

DPIA and monitoring pack

A pre-completed data protection impact assessment for the one thing about TeamTalk that a data protection officer, a works council or a recognised union will ask about first: **per-worker read receipts and chase lists are monitoring of workers**. This pack names that, assesses it, and says what the product deliberately does not do.

WHO THIS IS FOR, AND WHAT IT IS NOT

The customer is the **controller** and the DPIA is the controller's to carry out, sign and keep. TeamTalk is the **processor** and cannot do it for you, but it can do most of the typing. Everything below is written from TeamTalk's actual product behaviour; the [\[brackets\]](#) are the parts only you can answer, chiefly your purpose, your consultation and your risk appetite. **Adopt it, edit it, disagree with it in writing where you see it differently, and sign it.** A DPIA that reproduces a supplier's opinion unedited is worth less than one that argues with it.

WHAT A CONFIRMATION RECORD IS, AND WHAT IT IS NOT

The Service records that a person confirmed a notice. That is evidence of an act, not of comprehension, and it does not by itself discharge any duty under health and safety, food safety or other law. TeamTalk does not provide legal advice.

1. Why a DPIA, and whether one is strictly required

The ICO's guidance on monitoring workers says an employer **must** carry out a DPIA before any processing likely to result in a high risk, and **should** carry one out anyway even where there is no specific high risk, because it is a scalable tool that improves the decision. It lists examples of high-risk monitoring: biometric data, keystroke monitoring, monitoring that may result in financial loss such as performance management, and profiling or special category data used to decide on access to services.

TeamTalk's assessment, offered honestly rather than defensively: per-worker read receipts are **not** on that list. They are not biometric, not keystroke logging, not content analysis and not profiling, and TeamTalk does not support using them in performance management. On that basis a DPIA is arguably not mandatory. It is nonetheless recommended and pre-completed here, for three reasons: the processing is **systematic and covers all workers**; the workforce often includes people with limited English, agency workers and subcontractors, who are less able to challenge it and whose position the ICO treats as a factor in fairness; and **a DPIA is the artefact that ends the conversation** with a DPO or a union, which is worth more than the argument about whether it was compulsory. If you are on a unionised site, do it.

2. Describe the processing

Controller	[Customer legal name] . Processor: [TeamTalk Ltd] , under the data processing agreement dated [date] .
Nature	Workplace notices are published to named workers in their chosen language. The worker signs in with a one-time code to their mobile number. For a notice marked must-read, the worker taps to confirm. The system records the sign-in and the confirmation, each with a timestamp, and produces a per-site figure, a per-person record and a chase list of people who have not yet confirmed. Text is machine translated. Workers may submit hazard reports with a photograph.
Scope	[N] workers across [N] sites, including employees, agency workers and subcontractors' operatives. Data: name, mobile number, employer, site or team, job or trade, chosen language, start and leaving dates, notice and message content and its translations, sign-in and confirmation timestamps, hazard reports and photographs, device and browser type, IP address, notification tokens.
Context	A frontline workforce, often multilingual, often engaged through subcontractors and agencies, with an inherent imbalance of power. Some workers will have limited English and some limited literacy in any language. The relationship with each worker is [employment / agency / subcontract] .
Purposes	[Your purposes, stated specifically. TeamTalk's expectation: (a) to discharge the duty in s.2(2)(c) HSWA 1974 to provide information and instruction in a form the worker can understand; (b) to know that a safety-critical notice reached the people it had to reach; (c) to identify and chase the people it did not reach.] Do not write "to improve communication": that is not a purpose, it is an aspiration, and the ICO warns against monitoring "just in case".

Retention	The defaults in clause 4.7.5 of the DPA: confirmation records 24 months after the end of the relationship; worker accounts deactivated on the leaving date with identifiers minimised 12 months after; hazard photographs 24 months; logs 90 days. [State any different period you instruct, and why.]
Sub-processors and transfers	Data at rest is in the United Kingdom (AWS London, eu-west-2) . Twilio (United States) receives the mobile number for the sign-in code; Mux (United States) receives video; OpenAI (United States) receives text for translation: Post text, comment text, direct message text and hazard report text are sent for translation. No names, phone numbers or identifiers accompany the text. Bases and check dates are in Annex 3 of the DPA, checked 28 August 2026.

3. Consultation

The ICO says you **should** seek and document the views of workers or their representatives before introducing monitoring, and that if you decide not to you should record that decision with a clear explanation. It also says you should do this **during the early planning stages**, as part of the DPIA, because it avoids complaints later.

WHO	WHEN AND HOW	WHAT THEY SAID, AND WHAT CHANGED AS A RESULT
Workers, or a sample across trades and languages	[date, method]	[Record it. "No comments received" is an answer; leaving it blank is not.]
Recognised trade union or worker representatives	[date, method]	[If none is recognised, say so here.]
Site managers and supervisors who will see the chase list	[date]	[Brief them that the list is for chasing a notice, not for performance.]
Data protection officer	[date]	[If you have one, their independent advice must be sought and recorded before you decide.]
Processor (TeamTalk)	This pack	Product behaviour, sub-processors, transfers, retention and security measures as described. TeamTalk confirms the product has no location tracking, no message-content analysis and no productivity scoring feature.

4. Necessity and proportionality

Lawful basis

Article 6(1)(c), legal obligation, for notices that discharge a statutory duty to inform or instruct, principally s.2(2)(c) of the Health and Safety at Work etc. Act 1974 and, on construction sites, the information duties in the Construction (Design and Management) Regulations 2015. The ICO requires that you identify the specific provision, so cite it in the record rather than referring to "health and safety law" generally. **Article 6(1)(f), legitimate interests**, for everything else, with a legitimate interests assessment covering the purpose, necessity and balancing tests. **Consent is not used and should not be:** the ICO is explicit that consent is not usually appropriate in the employment context because of the imbalance of power.

Special category and criminal offence data

The Service is not designed for Article 9 data. It may arise incidentally in free text, for example an accident notice or dietary or religious information in a canteen notice. The ICO says that where monitoring may capture special category data incidentally you **must** identify a condition for processing, so identify one: [\[Article 9\(2\)\(b\) with DPA 2018 Sch. 1 para. 1, employment, social security and social protection, is the usual route for accident and health-related content\]](#). **Article 10 criminal offence data is a separate regime** and the Service must not be used for it.

Is it necessary, and is there a less intrusive way

The ICO's test is that you must be clear about your purpose and **select the least intrusive means** to achieve it. The alternatives, and why they were rejected:

ALTERNATIVE	INTRUSIVENESS	WHY IT DOES NOT ACHIEVE THE PURPOSE
Toolbox talk with a paper signing sheet	Lower	Records attendance at a talk, not receipt of a specific notice, and only for those present. Says nothing about the night shift, the person on holiday or the subcontractor who arrived on Tuesday. Sheets are collected late, lost, and signed on behalf of others.
Aggregate, anonymous confirmation counts only	Lower	Tells you 78% confirmed. Does not tell you which 22% to go and speak to, which is the entire point. A safety duty is owed to each worker individually, not to a percentage.

ALTERNATIVE	INTRUSIVENESS	WHY IT DOES NOT ACHIEVE THE PURPOSE
A group messaging app, for example WhatsApp	Higher in practice	Read receipts exist, are per person, are visible to every member of the group rather than to a manager, are outside the employer's control, and sit alongside personal numbers, profile photographs and out-of-hours contact. It is more intrusive than TeamTalk, not less, and it is uncontrolled.
Line manager confirms verbally on the worker's behalf	Lower	Records the manager's assertion, not the worker's act, and reintroduces the problem the system exists to solve.
Per-person confirmation, as implemented	The option chosen	Records the minimum needed: the fact and the time of a confirmation of a named notice. No location, no content analysis, no scoring, no continuous observation.

Data minimisation and function creep

What is recorded is the fact and timestamp of a sign-in and of a confirmation. There is **no** continuous location, **no** keystroke or screen capture, **no** analysis of what a worker writes, and **no** productivity score. The ICO warns that monitoring technologies gather more than is needed and that purposes creep over time, so the controller should **write down now** that confirmation records will not be re-used for performance management, and review that annually. [\[If you intend to use them in performance management, that is a different purpose, needs its own lawful basis and its own balancing test, and it is the use most likely to make the monitoring disproportionate. Take advice first.\]](#)

Transparency

The ICO says monitoring conducted without transparency is unfair, and that workers **must** be told in a way that is accessible and easy to understand. The worker privacy notice template supplied with this pack is written in short sentences, carries a **short form under 250 words for translation** into the languages on site, and names the monitoring explicitly rather than burying it. Give it out **before** the first post, on the join card and on the noticeboard as well as in the app.

5. Risks and measures

#	RISK TO THE INDIVIDUAL	BEFORE MEASURES	MEASURE	AFTER
1	A worker feels watched, or believes confirmation records are used to judge their work	Medium	Say the opposite, in writing, in the worker notice and to supervisors: the record is used to chase a missed notice, not to score work. Brief the people who see the chase list. Review annually that it has not crept.	Low
2	A worker confirms a notice they did not understand, and the record is treated as proof that they did	High	The boxed statement above appears in the pilot agreement, the DPA and the security summary, and in the worker notice in plain language: confirming means you got it, not that you understood it, and asking is expected. Keep human briefing for anything safety-critical; do not let the receipt replace the conversation.	Medium
3	Machine translation renders a safety-critical instruction wrongly	High	Translation is machine translation and the agreement says so. Have safety-critical wording checked by a competent speaker before publication. Keep sentences short. Pair critical notices with a briefing or a captioned video rather than relying on text alone.	Medium
4	Special category data arrives incidentally in free text and is processed without a condition	Medium	Identify the Article 9(2) condition now. Tell managers not to put health or personal detail in a general notice. Apply the same security to all content without distinction. Review free-text templates before launch.	Low
5	A worker's mobile number is used outside the purpose, or after they leave	Medium	Access revoked on the recorded leaving date, including mid-session. Identifiers minimised 12 months after that date. Numbers are not used for marketing and the acceptable use clause forbids it.	Low

#	RISK TO THE INDIVIDUAL	BEFORE MEASURES	MEASURE	AFTER
6	Personal data is exposed to another tenant or to a third party	Medium	Logical tenant isolation enforced at the data layer, with automated cross-tenant tests [not yet; target date] . Encryption in transit and at rest. Impersonation logged. Sub-processor list kept short and published. Ask the supplier for the date the cross-tenant tests ship and hold them to it.	Medium until the tests exist
7	Notice text is transferred to the United States for translation	Medium	Post text, comment text, direct message text and hazard report text are sent for translation. No names, phone numbers or identifiers accompany the text. Transfer under Article 46 on the ICO Addendum with a documented transfer risk assessment. Managers told not to name individuals in the body of a notice that will be translated.	Low
8	A photograph in a hazard report identifies a worker who did not consent to it	Medium	Tell workers, in the notice, that a hazard photograph may show people. Instruct reporters to photograph the hazard, not the person. Retain 24 months then delete. Handle any objection under Article 21.	Low
9	Agency and subcontractor workers are less able to object than direct employees	Medium	Give the notice to every worker on the same terms regardless of who employs them, and route questions to a named person on the customer's side, not to their agency. Record objections centrally.	Low
10	The supplier fails, and access to the records is lost	Medium	Export available for 30 days on termination for any reason including insolvency, written into the agreement. Take a periodic export of the briefing records you rely on and keep it yourself.	Low

6. Outcome, sign-off and review

Residual risk	[Low / Medium] . If any residual risk is assessed as high and cannot be reduced, you must consult the ICO before starting , under Article 36. TeamTalk's view is that with the measures above the residual risk is not high, but the assessment is yours.
DPO advice	[Record the independent advice and whether it was followed. Required where you have a DPO.]
Decision	[Proceed / proceed with conditions / do not proceed] , decided by [name, role] on [date] .
Before monitoring starts	The worker privacy notice is published and distributed, in the languages on site; supervisors are briefed; the Article 9 condition is recorded; the legitimate interests assessment is signed.
Review	At [6] months, then annually, and on any change to the purpose, the sub-processors or the product. Check specifically for function creep into performance management.

Not legal advice. This is a pre-completed draft prepared by a processor for a controller to adopt, edit and sign. It does not replace your own assessment and it does not bind the Information Commissioner. **Sources, verified 28 August 2026.** ICO, *Employment practices and data protection: monitoring workers*, in particular "Can we monitor workers?" (least intrusive means), "How do we identify a lawful basis?" (consent not usually appropriate in employment), "What if our monitoring involves special category data?" (a condition is required where capture is likely even if unintended), "Do we need to do a data protection impact assessment (DPIA) before we start monitoring?" (must for high risk, should otherwise, and the high-risk examples), "How do we ensure we are transparent about monitoring?", "Should we discuss the introduction of monitoring with our workers?" and "What do we need to consider if we use a third-party provider" [ico.org.uk monitoring workers](#). That guidance is marked as under review following the Data (Use and Access) Act 2025, so re-check it before each annual review; ICO, *Data protection impact assessments*, including the screening checklists and "Do we need to consult the ICO?" [ico.org.uk DPIAs](#); UK GDPR Articles 5, 6, 9, 10, 13, 21, 35 and 36 [legislation.gov.uk/eur/2016/679](#); Data Protection Act 2018 Sch. 1 [legislation.gov.uk/ukpga/2018/12/schedule/1](#); Health and Safety at Work etc. Act 1974 s.2(2)(c) [legislation.gov.uk/ukpga/1974/37/section/2](#); Construction (Design and Management) Regulations 2015, SI 2015/51 [legislation.gov.uk/uksi/2015/51](#).