Data Processing Agreement

Between the Customer as controller and TeamTalk as processor, for personal data processed through the TeamTalk service. Drafted to contain the terms required by Article 28(3) of the UK GDPR and to satisfy the Information Commissioner's published checklist of what a controller to processor contract must set out.

> **BASIS OF THIS AGREEMENT**
>
> Article 28(3) of the UK GDPR requires that processing by a processor is governed by a contract that "sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller", and that stipulates the eight matters at Article 28(3)(a) to (h). Each of those eight is marked in the margin of clause 4 below. Annex 1 supplies the descriptive detail required by the opening words of Article 28(3). The Information Commissioner does not publish its own set of Article 28 standard clauses, although Article 28(8) gives it the power to; this agreement is drafted against the statutory wording and the Commissioner's checklist rather than against any approved form.

Parties and effect

Processor	[TeamTalk Ltd], company number [number], registered office [address] ("**TeamTalk**")
Controller	[Customer legal name], company number [number], registered office [address] ("**the Customer**")
Principal agreement	The [order form / subscription agreement / pilot agreement] between the parties dated [date] (the "**Principal Agreement**")
Effective from	[date], and in any event from the date on which TeamTalk first processes personal data on the Customer's behalf

This agreement forms part of and is subject to the Principal Agreement. Where this agreement and the Principal Agreement conflict on any matter of data protection, **this agreement prevails**. Where this agreement conflicts with a transfer mechanism entered into under clause 7, the transfer mechanism prevails to the extent of the conflict.

1. Definitions

"**UK GDPR**", "**controller**", "**processor**", "**personal data**", "**processing**", "**data subject**", "**personal data breach**" and "**supervisory authority**" have the meanings given in the UK GDPR and the Data Protection Act 2018. "**Data Protection Legislation**" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any successor or amending legislation, including the Data (Use and Access) Act 2025. "**Customer Personal Data**" means personal data processed by TeamTalk on the Customer's behalf under the Principal Agreement, as described in Annex 1. "**Sub-processor**" means a processor engaged by TeamTalk to process Customer Personal Data. "**Restricted Transfer**" means a transfer of Customer Personal Data to a third country or international organisation to which Article 44A of the UK GDPR applies.

2. Roles of the parties

1. The Customer is the **controller** and TeamTalk is the **processor** in respect of Customer Personal Data. The Customer determines the purposes and means of the processing; TeamTalk carries it out on the Customer's behalf.
2. The Customer warrants that it has a lawful basis for the processing it instructs, that it has given the data subjects the privacy information required by Articles 13 and 14 of the UK GDPR, and that its instructions to TeamTalk will not cause TeamTalk to breach the Data Protection Legislation. TeamTalk relies on this warranty and does not assess the lawfulness of the Customer's own processing.
3. TeamTalk is a controller in its own right, and this agreement does not apply, in respect of: its own personnel and business contact data; billing and account records; and security, fraud prevention and service telemetry that does not

identify the Customer's workers. Where TeamTalk acts as a controller it does so under its own privacy notice at [https://team-comms.com/privacy].

4. If TeamTalk determines the purposes and means of processing Customer Personal Data other than as instructed, it is a controller in respect of that processing, as Article 28(10) of the UK GDPR provides.

3. Details of the processing

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**, as required by Article 28(3) of the UK GDPR. The parties will keep Annex 1 accurate and will update it in writing if the processing changes.

4. TeamTalk's obligations as processor

1. Art 28(3)(a) **Documented instructions.** TeamTalk will process Customer Personal Data **only on the Customer's documented instructions**, including in relation to any Restricted Transfer, unless required to process by law, in which case TeamTalk will inform the Customer of that legal requirement before processing unless the law prohibits it from doing so on important grounds of public interest.

   1.1 The Customer's documented instructions are: this agreement; the Principal Agreement; the configuration options the Customer sets on its tenant; and any further written instruction the parties agree. Use of the Service by the Customer's authorised administrators is an instruction.

   1.2 TeamTalk will **immediately inform the Customer if, in its opinion, an instruction infringes** the UK GDPR or other Data Protection Legislation, and may suspend performance of that instruction until it is withdrawn, amended or confirmed in writing.

   1.3 If the Customer's instruction requires TeamTalk to do something outside the scope of the Service, TeamTalk may charge for the additional work at its then-current rates, having told the Customer the cost first.

2. Art 28(3)(b) **Confidentiality.** TeamTalk will ensure that every person authorised to process Customer Personal Data **has committed themselves to confidentiality** or is under an appropriate statutory obligation of confidentiality. Those commitments survive the end of the individual's engagement. Access is limited to personnel who need it to provide the Service or to comply with law, and each such person receives data protection and security briefing on joining and at least annually.

3. Art 28(3)(c) **Security.** TeamTalk will take **all measures required by Article 32** of the UK GDPR. Taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk to data subjects, TeamTalk implements and maintains the technical and organisational measures set out in **Annex 2**. TeamTalk may update those measures, but not so as to reduce the overall level of security, and will publish the current version at [https://team-comms.com/security].

4. Art 28(3)(d) Art 28(2) Art 28(4) **Sub-processors.**

   4.1 The Customer gives TeamTalk **general written authorisation** to engage the Sub-processors listed in **Annex 3**, and to engage further Sub-processors in accordance with this clause.

   4.2 TeamTalk will **inform the Customer in writing of any intended addition or replacement of a Sub-processor at least 30 days before that Sub-processor begins processing**, by email to the Customer's notice address and by updating the list published at [https://team-comms.com/sub-processors]. The Customer may subscribe to notification of changes to that page.

   4.3 **Right to object.** The Customer may object to a new or replacement Sub-processor on reasonable data protection grounds by written notice within **30 days** of being informed. The parties will discuss the objection in good faith. If TeamTalk cannot, within 30 days of the objection, offer a reasonable alternative or a change that resolves the objection, **the Customer may terminate the Principal Agreement, without penalty, on 30 days' written notice, with a pro rata refund of fees paid for the unexpired period** of the then-current term. That is the Customer's sole remedy for an objection under this clause.

   4.4 TeamTalk will impose on each Sub-processor, by written contract, **the same data protection obligations as are set out in this agreement**, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organisational measures. **Where a Sub-processor fails to fulfil its data protection obligations, TeamTalk remains fully liable to the Customer for the performance of that Sub-processor's obligations.**

4.5 TeamTalk will make available to the Customer, on request, the data protection terms of its contract with any Sub-processor, redacted only as necessary to protect commercially confidential information.

4.6 An emergency replacement of a Sub-processor required to maintain the security or availability of the Service may be made on shorter notice, with the reasons given to the Customer in writing at the time and the objection right in clause 4.4.3 preserved.

5. Art 28(3)(e) **Assistance with data subject rights.** Taking into account the nature of the processing, TeamTalk will **assist the Customer by appropriate technical and organisational measures, insofar as this is possible**, in fulfilling the Customer's obligation to respond to requests to exercise the rights in Chapter III of the UK GDPR, being the rights of access, rectification, erasure, restriction, portability and objection, and rights relating to automated decision-making.

5.1 The Service allows the Customer's administrators to locate, view, correct, export and delete an individual worker's record without TeamTalk's involvement. Where the Customer needs further help, TeamTalk will respond within **[5] working days** of a written request.

5.2 If a data subject contacts TeamTalk directly about Customer Personal Data, TeamTalk will not respond substantively but will **forward the request to the Customer without undue delay** and tell the data subject that it has done so.

5.3 Assistance under this clause is provided at no charge unless the volume or complexity of requests is materially beyond the ordinary operation of the Service, in which case TeamTalk may charge its reasonable costs, notified in advance.

6. Art 28(3)(f) **Assistance with Articles 32 to 36.** Taking into account the nature of the processing and the information available to it, TeamTalk will assist the Customer in ensuring compliance with its obligations under Articles 32 to 36 of the UK GDPR, being security of processing, notification of personal data breaches to the Information Commissioner and to data subjects, data protection impact assessments and prior consultation. TeamTalk maintains a pre-completed data protection impact assessment pack describing the Service, which it will supply on request to assist the Customer's own assessment. The Customer remains responsible for carrying out and recording its own assessment.

7. Art 28(3)(g) **Deletion or return. At the choice of the Customer**, TeamTalk will delete or return all Customer Personal Data after the end of the provision of services relating to processing, and will delete existing copies unless required by law to store them.

7.1 Unless the Customer instructs otherwise in writing before the end of the period, TeamTalk will make Customer Personal Data available for export in a machine-readable format for **30 days** after the end of the Principal Agreement, and will then **delete it within a further 30 days**.

7.2 Customer Personal Data present in encrypted backups is not restored into the live environment and is **deleted when the backup expires, within [30] days**. Until then it remains subject to this agreement, including the security measures in Annex 2.

7.3 TeamTalk will confirm deletion in writing on request.

7.4 Where TeamTalk is required by law to retain Customer Personal Data, it will inform the Customer of the requirement, retain only what the law requires, and continue to protect it under this agreement.

8. Art 28(3)(h) **Information and audits.** TeamTalk will **make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28, and allow for and contribute to audits, including inspections**, conducted by the Customer or another auditor mandated by the Customer.

8.1 TeamTalk will satisfy this obligation in the first instance by supplying its current security summary, its Cyber Essentials certificate, its sub-processor list, its policies and its answers to the Customer's information security questionnaire.

8.2 If that is not sufficient, the Customer may audit TeamTalk's processing, in person or remotely, **once in any 12-month period** on at least **30 days' written notice**, during normal business hours, for no longer than [two] working days, and subject to confidentiality undertakings. The Customer will minimise disruption and will not access the personal data or confidential information of any other TeamTalk customer.

8.3 The Customer may audit more frequently, and on shorter notice, where required to do so by a supervisory authority or following a personal data breach affecting Customer Personal Data.

8.4 Each party bears its own costs. The Customer will pay TeamTalk's reasonable costs of an audit that goes beyond one audit in any 12-month period, unless the audit reveals a material breach by TeamTalk.

8.5 Nothing in this clause limits the Customer's or a supervisory authority's statutory rights.

5. Personal data breaches

1. TeamTalk will **notify the Customer without undue delay after becoming aware of a personal data breach** affecting Customer Personal Data, as Article 33(2) of the UK GDPR requires. **TeamTalk commits to notifying the Customer within 24 hours of becoming aware**, so that the Customer has time to meet its own obligation under Article 33(1) to notify the Information Commissioner without undue delay and, where feasible, not later than 72 hours after it becomes aware.
2. The notification will be sent to the Customer's notice address in Annex 1 and will describe, so far as known at the time: the nature of the breach including, where possible, the categories and approximate number of data subjects and of records concerned; the name and contact details of TeamTalk's contact point; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. Where the information is not all available at once, TeamTalk will provide it in phases without further undue delay.
3. TeamTalk will take all reasonable steps to contain, investigate and remediate the breach, will preserve evidence, and will provide a written post-incident report within [10] working days of containment.
4. TeamTalk will assist the Customer in communicating the breach to data subjects under Article 34 where the Customer decides that is required.
5. **TeamTalk will not notify the Information Commissioner or any data subject on the Customer's behalf, and will not make any public statement identifying the Customer, unless the Customer instructs it to in writing or TeamTalk is required to by law.** Nothing in this clause prevents TeamTalk from meeting its own legal obligations as a controller.

6. Records

TeamTalk maintains a record of all categories of processing carried out on behalf of the Customer, in accordance with Article 30(2) of the UK GDPR, and will make it available to the Customer or to the Information Commissioner on request.

7. International transfers

> **NOTE ON THE LAW AS IT NOW STANDS**
>
> Chapter V of the UK GDPR was substantially rewritten with effect from **5 February 2026** by section 85 of and Schedule 7 to the Data (Use and Access) Act 2025, commenced by SI 2026/82. **Articles 44 and 45 were omitted** and replaced by new Articles 44A, 45A, 45B and 45C, and Article 46 was amended. Sections 17A to 18 of the Data Protection Act 2018 were repealed, with existing adequacy regulations preserved and treated as made under Article 45A. Any transfer clause, transfer risk assessment or supplier questionnaire answer drafted before that date and citing Article 45 or section 17A is citing repealed provisions and must be refreshed.

1. TeamTalk will not make a Restricted Transfer of Customer Personal Data except in accordance with this clause, which is the Customer's documented instruction on transfers for the purposes of Article 28(3)(a).
2. The Customer authorises the Restricted Transfers described in **Annex 3**. TeamTalk will ensure that each is made on one of the bases permitted by Article 44A(2) of the UK GDPR, namely that it is approved by regulations under Article 45A, is made subject to appropriate safeguards under Article 46, or falls within a derogation under Article 49.
3. **Transfers to Twilio and to Mux** are made in reliance on the **UK Extension to the EU–US Data Privacy Framework**, given effect by the Data Protection (Adequacy) (United States of America) Regulations 2023 (SI 2023/1028), in force 12 October 2023, which are preserved by paragraph 26 of Part 2 of Schedule 9 to the Data (Use and Access) Act 2025 and now take effect as regulations under Article 45A. Neither a transfer risk assessment nor a separate transfer agreement is required for a transfer to an entity actively certified under the UK Extension for the relevant data. **TeamTalk will verify, at least annually and before relying on this route, that the receiving legal entity remains actively certified for the UK Extension on the Data Privacy Framework List**, and will move the transfer to the Article 46 route in clause 7.4 if it is not. TeamTalk notes that the UK adequacy regulations are independent of the European Commission's own adequacy decision for the United States, so a challenge to the latter would not automatically end this route.
4. **Transfers to OpenAI OpCo, LLC** are not covered by the Data Privacy Framework, under which OpenAI holds no certification. They are made subject to appropriate safeguards under Article 46, using the **International Data**

Transfer Addendum to the European Commission's Standard Contractual Clauses (version B1.0), or the **International Data Transfer Agreement (version A1.0)**, each issued by the Information Commissioner under section 119A of the Data Protection Act 2018, laid before Parliament on 2 February 2022 and in force from 21 March 2022. OpenAI's own data processing addendum adopts the Addendum route for United Kingdom data. TeamTalk holds a **documented transfer risk assessment** for that transfer, carried out against the test in Article 46(6), namely whether the standard of protection provided for the data subject after the transfer **would not be materially lower** than the standard provided under the UK GDPR and the Data Protection Act 2018, taken as a whole. TeamTalk will provide the assessment to the Customer on request and will review it at least annually and on any material change.

5. **Transfer minimisation.** As a design measure, **only the text content of a post, caption or comment is sent for translation. No name, phone number, email address or user identifier is sent to OpenAI.** The Customer is responsible for the content it publishes and should not include the personal data of identifiable individuals in the body of a post that will be translated. All Customer Personal Data at rest remains in the United Kingdom. OpenAI retains application programming interface inputs and outputs for up to 30 days for abuse monitoring and does not use them to train its models.

6. If a transfer mechanism relied on under this clause is invalidated, suspended or withdrawn, TeamTalk will inform the Customer without undue delay and will, at its option, adopt an alternative lawful mechanism, apply supplementary measures, or cease the transfer and the affected feature.

8. Liability

The parties' liability under this agreement is **governed by, and subject to, the limitations and exclusions of liability in the Principal Agreement**, which apply to this agreement as if set out here in full, and the caps in the Principal Agreement apply in aggregate across both agreements rather than separately to each. Nothing in this agreement or in the Principal Agreement limits or excludes a data subject's rights under the Data Protection Legislation, either party's liability to a supervisory authority, or any liability that cannot lawfully be limited or excluded. Where a claim is made against both parties by a data subject or a supervisory authority, each will bear the share of responsibility attributable to it under Article 82 of the UK GDPR.

9. Term, and general

1. This agreement takes effect on the date stated above and continues for as long as TeamTalk processes Customer Personal Data, and thereafter to the extent of clauses that by their nature survive, including clauses 4.2, 4.7, 4.8, 5 and 8.

2. TeamTalk may update this agreement on **30 days' written notice** where required by a change in law, in guidance from the Information Commissioner, or in the Service. No update may reduce the protections given to Customer Personal Data. If an update does so in the Customer's reasonable opinion, the Customer may object under the process in clause 4.4.3.

3. This agreement is in writing, including in electronic form, as Article 28(9) of the UK GDPR requires. It may be signed in counterparts and by electronic signature.

4. This agreement is governed by **the law of England and Wales** and the parties submit to the exclusive jurisdiction of the courts of England and Wales, without prejudice to any mandatory jurisdiction under the Data Protection Legislation.

Annex 1 · Details of the processing

Supplied as required by the opening words of Article 28(3) of the UK GDPR and by the Information Commissioner's contracts checklist.

Subject matter	The provision of the TeamTalk service: delivery of workplace notices, safety briefings and messages to the Customer's frontline workforce, translated into each recipient's chosen language, with recorded confirmation of receipt and an exportable record of who was told what and when.
Duration	The term of the Principal Agreement, plus the export and deletion periods in clause 4.7 (30 days for export, then deletion within a further 30 days, with backups aged out within [30] days).
Nature of the processing	Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, machine translation, transmission and dissemination, restriction, erasure and destruction; carried out by automated means on hosted infrastructure.
Purpose of the processing	To enable the Customer to communicate with its workforce, to record and evidence that individual workers have received and confirmed mandatory notices, to allow workers to report hazards, and to assist the Customer in discharging its own statutory duties to provide comprehensible information, instruction and training. Processing is carried out solely for the Customer's purposes and not for any purpose of TeamTalk's own.
Types of personal data	**Identity and contact:** first and last name; mobile telephone number; email address (optional); employee or payroll reference (optional). **Profile:** preferred language; job role or trade (optional); employer or subcontractor name; site, depot or team; user group membership; role within the tenant (administrator, moderator, worker); start date and leaving date. **Content:** the text of posts, comments and direct messages authored by or addressed to the individual, and machine translations of that text; video and audio uploaded by the Customer, including captions; hazard reports, including free text, a location and photographs, which may incidentally show identifiable individuals. **Usage and evidential records:** sign-in events and timestamps; confirmations of receipt of mandatory posts, with timestamps; read and delivery status; device and browser type; IP address; push notification subscription tokens. **Special category data:** none is required or requested. The Customer must not use the Service to process data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation, or data relating to criminal convictions and offences. Preferred language is collected to deliver translation and is not used or inferred as a proxy for nationality or ethnicity.
Categories of data subjects	The Customer's **employees**; **workers and agency staff** engaged by or through the Customer; **employees and operatives of subcontractors** working at the Customer's sites or on the Customer's contracts; the Customer's **managers, supervisors and administrators** who use the Service to publish and to monitor; and, incidentally, **any individual appearing in a photograph** attached to a hazard report or in video content published by the Customer.
Frequency	Continuous for the duration of the Principal Agreement.
Customer contact for data protection	Name [name] · role [role] · email [email] · telephone [number]. This is the address for breach notification under clause 5.2.
TeamTalk contact for data protection	Name [name] · email [privacy@team-comms.com] · telephone [number]. TeamTalk is not required to appoint a data protection officer under Article 37 of the UK GDPR and has not appointed one; this is the responsible named individual.
ICO registration	TeamTalk is registered with the Information Commissioner under registration number [number] and pays the annual data protection fee (tier 1, micro organisations, £52, or £47 by direct debit).

Annex 2 · Technical and organisational measures

The measures TeamTalk implements under clause 4.3 and Article 32 of the UK GDPR. Values in [square brackets] are confirmed per deployment. The full security summary is a separate document and forms part of this annex.

MEASURE	IMPLEMENTATION
Pseudonymisation and encryption **Art 32(1)(a)**	TLS 1.2 or above for all data in transit, with automatically renewed certificates and HTTP redirected to HTTPS. AES-256 encryption at rest on Amazon EBS volumes and Amazon S3 objects, including backups. Administrator passwords stored only as bcrypt hashes. Uploaded files served through short-lived signed URLs and never publicly listable. Only post content, and no identifiers, is sent to the translation sub-processor.
Confidentiality **Art 32(1)(b)**	Multi-tenant isolation enforced in the application layer: every record carries a tenant identifier and every query is scoped to the tenant resolved from the request domain. Role-based access within each tenant (administrator, moderator, worker). Sign-in by one-time code to a verified mobile number, with no worker passwords. Sessions expire after 30 days. Access revoked automatically, including mid-session, on a worker's recorded leaving date. Support impersonation is restricted to named TeamTalk personnel and every use is logged with operator, subject, tenant and timestamp. TeamTalk staff access to production uses individual named accounts, SSH keys and multi-factor authentication, on the principle of least privilege, with administrative accounts kept separate from day-to-day accounts and access reviewed [quarterly].
Integrity **Art 32(1)(b)**	Framework-level protection against SQL injection, cross-site scripting and cross-site request forgery, not disabled. Audit logging of administrator actions, impersonation, account creation and deletion, leaving-date changes, and publication and deletion of posts. Changes deployed from a protected branch under source control.
Availability and resilience **Art 32(1)(b)**	Hosted on Amazon Web Services in the **eu-west-2 (London)** region. Uptime and error monitoring with alerting to an on-call engineer. Databases and caches not reachable from the public internet; only HTTPS and restricted SSH exposed. Infrastructure reproducible through Laravel Forge.
Restoration **Art 32(1)(c)**	Encrypted database backups taken [daily] and retained [30] days in the same UK region. Object storage versioned. Recovery time objective [4] hours; recovery point objective [24] hours.
Testing and review **Art 32(1)(d)**	Restore to a scratch environment tested [quarterly] with the date and outcome recorded. Dependencies reviewed and updated [monthly] with automated vulnerability alerting. Operating system and application updates for vulnerabilities rated critical or high, or with a CVSS v3 base score of 7 or above, applied **within 14 days of release**, which is the Cyber Essentials requirement. Unsupported software removed or upgraded. [Independent penetration test carried out by [supplier] on [date].]
Organisational	Written confidentiality obligations for all personnel, surviving engagement. Security awareness briefing on joining and at least annually. Right to work checks. Access removed on the last working day. Written incident response procedure with a named owner. Information security policy aligned to the five Cyber Essentials control areas. Cyber Essentials certificate [number, date].
Certification	Cyber Essentials, certified by an IASME certification body against the current question set. TeamTalk is not certified to ISO/IEC 27001; a written information security management roadmap is available on request. TeamTalk does not claim certification it does not hold.

Annex 3 · Authorised sub-processors

Authorised under clause 4.4.1. The current list is published at [https://team-comms.com/sub-processors]. Changes are notified at least 30 days in advance and may be objected to under clause 4.4.3.

SUB-PROCESSOR	PROCESSING CARRIED OUT	PERSONAL DATA RECEIVED	LOCATION OF PROCESSING	TRANSFER BASIS UNDER CHAPTER V
Amazon Web Services Contracting entity [AWS EMEA SARL]	Hosting of the application, database, object storage of files and photographs, and encrypted backups	All Customer Personal Data described in Annex 1	United Kingdom, region eu-west-2 (London)	Not a Restricted Transfer for data at rest: the region is contractually controlled and AWS will not move or replicate content outside it without agreement. Support access from outside the UK runs under **Article 46**, on the AWS UK GDPR Addendum, which incorporates the ICO's International Data Transfer Addendum. AWS's contract documents make no Data Privacy Framework claim, so the Addendum, not the data bridge, is the operative route.
Twilio Twilio Verify and Programmable Messaging	Delivery of one-time codes for sign-in, and delivery of posts by SMS where the Customer enables it	Mobile telephone number; message text where SMS delivery of posts is enabled	United States	**Article 45A**, via the UK Extension to the EU–US Data Privacy Framework. Twilio Inc. is actively certified for the UK Extension, so no transfer agreement and no transfer risk assessment is required. Twilio's addendum sets a precedence order that falls back to the ICO Addendum if the certification is withdrawn.
OpenAI	Machine translation of the text of posts, video captions and comments	**Post content only.** No name, telephone number, email address or user identifier is transmitted	United States	**Article 46**, via the ICO's International Data Transfer Addendum (version B1.0) to the EU Standard Contractual Clauses, as adopted in OpenAI's own data processing addendum, supported by a documented transfer risk assessment carried out against the Article 46(6) "not materially lower" test. The ICO's transfer risk assessment tool and its published shortcut relying on the UK government's analysis of the United States may both be used.
Mux	Video ingest, encoding, storage, delivery and automatic caption generation	Video and audio content published by the Customer, which may show or identify individuals	United States	**Article 45A**, via the UK Extension to the EU–US Data Privacy Framework. Mux, Inc. is certified, but its listed status is "active, re-certification under review" and its last certification period ended 5 May 2026, so this is the one route in this annex that needs watching. Mux's addendum falls back to the ICO Addendum if the Framework ceases to be available.
Pusher optional; not used where Laravel Reverb is self-hosted	Real-time delivery of updates to the browser	Message payloads and channel identifiers	[EU cluster / UK]	Pusher holds no Data Privacy Framework certification, so the UK Extension is not available for it. [State the basis once the cluster and contracting entity are fixed.]
[Mailgun / Amazon SES]	Delivery of transactional email to the Customer's administrators	Email address, name, message content	[EU / UK]	Mailgun Technologies, Inc. is actively certified under the UK Extension to the EU–US Data Privacy Framework, so **Article 45A** applies where that entity is the contracting party. Amazon SES is covered by the AWS UK GDPR Addendum under **Article 46**.

SUB-PROCESSOR	PROCESSING CARRIED OUT	PERSONAL DATA RECEIVED	LOCATION OF PROCESSING	TRANSFER BASIS UNDER CHAPTER V
[Error and uptime monitoring provider]	Capture of application errors and availability monitoring	Potentially IP address, user identifier and request context contained in an error report	[region]	[State the basis.]

Not sub-processors. Laravel Forge is used to provision and configure servers and holds deployment credentials, but does not store or process Customer Personal Data.

SIGNED FOR THE CUSTOMER (CONTROLLER)

SIGNATURE

NAME AND TITLE

DATE

SIGNED FOR TEAMTALK (PROCESSOR)

SIGNATURE

NAME AND TITLE

DATE

Internal checklist · remove this page before issuing the agreement

THIS PAGE IS FOR TEAMTALK, NOT FOR THE CUSTOMER

The agreement above is drafted to be signed as it stands once the bracketed values are filled in. These are the points that must be confirmed against the live deployment and the live certification position **before** the agreement is sent to anyone. Delete this page from the version you issue.

1. Confirm the Customer has not configured free-text fields that invite health data, for example return-to-work notices
2. Confirm no Article 37 trigger applies as the business grows
3. RTO, RPO, backup frequency and retention
4. Date and supplier of the most recent penetration test and restore test
5. Confirm the AWS contracting entity and the current DPA version
6. Re-check the certification at each annual review
7. Confirm the executed Addendum is on file and the assessment is dated within 12 months
8. Re-check Mux's status on the Data Privacy Framework List before each renewal and before answering a questionnaire
9. Whether Pusher is in use at all, the cluster region and the contracting entity; if Reverb is self-hosted, delete this row
10. Which provider, which contracting entity and which sending region is configured; a Sinch group entity other than Mailgun Technologies, Inc. is not covered by that certification
11. If the monitoring tool captures request payloads it is a sub-processor and must be listed here; if it does not, record that finding in writing
12. Confirm this remains accurate; if Forge holds database credentials that permit access to personal data, take a view with the solicitor on whether it must be listed
13. Confirm the solicitor's review has been completed and record the date and the version reviewed.
14. Re-check the Data Privacy Framework participant list for every sub-processor relied on under Article 45A, and record the date of the check.
15. Confirm the sub-processor page at the published URL matches Annex 3 exactly, and that the two are versioned together.

Not legal advice. This is a template drafted against the statutory wording. It must be reviewed by a solicitor qualified in England and Wales before first use, and re-checked whenever the sub-processor list or the hosting arrangement changes. **Sources, all verified 28 August 2026:** UK GDPR Article 28 legislation.gov.uk/eur/2016/679/article/28; Articles 30, 32, 33, 34, 35 and 37 in the same instrument; Chapter V as substituted, Articles 44A, 45A, 45B, 46 and 49 legislation.gov.uk/eur/2016/679/chapter/V; Data (Use and Access) Act 2025 (c. 18) s.85 and Sch. 7 legislation.gov.uk/ukpga/2025/18/section/85, commenced 5 February 2026 by SI 2026/82 reg. 2(m) and (z9) legislation.gov.uk/uksi/2026/82; ICO, "Contracts and liabilities between controllers and processors" ico.org.uk and the "Contracts" checklist ico.org.uk; ICO international transfer tools, IDTA version A1.0 and Addendum version B1.0, laid before Parliament 2 February 2022 under s.119A Data Protection Act 2018, in force 21 March 2022 ico.org.uk international transfers, and the ICO transfer risk assessment tool; ICO data protection fee tiers ico.org.uk/data-protection-fee, set by SI 2018/480 as amended by SI 2025/63; Data Protection (Adequacy) (United States of America) Regulations 2023, SI 2023/1028 legislation.gov.uk/uksi/2023/1028, and the Data Privacy Framework participant list dataprivacyframework.gov/list, statuses checked 28 August 2026; Cyber Essentials requirements ncsc.gov.uk/cyberessentials.