

Cover note: what is in this pack and what to do with it

Seventeen documents, plus this note, that answer before it is asked almost everything a UK housebuilder, contract caterer or facilities management company puts to a supplier during onboarding. **None of it is legal advice**, and three documents must go to a solicitor before you use them once. Page 2 records what was verified and what was not.

What is in the pack

FOUR FACTS EVERY DOCUMENT IN THIS PACK IS NOW WRITTEN TO BE TRUE OF

One director, no employees. Pre-revenue. Cyber Essentials not currently held. Insurance not yet bought. Nothing in the pack asserts otherwise, and where a document names a role, a review cycle or a certificate that does not exist yet, it says so and gives a date. That is deliberate: a young supplier who names its gaps is easy to buy from, and one who is caught overstating them is not. **Two documents are built twice**, because each contains material that must never reach a customer: send the –ISSUE file and keep the –INTERNAL one.

DOCUMENT	PAGES	BEFORE USE	WHAT IT IS FOR
data-processing-agreement-ISSUE also built as -INTERNAL, 12 pages, with the checklist page	11	SOLICITOR	UK GDPR Article 28 terms, you as processor, with annexes for the processing detail, the controller's own obligations and rights, the security measures and the sub-processors. Carries the retention clause and the hosting commitment. Send the ISSUE file: the INTERNAL one ends with a page telling the customer what is not confirmed.
terms-of-service-outline	8	SOLICITOR	Instructions to counsel: every clause your subscription terms need, and suggested wording. Never send this to a customer.
pilot-agreement	4	SOLICITOR	The £2,500 60-day proof of reach, and the only contract : the sales proposal is now accepted subject to it, and the signature lives here. Four success criteria, the refund with its exclusions, the data-protection super-cap, and the year-one price on the paper.
security-summary	4	TICK, THEN ISSUE	A checklist, not an assertion: tick only what is true today and write "not yet" for the rest. Sent unprompted after the demo, this turns a six-week IT queue into a two-week one.
supplier-questionnaire-answer-bank-ISSUE also built as -INTERNAL, 8 pages, with the verify badges	6	INTERNAL	The 60 questions UK buyers ask most, answered from your actual stack and your actual company. The orange verify badges are instructions to you, not answers. The ISSUE build strips them out.
dpia-and-monitoring-pack	4	ISSUE AS IS	New. A pre-completed DPIA naming per-worker read receipts and chase lists as monitoring under the ICO's employment practices guidance, with the proportionality argument, the alternatives considered, ten risks and their measures, and what the product deliberately does not do. Volunteer it. On a unionised site it is the first question and this is the answer.
worker-privacy-notice-template	3	ISSUE AS IS	New. For the customer to adapt and publish in its own name, because it is the customer's controller duty. Ends with a short form under 250 words written for translation into the languages on site. This removes the customer's biggest deployment objection.
privacy-notice-prospects	3	PUBLISH FIRST	New. Your own Article 13 and 14 notice for business development contacts. This must be live at team-comms.com/privacy before the first cold email , and linked from the footer of every one.
cyber-essentials-checklist	4	INTERNAL	The five controls mapped to Laravel on AWS via Forge plus laptops, and where the automatic fails are. Work through it, then book the assessment.
policies/ health and safety, modern slavery, anti-bribery, equal opportunities, quality, environmental, information security, business continuity	1 each	SIGN AND DATE	The eight one-pagers a supplier form asks for. Each now carries a scale note saying what the company actually is, so no one has to pretend there is a board, a second approver or a monthly team meeting. Fill the brackets, sign, keep them in one folder: every item you cannot produce on the day adds one to three weeks to a deal.

The three that must go to a solicitor, and why

Send all three in one instruction: they share definitions and cross-refer, and one instruction is materially cheaper than three. Budget **[£1,500 to £3,000]** for a solicitor qualified in England and Wales. **The DPA**, because it creates statutory obligations you cannot vary, because its liability, audit and sub-processor clauses are what a customer's counsel redlines, and because Chapter V of the UK GDPR was rewritten on 5 February 2026 so older templates cite repealed provisions. **The terms of service**, because your liability cap sits on your own written standard terms and is subject to the reasonableness test in s.3 of the Unfair Contract Terms Act 1977: a cap set badly can be struck out entirely, leaving you uncapped. Start from Bonterms or Common Paper, never a US template. **The pilot agreement**, because it is now the **only** paper a plc division signs, and it carries a refund promise with exclusions, an incorporated DPA, a general liability cap and a data-protection super-cap set at your cyber policy limit.

The other fifteen documents do not need a solicitor. They need **accurate numbers and two purchases**, which is a different and more urgent problem. The two purchases are the cyber policy and the Cyber Essentials assessment, and everything else in the pack is drafted so that it stays true until they are made.

The order to do this in

#	DO THIS	ELAPSED	WHY IN THIS POSITION
1	Buy the insurance, cyber first. Then fill in the company basics: company number, VAT position, registered office, ICO registration, bank details, named contacts. Cyber before professional indemnity and public liability , because pilot agreement clause 14.3 sets the data-protection super-cap at the cyber policy limit and the clause cannot be written until the limit exists.	1 to 3 days	Every other document has these in square brackets, so doing it once completes them all. Raising an insurance limit mid-procurement costs about three weeks: buy it before you are asked. Until it is bought, the pilot agreement says "will hold, before launch day", which is true; it must never say "holds", which would not be.
2	Book Cyber Essentials. Read the Danzell question set free first, fix the gaps, then pay the £320 plus VAT. Until the certificate is in hand, every document in this pack says " Cyber Essentials: not currently held. Assessment booked with [body], target [date]. " Fill in the body and the date; do not delete the sentence.	1 to 3 weeks	Longest lead time here and the item most frequently demanded. It is on the critical path of your first housebuilder deal. Start it today.
3	Measure the numbers marked [verify]. Run a timed restore drill; confirm backup frequency and retention; record the restore test date; decide the penetration testing position.	2 to 3 days	These block the security summary and the answer bank, the two documents that actually shorten deals. A wrong answer here is worse than a slow one.
4	Sign and date the eight policies , publish the modern slavery statement, and instruct the solicitor on the DPA, the terms and the pilot agreement together.	1 day, then 1 to 2 weeks	The policies depend on nothing else and a supplier portal will refuse to progress without them. The solicitor's work runs in parallel with Cyber Essentials, so start it the same week.
5	Publish the prospect privacy notice, the sub-processor list, the terms and the DPA at stable, versioned URLs, then send the security summary and the DPIA pack unprompted after every demo.	1 day, then ongoing	The DPA and the order form incorporate documents by URL, so those URLs must exist, and the privacy notice must be live before the first cold email rather than after it. Sending the summary and the DPIA pack unprompted is the habit that compounds.

What was verified, and against what

Every regulatory reference was checked against the primary source on 28 August 2026, not against secondary commentary. The material findings, several of which correct what is in general circulation:

- **UK GDPR Chapter V was rewritten with effect from 5 February 2026** by s.85 of and Sch. 7 to the Data (Use and Access) Act 2025, commenced by SI 2026/82. **Articles 44 and 45 are omitted**, replaced by new Articles 44A, 45A, 45B and 45C; Article 46 is amended; DPA 2018 ss.17A to 18 are repealed. The transfer test is now whether protection is "**not materially lower**" than under UK law. Anything citing Article 45 or s.17A is citing repealed law.
- **Article 28(3)(a) to (h) is unchanged** and is reproduced faithfully in the DPA, each subparagraph marked in the margin. **The ICO publishes no Article 28 standard clauses of its own**, though Article 28(8) gives it the power; it points to the Danish authority's clauses instead.
- **The IDTA is version A1.0; the Addendum is version B1.0.** Both laid before Parliament on 2 February 2022 under s.119A DPA 2018, in force 21 March 2022. "IDTA B1.0" is a common and wrong citation.
- **Data Privacy Framework statuses, read from the official participant list on 28 August 2026, not from vendor marketing.** Twilio Inc.: **Active** for the EU-US, Swiss-US and UK Extension. **Mux: Active, re-certification under review** on all three, which is the one status here that can lapse and which every document in the pack now states openly. **Mailgun Technologies, Inc.: Active.** **Amazon.com, Inc.: Active.** **OpenAI: not on the list at all**, 0 of 7,567 records, so its transfer runs on the ICO Addendum with a transfer risk assessment. **Pusher: not on the list.** The UK adequacy regulations are SI 2023/1028, in force 12 October 2023. **AWS makes no DPF claim in its own contract documents**, so its route is the AWS UK GDPR addendum. **Diarise a re-check every six months**; this is a claim that decays.
- **The current Cyber Essentials question set is Danzell**, v16.3, in effect from 27 April 2026, with *Requirements for IT Infrastructure v3.3*. It is not Willow, which it superseded. IASME fees are £320 micro, £440 small, £500 medium, £600 large, plus VAT. **MFA on all cloud services, and 14-day patching, are now automatic-fail questions.**
- **Per-worker read receipts are worker monitoring** under the ICO's *Employment practices and data protection: monitoring workers* guidance, which says an employer **must** carry out a DPIA before processing likely to be high risk and **should** carry one out anyway; must select the **least intrusive means**; must **tell workers**, because monitoring without transparency is unfair; **should** seek and record workers' or representatives' views before introducing it; and **must** identify an Article 9 condition where special category data is likely to be captured even unintentionally. That guidance is marked under review following the Data (Use and Access) Act 2025, so re-check it at each annual review. **Article 9 and Article 10 are different regimes**: Article 9 is special categories, Article 10 is criminal convictions and offences, permitted only under official authority or where domestic law authorises it with safeguards. The pack no longer conflates them.
- **Modern slavery**: the £36m threshold is reg. 2 of SI 2015/1833, unamended, so your statement is voluntary and says so. **Health and safety**: the written-policy exemption below five employees is reg. 2 of SI 1975/1584, and it ends the day your fifth employee starts. **The ICO fee** is £52 for tier 1, or £47 by direct debit, under SI 2018/480 as amended by SI 2025/63; **employers' liability** minimum cover is £5m under reg. 3(1) of SI 1998/2573, though most insurers write £10m. **ISO 14001:2015 is withdrawn**, superseded by ISO 14001:2026, so do not cite the 2015 edition in a 2026 supplier pack; ISO 9001:2015 stands with Amendment 1:2024.

What could not be verified, and what you must confirm yourself

- **Every value in square brackets.** Nothing about your live deployment was measured. Buyers follow up hardest on the recovery time and recovery point objectives, backup retention, the date of the last successful restore test, and whether a penetration test has ever been carried out. The answer bank lists all sixteen in one table.
- **Nothing about the company's own commercial position was verified, because it does not exist yet.** Cyber Essentials is not held and no assessment has been booked; no insurance has been bound; there are no filed accounts and no customers. Every document is drafted to be true of that, and each carries the wording that becomes false the moment it stops being true. **Update them on the day, not before it.**
- **Mux's DPF status needs watching.** It read "Active, re-certification under review" on 28 August 2026. It is the weakest link in the sub-processor list; re-check it before answering any questionnaire, and at least every six months.
- **Three details of your own sub-processor list.** Whether Pusher is in use at all and, if so, its cluster region and contracting entity: the pack now says "**self-hosted Reverb; Pusher only if enabled**", and if Reverb is self-hosted you should delete that row, because a shorter list is a sales asset. Which email provider is configured, "**Amazon SES / Mailgun, confirm which**", and in which region: a Sinch group entity other than Mailgun Technologies, Inc. is not covered by that certification. And whether your error monitoring tool stores request payloads: if it does, it is a sub-processor and must be listed, and if it does not, record that finding in writing.
- **The automated cross-tenant isolation tests do not exist yet**, and the security summary and the DPA both say "not yet" in the same sentence as the isolation claim. That is the right answer today. Write the tests, then delete the marker: it is the question a security reviewer asks twice.

- **The Cyber Essentials Plus test specification version** for Danzell: NCSC still lists v3.2 and IASME publishes none under the Danzell heading. Ask a certification body if Plus is on your roadmap. Danzell's go-live is 27 April 2026 on IASME's and NCSC's pages; some consultancies say 28 April, and the primary sources are used here.
- **The 50% shareholder exemption from employers' liability insurance** appears in HSE leaflet HSE40, not as a provision that could be displayed on legislation.gov.uk. Cite it as HSE guidance, not as statute.
- **ISO 9001's sixth edition** was scheduled for 16 September 2026 and was unpublished when this pack was written, so check before citing an edition year. Separately, **the ICO has said it plans to update the IDTA and Addendum during 2026**: A1.0 and B1.0 are current, so diarise a check.
- **The EU–US adequacy decision is in force** but under appeal in Case C-703/25 P, whose pending status is inferred from the absence of a published judgment. The ICO confirmed on 30 July 2026 that **the UK Extension is independent of the EU decision and would not automatically fall with it**, so this is a watch item rather than a problem.
- **Two figures quoted from your commercial research rather than re-fetched**: the insurance benchmark of £5m professional indemnity, public and employers' liability with six-year run-off, taken from Crown Commercial framework RM6263 Joint Schedule 3; and the competitor availability figures in the terms outline, Microsoft at 99.9% monthly and Salesforce publishing none. Check your targets' own insurance thresholds, and verify a vendor's uptime commitment on its legal page before quoting it to a buyer.

This pack is not legal advice, and nothing in it creates a solicitor and client relationship. It is a set of well-researched drafting aids and internal checklists. The data processing agreement, the terms of service built from the outline, and the pilot agreement must each be reviewed by a solicitor qualified in England and Wales before first use, and re-checked whenever the sub-processor list, the hosting arrangement or the law changes. **Primary sources throughout, all checked 28 August 2026:** legislation.gov.uk; ico.org.uk; ncsc.gov.uk and iasme.co.uk; dataprivacyframework.gov; hse.gov.uk; gov.uk. Each document carries its own source line in its footer.