Supplier questionnaire: answer bank

The sixty questions UK housebuilders, contract caterers and facilities management companies ask most often, with an answer written from TeamTalk's actual stack. Copy the answer, replace the [placeholders], and keep the filled-in version: the second questionnaire always takes a quarter of the time the first one did.

HOW TO USE THIS, AND THE ONE RULE

Answers marked contain a value that has never been measured or that changes over time, or an instruction to you. **They are not part of any answer. Do not send a questionnaire with one of those still in it, and send the –ISSUE build, which has them stripped out.** Confirm the number against the live deployment first. A wrong answer that a customer's IT team later discovers costs the deal and the relationship; a slow answer costs a day. Where the honest answer is "we do not do that", say so and give the date by which you will, which reads far better than a vague claim that unravels under a follow-up question.

SCALE NOTE: READ THIS BEFORE YOU COPY ANYTHING BELOW

As at [date] TeamTalk has **one director and no employees**, is **pre-revenue**, does **not yet hold Cyber Essentials** and has **not yet bought insurance**. Every answer below is written to be true of that company. Where an answer names a second role or a review cycle, it takes effect when that person is engaged. External escalation route: [accountant / solicitor]. **The build produces two files: `supplier-questionnaire-answer-bank-ISSUE.pdf` without the orange verify badges, and `-INTERNAL.pdf` with them. The badges are instructions to you, not answers: never let one reach a customer.**

A · Company and commercial (1 to 8)

	QUESTION	ANSWER
1	**Full registered name, company number and registered office**	[TeamTalk Ltd], a private company limited by shares registered in England and Wales under company number [number], registered office [address]. Records are public at find-and-update.company-information.service.gov.uk.
2	**Trading address and places of business**	[address]. TeamTalk is a software supplier with no operatives, plant or vehicles. TeamTalk staff visit customer premises for onboarding and training only, under the customer's site rules and induction; no construction or operational work is carried out.
3	**VAT registration number**	[GB number].
4	**Date of incorporation and years trading**	Incorporated [date]. **TeamTalk is pre-revenue and says so. There are no customer references yet; the refundable 60-day pilot is offered instead.** The pilot is £2,500 plus VAT for 60 days on up to three sites and 250 workers, with written success criteria measured from the product's own reporting, and **the pilot fee is refunded only if both criterion 1 and criterion 2 are missed**. That is a stronger assurance than a reference from a customer you cannot telephone.
5	**Number of employees**	**One director and no employees** as at [date], plus [N] contractors. Stated plainly because a supplier form that says "5 to 10" and a Companies House record that says one director is the fastest way to lose a procurement team.
6	**Annual turnover and financial standing**	**No filed accounts yet (incorporated [date]); we offer [prepayment / a director's guarantee / a short-form financial statement] in place of a credit history.** TeamTalk is pre-revenue, has no county court judgments, is not in any insolvency procedure and has no overdue statutory filings. A credit check will return a thin file rather than a bad one, and the three substitutes above are what a procurement team can actually act on: say which you are offering rather than leaving the buyer to ask. The pilot fee is payable in advance in any event, so the customer's financial exposure to TeamTalk during the pilot is the fee itself, which is refundable on the criteria in the pilot agreement.
7	**Bank details and payment terms**	Bank details are supplied only through a verified channel, on request, and never by email alone. Standard terms are 30 days from invoice, by Bacs. TeamTalk does not accept payment by card as standard.
8	**Named contacts**	Commercial and contract: [name, email, mobile]. Technical and security: [name, email, mobile]. Data protection: [name, email]. Escalation and incidents: [name, mobile], monitored [08:00 to 18:00 UK, Monday to Friday].

B · Data protection and UK GDPR (9 to 22)

	QUESTION	ANSWER
9	**Are you registered with the Information Commissioner?**	Yes. Registration number [number], tier 1 (micro organisations), fee £52 a year, or £47 by direct debit. The entry is public on the ICO register.
10	**Are you a controller or a processor?**	For the worker personal data in your tenant, **you are the controller and TeamTalk is the processor**. TeamTalk is a controller only for its own business contact data, billing records and service telemetry that does not identify your workers.
11	**What personal data will you process?**	Name; mobile telephone number; optional email address; preferred language; employer or subcontractor; site, depot or team; group membership; role; start and leaving dates; the content of posts, comments and messages and their machine translations; video and captions; hazard reports including free text, location and photographs, which may show identifiable people; sign-in events; confirmations of receipt with timestamps; device and browser type; IP address; push notification tokens.
12	**Whose personal data?**	Your employees; your workers and agency staff; employees and operatives of your subcontractors working on your sites or contracts; your managers and administrators; and, incidentally, anyone appearing in a photograph or video published on the tenant.
13	**Do you process special category or criminal offence data?**	**The Service is not designed for special category data. It may arise incidentally in free text (for example accident notices or dietary/religious information in a canteen notice). The Controller is responsible for the lawful basis for any such data; the Annex 2 measures apply to all Customer Data without distinction.** That is the honest answer: a contractual prohibition would not stop it arriving. Nothing in the Service requires or requests Article 9 data, and preferred language is collected to deliver translation and is not used or inferred as a proxy for nationality or ethnicity. **Criminal offence data under Article 10 is a separate regime**, permitted only under the control of official authority or where domestic law authorises it with appropriate safeguards, which in the UK means a condition in Schedule 1 to the Data Protection Act 2018: **the Service must not be used for it and offers no field for it.**
14	**What is the lawful basis?**	You determine it as controller. In practice it is normally legitimate interests, or compliance with a legal obligation where the communication discharges a statutory duty to inform or instruct. TeamTalk does not rely on consent for the operation of the service and does not use worker data for marketing.
15	**Will you sign a data processing agreement?**	Yes. TeamTalk offers its own Article 28 compliant agreement, which can be signed the same day, and will review yours instead if you prefer. TeamTalk's version is available before contract so your data protection officer can read it during evaluation rather than at signature.
16	**Where is personal data stored and processed?**	**United Kingdom (AWS London, eu-west-2).** This is a commitment in clause 7.1 of the data processing agreement, not a configuration preference: TeamTalk will not move the hosting region without the customer's prior written agreement. AWS will not move or replicate content outside the chosen region without agreement.
17	**Is any personal data transferred outside the UK, and on what basis?**	All data at rest stays in the UK. Three sub-processors are in the United States. **Twilio Inc.** (SMS sign-in codes) is listed **Active** and **Mux** (video) **Active, re-certification under review** under the **UK Extension to the EU–US Data Privacy Framework**, given effect by SI 2023/1028, so those transfers run on the Article 45A adequacy route and need no transfer agreement or risk assessment while the certifications stand. **OpenAI** (translation) is not certified, at 0 of 7,567 records on the list, so that transfer runs on the ICO's **International Data Transfer Addendum, version B1.0**, supported by a documented transfer risk assessment carried out against the Article 46(6) test as amended by the Data (Use and Access) Act 2025. Post text, comment text, direct message text and hazard report text are sent for translation. No names, phone numbers or identifiers accompany the text. **All three statuses were checked against dataprivacyframework.gov/list on 28 August 2026, and one caveat is volunteered rather than hidden: Mux is listed "Active, re-certification under review".** Certifications lapse, so TeamTalk re-checks every status every six months and before answering any questionnaire.
18	**Do you have a data protection officer?**	TeamTalk is not required to appoint one under Article 37 of the UK GDPR: it is not a public authority, its core activities do not consist of large-scale regular and systematic monitoring, and it does not process special category data at scale. A named individual is accountable for data protection: [name, email]. This position is reviewed as the business grows.
19	**How long is data retained, and how is it deleted?**	These are contractual, not descriptive: clause 4.7.5 of the data processing agreement sets them as defaults and you may instruct otherwise. Posts, comments, translations and confirmation records including briefing record exports: **24 months** after the end of the relationship. Worker accounts: **deactivated on the recorded leaving date**, identifiers **minimised 12 months** after. Hazard reports and photographs: **24 months**. Logs including the impersonation log: **90 days**. Backups [30] days. On termination, 30 days to export, then deletion within a further 30 days with written confirmation.

	QUESTION	ANSWER
20	**How do you support data subject rights requests?**	Your administrators can locate, view, correct, export and delete an individual worker's record without contacting TeamTalk. Where more is needed, TeamTalk assists within [5] working days of a written request, at no charge for ordinary volumes. If a data subject approaches TeamTalk directly it will not respond substantively but will forward the request to you without undue delay.
21	**What are your personal data breach notification timescales?**	TeamTalk notifies the affected customer **without undue delay and in any event within 24 hours** of becoming aware of a breach involving personal data, which is tighter than the Article 33(2) standard, so that you as controller have time to meet your own duty under Article 33(1) to notify the Commissioner without undue delay and where feasible within 72 hours. The notification carries the information Article 33(3) requires. A written post-incident report follows within [10] working days. TeamTalk does not notify the Commissioner on your behalf unless instructed in writing.
22	**Will you assist with a data protection impact assessment?**	Yes, and TeamTalk names the reason for it rather than waiting to be asked. **Per-worker sign-in timestamps, confirmation records and chase lists are monitoring of workers** within the meaning of the ICO's employment practices guidance, which expects a DPIA, worker transparency and a proportionality assessment. TeamTalk supplies a **pre-completed DPIA and monitoring pack** covering purpose, necessity, proportionality, the less intrusive alternatives considered, worker consultation and the residual risks, together with a **worker privacy notice template** you can adapt. **What the Service does not do, and has no feature for: no location tracking, no message-content analysis, no productivity scoring.** You remain the controller and carry out your own assessment; supplying ours up front routinely removes two to four weeks from procurement.

C · Information security (23 to 38)

	QUESTION	ANSWER
23	**What security certifications do you hold?**	**Cyber Essentials: not currently held. Assessment booked with [body], target [date].** The gap analysis against the current IASME question set is complete and is available on request, as is the remediation list and its dates. Cyber Essentials Plus: not held. TeamTalk is **not** certified to ISO/IEC 27001 and does not claim to be; a written information security management roadmap is available. Say this plainly with a date rather than leaving the field blank: a booked assessment is a credible answer and a blank is not.
24	**Do you have an information security policy?**	Yes, a written policy owned by [name, Director], reviewed annually and on material change, aligned to the five Cyber Essentials technical control areas. A copy is supplied on request. Every person with access to customer data is briefed on it on joining and at least annually; with one director and no employees that is one person today, and it applies to each further person from the day they are engaged.
25	**Is data encrypted in transit and at rest?**	In transit: TLS 1.2 or above on all connections, certificates issued and renewed automatically, HTTP redirected to HTTPS, HTTP Strict Transport Security enabled. At rest: AES-256 on Amazon EBS volumes and S3 objects, including backups.
26	**How are encryption keys and secrets managed?**	Volume and object encryption uses AWS-managed keys. Application secrets and third-party API keys are held in server environment configuration, never in source control, and are rotated on personnel change and on suspicion of compromise. Administrator passwords are stored only as bcrypt hashes and are not recoverable.
27	**How is access to customer data controlled?**	Least privilege, individual named accounts rather than shared ones, and separate administrative accounts kept apart from day-to-day accounts. Production access is limited to [N, currently one] named people, protected by multi-factor authentication and SSH keys, reviewed [quarterly] and removed on a person's last working day.
28	**Is multi-factor authentication enforced?**	**For administrators and staff, yes.** Multi-factor authentication is enforced on every cloud service account TeamTalk holds, including AWS, the deployment platform, the source code repository and every third-party service, and on staff access to production. This is a mandatory Cyber Essentials requirement and an automatic fail if it is not in place. **For workers, no, and TeamTalk does not claim otherwise:** worker sign-in is a single-use SMS code to a verified mobile number with no password, which is **single-factor possession**. See question 30 for why that is the right control for a frontline workforce. The two are answered separately here on purpose, because a reviewer who finds them conflated will discount the whole document.
29	**What is your password policy?**	Multi-factor authentication with a password of at least 8 characters and no maximum length, which is one of the three permitted Cyber Essentials options. Brute-force protection is in place. Password expiry is **not** enforced and complexity rules are **not** enforced, in line with NCSC guidance and the current scheme requirements.

	QUESTION	ANSWER
30	**How do end users authenticate to the service?**	Workers sign in with a mobile telephone number and a single-use, time-limited code delivered by SMS. There is no worker password and no email address is required. **This is single-factor possession, not multi-factor authentication.** It is the right control here and the reasoning is offered rather than hidden: **there is no password to phish, share or reuse**, which removes the two commonest frontline credential risks; the factor is **per-device and per-number**, so it cannot be passed round a site the way a shared password is; and the code is **short-lived and single-use**. The residual risk is loss of the handset, mitigated by revoking access automatically on a worker's recorded leaving date, including mid-session. Session lifetime, device binding and invalidation on a change of mobile number are [planned before first customer]. Single sign-on and SCIM are **not** currently supported.
31	**What audit logging is in place?**	Administrator actions, support impersonation, account creation and deletion, leaving-date changes, and publication and deletion of posts are all logged. Every support impersonation records the operator, the impersonated user, the tenant and the timestamp, and the log is available to you on request. Application and access logs are retained [90] days.
32	**How is the service monitored?**	External uptime monitoring at [1 minute] intervals and in-application error monitoring, both alerting **the named director** by [email and SMS]. **There is no on-call engineer and no 24/7 rota, and neither is claimed**; the security contact is monitored [08:00 to 18:00 UK, Monday to Friday].
33	**How do you manage patching and vulnerabilities?**	Unattended security updates are enabled on all servers. Updates for vulnerabilities the vendor rates critical or high, or carrying a CVSS v3 base score of 7 or above, are applied **within 14 days of release**, which is the Cyber Essentials requirement, and within [72 hours] where a vulnerability is being actively exploited. Dependencies are reviewed [monthly] with automated vulnerability alerting. Software is removed or upgraded before it reaches end of support.
34	**When was your last penetration test?**	[An independent external test was carried out by [supplier] on [date]. A summary report and the remediation status are available under a mutual non-disclosure agreement.] If no test has been carried out, say so and give the planned date rather than leaving this blank; a scheduled date is a credible answer and an evasion is not.
35	**Do you follow a secure development process?**	All changes go through source control and deploy from a protected branch. The framework provides protection against SQL injection, cross-site scripting and cross-site request forgery by default and those protections are not disabled. Dependencies are pinned and monitored for known vulnerabilities. Production personal data is not copied into development or staging environments.
36	**How is our data segregated from other customers'?**	**Logical tenant isolation enforced at the data layer, with automated cross-tenant tests [not yet; target date].** TeamTalk is multi-tenant and does not describe itself as single-tenant. Each customer has its own subdomain or custom domain, branding and users. Every record carries a tenant identifier and every query is scoped to the tenant resolved from the request domain, enforced globally in the application layer rather than left to individual queries. File storage is partitioned by tenant. A user in one tenant cannot enumerate, read or address users, posts or files in another. Dedicated-database deployment is available for enterprise customers.
37	**How are personnel vetted and trained?**	TeamTalk has **one director and no employees**, so today this describes one person. The measures apply to the director now and to each person engaged from the day they are engaged: **right to work check before starting**, written confidentiality obligations surviving the end of engagement, security and data protection briefing on joining and at least annually, and access removal on the last working day. [Basic DBS checks are obtained where a customer requires them.] BS 7858 screening is **not** carried out and is not claimed.
38	**How are end-user devices and remote working secured?**	All laptops, being [N, currently the director's], have full-disk encryption, an enabled software firewall, automatic operating system updates, malware protection and automatic screen lock. Company data is accessed only through the browser and the hosted tooling, not stored on the device where avoidable. Removable media is not used for customer data. Devices will be in scope of the Cyber Essentials assessment booked under question 23.

D · Business continuity, backup and incident response (39 to 45)

	QUESTION	ANSWER
39	**Do you have a business continuity and disaster recovery plan?**	Yes, a written one-page plan covering loss of the production environment, loss of a critical third-party service, loss of key personnel and loss of premises, reviewed [annually] and after any incident. With one director, **loss of key personnel is the material scenario** and the plan says so; see question 45. A summary is supplied as a separate document.
40	**What are your RTO and RPO?**	Recovery time objective [4] hours for the application from a confirmed loss of the production server. Recovery point objective [24] hours, or [5 minutes] where point-in-time recovery is enabled on the managed database.

	QUESTION	ANSWER
41	**How often is data backed up, and where is it held?**	The database is backed up [daily], encrypted, and stored in Amazon S3 in the same UK region with versioning enabled. Uploaded files are held in S3, which is designed for high durability. Backups never leave the UK.
42	**How long are backups kept, and are restores tested?**	Backups are retained [30] days and then deleted automatically. A full restore to a scratch environment is performed [quarterly], with the date, duration and outcome recorded. The most recent successful restore test was on [date].
43	**Do you have a documented incident response process?**	Yes, with a single named owner. It covers detection, containment, assessment, customer notification, remediation, and a written post-incident review. It is exercised [annually] as a tabletop walkthrough.
44	**How and when would you tell us about an incident?**	By telephone and email to your named contact, without undue delay and in any event within 24 hours of becoming aware where personal data is involved, and within [24 hours] for a security incident that does not involve personal data. You receive facts as they are confirmed, in phases if necessary, rather than a single late report.
45	**What happens if you cease trading, or a key person is unavailable?**	TeamTalk has **one director and no employees**, and says so rather than letting a buyer discover it at Companies House. Credentials for all critical systems are held in [a password manager] with a documented emergency access arrangement held by [named person or the company's solicitor], who is also the external escalation route named in every policy. On termination for any reason, including insolvency, your data is available for export in a machine-readable format for 30 days. Source code escrow is not offered as standard and would be considered for an enterprise agreement.

E · Sub-processors and supply chain (46 to 49)

	QUESTION	ANSWER
46	**Who are your sub-processors?**	Amazon Web Services (hosting, storage, backups; **United Kingdom (AWS London, eu-west-2)**; no transfer for hosting, AWS UK GDPR addendum for support access); **Twilio Inc.** (SMS sign-in codes; United States; UK Extension to the DPF, *Active*); **Mux, Inc.** (video and captions; United States; UK Extension, *Active, re-certification under review*); **OpenAI OpCo, LLC** (translation, text only, no identifiers; United States; no DPF certification, so IDTA or Addendum plus a transfer risk assessment); transactional email [Amazon SES / Mailgun, confirm which]; real-time delivery [self-hosted Reverb; Pusher only if enabled]; [error and uptime monitoring provider]. **All statuses checked 28 August 2026 and re-checked every six months.** The current list is published at [https://team-comms.com/sub-processors] and is versioned with Annex 3 of the DPA. The list is deliberately short.
47	**How are we told about changes, and can we object?**	At least **30 days' written notice** before a new or replacement sub-processor begins processing, by email and by updating the published list. You may object on reasonable data protection grounds within 30 days. If TeamTalk cannot offer a reasonable alternative, you may terminate without penalty and receive a pro rata refund for the unexpired term.
48	**What due diligence do you carry out on sub-processors?**	Before engagement and **at least every six months**: the provider's data processing terms and security documentation, its certifications, its data location, and its transfer mechanism, including verifying an active UK Extension certification on the Data Privacy Framework List where that route is relied on. Findings are recorded with the date of the check. Last checked **28 August 2026**.
49	**Do your contracts with sub-processors flow down the same obligations?**	Yes. Each is engaged under a written contract imposing the same data protection obligations as the customer agreement, as Article 28(4) of the UK GDPR requires. **Where a sub-processor fails to meet its obligations, TeamTalk remains fully liable to you for its performance.** Redacted terms are available on request.

F · Insurance (50 to 53)

	QUESTION	ANSWER
50	**Professional indemnity insurance**	**Not yet in place. Cover of £[1m] in the aggregate will be bound before launch day with [insurer], and the certificate provided on request.** The pilot agreement states this as a commitment to hold cover before launch day, not as a present-tense warranty, because warranting cover you do not hold is a misrepresentation and would void the cover it describes. Note that many construction and facilities framework schedules require £5m maintained for six years after the end date, so check the limit your target buyers require before you bind.
51	**Public liability insurance**	**Not yet in place. Cover of £[1m] per occurrence will be bound before launch day with [insurer].** TeamTalk staff visit customer premises for onboarding and training only, under the customer's site rules and induction; no construction or operational work is carried out. A lower public liability limit is frequently agreed for a pure software supplier on that basis. Ask.

	QUESTION	ANSWER
52	**Employers' liability insurance**	[£10m with [insurer], policy [number]]. The statutory minimum under the Employers' Liability (Compulsory Insurance) Regulations 1998 is £5m; most insurers write £10m. If TeamTalk currently employs only its owner, who holds 50% or more of the issued share capital, the HSE treats it as exempt: say that plainly rather than leaving the field blank.
53	**Cyber liability insurance**	**Not yet in place. Cover of £ [amount] including data breach response costs will be bound before launch day with [insurer]. Buy this one first.** Clause 14.3 of the pilot agreement sets a data-protection super-cap at the cyber policy limit, which is what lifts liability for a personal data breach above the £2,500 fee cap and is the clause a plc legal team looks for. The super-cap cannot be written until the policy limit exists.

G · Modern slavery, ethics and equality (54 to 56)

	QUESTION	ANSWER
54	**Do you have a modern slavery statement?**	Yes, published voluntarily. TeamTalk's turnover is below the £36 million threshold at which section 54 of the Modern Slavery Act 2015 requires a statement, so it is not legally obliged to publish one, and the statement says so. A one-page statement is attached and is published at [URL].
55	**Do you have an anti-bribery policy?**	Yes. TeamTalk is a relevant commercial organisation for the purposes of section 7 of the Bribery Act 2010, which has no size threshold, and maintains procedures proportionate to its risk in line with the Ministry of Justice statutory guidance. A one-page policy is attached. No director or employee has been convicted of a bribery or corruption offence.
56	**Do you have an equal opportunities or diversity policy?**	Yes, a one-page policy covering the nine protected characteristics in section 4 of the Equality Act 2010. TeamTalk has not been the subject of any Equality and Human Rights Commission investigation or any finding of unlawful discrimination. The public sector equality duty does not apply to TeamTalk, which does not exercise public functions.

H · Health and safety (57 to 58)

	QUESTION	ANSWER
57	**Do you have a health and safety policy?**	Yes. TeamTalk employs fewer than five people, so it is excepted from the duty in section 2(3) of the Health and Safety at Work etc. Act 1974 to prepare a written policy, by the Employers' Health and Safety Policy Statements (Exception) Regulations 1975. A written policy is maintained anyway and is attached. TeamTalk is a desk-based business: the material risks are display screen equipment, electrical safety and lone or home working, all assessed and recorded. TeamTalk staff visit customer premises for onboarding and training only, under the customer's site rules and induction; no construction or operational work is carried out.
58	**Accident record, RIDDOR reports and enforcement history**	No reportable incidents under RIDDOR 2013 in the last [three] years, no enforcement notices, and no prosecutions. TeamTalk staff visit customer premises for onboarding and training only, under the customer's site rules and induction; no construction or operational work is carried out. Personnel are escorted where the occupier requires it.

I · Environment (59 to 60)

	QUESTION	ANSWER
59	**Do you have an environmental policy or ISO 14001?**	A one-page environmental policy is maintained and attached. TeamTalk is not certified to ISO 14001 and does not claim to be. It is below the thresholds for Streamlined Energy and Carbon Reporting and for the Energy Savings Opportunity Scheme, and, as a micro business, the workplace recycling separation duty applies to it from 31 March 2027.
60	**What is your carbon reduction or net zero commitment?**	TeamTalk is a remote-first software business with no premises-based operations, no fleet and no manufacturing, so its direct emissions are minimal and its principal impact is the energy used by its cloud hosting. It hosts in the United Kingdom (AWS London, eu-west-2), and AWS publishes its own renewable energy commitments. [A carbon reduction plan to PPN 006 format is available where a customer requires one.]

Not legal advice. These are drafting aids, not warranties. Every answer becomes a contractual representation once it is in a completed questionnaire, so confirm each one before sending. **Sources, verified 28 August 2026:** UK GDPR Articles 28, 30, 32, 33 and 37, and Chapter V as substituted with effect from 5 February 2026 legislation.gov.uk/eur/2016/679; Data (Use and Access) Act 2025 s.85 and Sch. 7, commenced by SI 2026/82 legislation.gov.uk/ukpga/2025/18; ICO data protection fee, tier 1 £52, or £47 by direct debit, under SI 2018/480 as amended by SI 2025/63 ico.org.uk/data-protection-fee; ICO transfer tools, IDTA version A1.0 and Addendum version B1.0, in force 21 March 2022 ico.org.uk international transfers; Data Protection (Adequacy) (United States of America) Regulations 2023, SI 2023/1028 legislation.gov.uk/uksi/2023/1028; NCSC *Cyber Essentials: Requirements for IT Infrastructure v3.3* ncsc.gov.uk/cyberessentials; Modern Slavery Act 2015 s.54 and SI 2015/1833 reg. 2 (£36m threshold) legislation.gov.uk/ukpga/2015/30/section/54; Bribery Act 2010 s.7 legislation.gov.uk/ukpga/2010/23/section/7; Equality Act 2010 s.4 legislation.gov.uk/ukpga/2010/15/section/4; Health and Safety at Work etc. Act 1974 s.2(3) and SI 1975/1584 reg. 2 legislation.gov.uk/uksi/1975/1584; Employers' Liability (Compulsory Insurance) Regulations 1998, SI 1998/2573 reg. 3(1), and HSE leaflet HSE40 hse.gov.uk/pubns/hse40.pdf; RIDDOR 2013, SI 2013/1471 legislation.gov.uk/uksi/2013/1471; Simpler Recycling micro-firm date, SI 2025/140 reg. 4 legislation.gov.uk/uksi/2025/140; ICO, *Employment practices and data protection: monitoring workers* ico.org.uk monitoring workers; Data Privacy Framework participant list, statuses for Twilio Inc. (Active), Mux (Active, re-certification under review), Mailgun Technologies, Inc. (Active), Amazon.com, Inc. (Active) and OpenAI and Pusher (not listed) read from dataprivacyframework.gov/list on 28 August 2026.