileged and security-sensitive activity.
- Backup, restoration and resilience arrangements appropriate to the contracted Service.
- Physical security for equipment and storage media held at Tetrabyte premises or in transit.
- Staff confidentiality, data protection awareness and role-appropriate security training.
- Incident response, vulnerability management, supplier management and periodic control review.
- Tetrabyte holds Cyber Essentials certification (not Cyber Essentials Plus) and keeps it renewed.

Annex 3: Sub-processors

These suppliers may process Client Personal Data on Tetrabyte's behalf for the Services shown. A Sub-processor is relevant to the Client only where the Client's Services use it; some are listed because they are available to clients (marked 'where sold', 'where used' or 'where a customer takes the service'). A supplier marked 'to be engaged' will not process Client Personal Data until Tetrabyte has finished onboarding with it. Where Tetrabyte buys a service through another supplier (marked 'via Giacom' or 'via Brigantia'), both that supplier and the vendor it brings in are covered, and clause 7.5 applies to their own sub-processors. Hosting locations and transfer mechanisms are provided on request (clause 8.2). Last updated: 9 November 2026.

Sub-processor	Service supported	Personal data that may be involved
Cloud, hosting and identity		
Microsoft	Microsoft 365, Entra ID, Exchange Online, SharePoint, OneDrive, Intune, Azure, Windows 365 and Azure Virtual Desktop (customer tenants and Tetrabyte's own)	User identities, mailboxes, messages, files, groups, sign-in and device information
Giacom (Cloud Market)	Cloud marketplace, licensing and billing platform through which Tetrabyte buys cloud services (Microsoft, Acronis, Bitdefender, Exclaimer, usecure, Cirius, BitTitan and others), together with the suppliers Giacom brings in for each service	Customer organisation and administrator names and emails, tenant identifiers, licence orders
IONOS	Hosting of the virtual servers that run customer websites and Tetrabyte's internal systems (client notes, tickets), with datacentre networking and power	Website data and form submissions; client notes, ticket records, contact details and files held on those servers
Cloudflare	DNS, domain registration, proxy and content delivery	Domain registrant contacts, DNS records, visitor IP addresses and traffic metadata
Names.co.uk	Domain registration and web hosting accounts managed for customers	Domain registrant contacts, website administrator accounts, website data and form submissions
OVHcloud	Domain registration and web hosting accounts managed for customers	Domain registrant contacts, website administrator accounts, website data and form submissions
Remote support and device management		
ConnectWise (ScreenConnect)	Remote support and access agents	Device names, user names, IP addresses and session content
Bitwarden	Password manager holding credentials for customer systems	Credentials and account identifiers for customer systems
Jamf Now	Mobile device management, where a customer takes the service	Device serials, owner names and emails, installed apps, location where enabled
Samsung Knox MSP	Mobile device management, where a customer takes the service	Device serials, owner names and emails, installed apps, location where enabled
Apple Business Manager	Apple device enrolment and management, where a customer takes the service	Device serials, managed Apple account names and emails
SOTI	Mobile device management, where a customer takes the service	Device serials, owner names and emails, installed apps, location where enabled
Cisco Meraki	Cloud dashboard for managed customer networks, where a customer's network uses it	Network client lists (device names, MAC addresses), usage data and administrator account details
Ubiquiti (UniFi cloud)	Cloud consoles for managed customer networks	Network client lists (device names, MAC addresses) and administrator account details
Fydelia	Guest Wi-Fi captive portals for UniFi networks, where a customer uses it	Guest names, emails, phone numbers, device MAC addresses and login times
DrayTek (VigorACS)	Central management of customer routers	Router configuration, VPN user names and device identifiers
Security and email protection		
Bitdefender (via Giacom)	Endpoint protection, patch management and managed detection and response	Device and user identity, detections, suspicious file metadata, IP addresses and telemetry
Sophos	Sophos Central endpoint and firewall management for some customers	Device and user identity, detections, IP addresses and telemetry

Sub-processor	Service supported	Personal data that may be involved
Avast Business / AVG	Endpoint protection for customers still on it (being replaced)	Device and user identity, detections, IP addresses and telemetry
KnowBe4 (via Brigantia)	Security awareness training and phishing simulation	Employee names, work emails, training completion and phishing-test results
usecure (via Giacom)	Security awareness training	Employee names, work emails, training completion and test results
CyberSmart (via Brigantia)	Cyber Essentials assessment and compliance platform	Staff and device inventories, configuration evidence, vulnerability results
Brigantia / Elovade	Distributor for CyberSmart, KnowBe4 and Rootshell	Customer organisation and administrator contact details
Rootshell Security	Vulnerability scanning and penetration testing, where sold	IP addresses, system and vulnerability data
InsecureWeb	Dark-web monitoring of customer domains and email addresses	Email addresses, domains and exposed credentials found
Exclaimer (via Giacom)	Email signature management	Staff names, roles, contact details and directory attributes
Crossware	Email signature management	Staff names, roles, contact details and directory attributes
CodeTwo	Email signature management, where sold	Staff names, roles, contact details and directory attributes
Mesh Security	Cloud email security, where sold	Email content and metadata
Cirius / DeliverySlip (via Giacom)	Secure email messaging, where sold	User identifiers and encrypted message content
Backup, storage and migration		
Acronis (via Giacom)	Cyber Protect Cloud backup	Backed-up files, mailboxes and server data, and backup metadata
Dropbox	Storage destination for AhsayCBS backup sets	Backed-up customer data
BitTitan (via Giacom)	Mailbox and file migration, where used	Mailbox and file content during migration, user identities
Voice, connectivity and switching		
8x8	Hosted voice and contact centre	User names, numbers, call records, voicemail and recordings
Onecom Partners Limited (Gradwell)	Hosted voice platform	User names, numbers, call records, voicemail and recordings
BT Wholesale (HV.Select / BroadWorks)	Hosted voice and wholesale lines, including Openreach lines supplied through Giacom	User names, numbers, call records, voicemail, recordings and line details
Tollring	Call analytics on the hosted voice platform, where used	Call records and user names
Cisco (Webex for BroadWorks)	Softphone and collaboration client on the hosted voice platform, where used	User provisioning data
Giacom Comms	Broadband, PSTN, mobile and voice wholesale, together with the carriers and network providers Giacom brings in for each service	Customer and site contact details, numbers, line and usage records
Yealink (YMCS)	Handset provisioning	Phone MAC addresses or serials, extensions, SIP identity and provisioning details
Snom (SRAPS)	Handset provisioning	Phone MAC addresses or serials, extensions, SIP identity and provisioning details
Poly (Zero Touch Provisioning)	Handset provisioning	Phone MAC addresses or serials and provisioning redirect details
TOTSCo	Switching hub for moving broadband and landlines between providers	Customer name, address, telephone numbers and line identifiers in switch orders
Billing and logistics		
Intelligent Billing (p-rd.com)	Telecoms billing and invoicing platform	Customer names, billing contacts, call and usage records
World Options	Courier and postage booking platform	Recipient name, address, telephone and email

Sub-processor	Service supported	Personal data that may be involved
Fidelity Group (to be engaged)	Wholesale telecoms, energy and payments services, where a customer takes them through Fidelity, once onboarding is complete	Customer and site contact details and account details for the services ordered

Annex 4: Independent recipients (for information)

These recipients use the personal data they receive for their own purposes under their own terms. Tetrabyte shares only what each needs.

Category	Examples	Personal data shared
Network operators and carriers	O2, Vodafone, KCom, CityFibre, Lightning Fibre, G.Network	Subscriber and installation contact details, site addresses, line identifiers
Hardware distributors and resellers	TD Synnex, Laptops Direct	Delivery name, address, telephone and email; returns and serial-number details
Couriers and postal services	DHL Express, Royal Mail, UPS, Parcelforce, DPD	Recipient and collection name, address, telephone and email; parcel description
Manufacturer warranty and support portals	Dell, HP	End-user organisation and contact name; device serial numbers
Payment collection	GoCardless	Payer name, email, address and bank details for clients who pay by Direct Debit
Security software vendors acting as joint controllers	Bitdefender	Business contact details of the people who administer a service (joint controller arrangement under its reseller terms)
Backup vendor, for its own account and service data	Acronis (the backup content itself is covered in Annex 3)	Administrator contact details, licensing and billing data, and service-usage and device telemetry, which Acronis handles as an independent controller under its DPA
Referral partners	BigChange	Contact details of a client Tetrabyte refers, passed on with the client's agreement