



Changing the world
of work for good

Empowering people through data intermediaries

**The TUC's response to the
consultation by the Department for
Digital, Culture, Media & Sport**

The Trades Union Congress (TUC) represents the 5.3 million working people who make up our 47 member unions. We support unions to grow and thrive, and we stand up for everyone who works for a living.

Our core mission is to protect and advance the interests of working people. How workers' personal data is captured, analysed, and used in the workplace – as well as how workers and their unions can access and benefit from that data – is a key concern for the TUC. It is crucial that workers have rights to access their own data, are protected from employer misuse of data and are informed about these rights.

Therefore, our response to this consultation focuses on data rights specifically in the employment context. We believe that there is scope for greater alignment between the employment rights and data rights regimes.

Data intermediaries, in the form of not-for-profit data trusts stewarded by trade unions, could bring clear economic benefits by enabling workers to secure better pay and conditions through their workplace data – only where strict safeguards exist against commercialisation, employer capture, and coerced consent. Enabling data portability through these intermediaries could be a useful step towards a more level playing field between workers and their employer in the context of data rights, but it is not sufficient on its own.

In May 2025, [the TUC responded](#) to the Department for Science, Innovation and Technology's call for evidence on data intermediaries. Several of our key points are reiterated here.

Data rights in the workplace

As increasingly advanced technologies are being rolled out in the workplace, employers have access to a growing range of worker data. This data is most valuable when it can be analysed at scale. For employers, this can mean measuring performance across the workforce, identifying patterns, and predicting needs or prescribing changes.

Whilst employers benefit from workers' data, workers themselves have extremely limited access to data and few opportunities to benefit from the data that they create. Under the UK General Data Protection Regulation (UK GDPR), workers only have the right to access their data on an individual basis, primarily through subject access requests (SARs). This system allows individuals to obtain a copy of their personal information and other supplementary information. But compliance with these rules is patchy. When workers do receive data through a SAR, it is often difficult for them to interpret and utilise that data in isolation to improve their position in the workplace.

However, how employers use and analyse worker data, including through algorithms, has collective implications for workers. An individualised system is therefore ill-suited for the workplace context, where rights often must be exercised collectively to address the power imbalance between workers and their employer.

This imbalance creates barriers to individuals exercising their data rights in the workplace context: decisions involving worker data are made by an employer in private. Workers need to be highly informed and engaged to request their data – and they need to be willing to identify themselves to their employer as the person making the request or complaint. Even where workers can access their individual data, they often find that they are unable to meaningfully analyse it.

Workplace technologies increasingly enable employers to collect data that goes beyond what's necessary for its intended purpose. This includes things like granular behavioural data, location data, and biometric and health data. The increased use of algorithmic decision-making in the workplace has enabled employers to use these disparate data points to profile workers and make decisions that impact their jobs.

For example, [dynamic pay systems](#) use algorithms to decide, in real time, how much individual drivers are offered for each journey, based on factors including drivers' personal data and behaviour. Two different drivers can be offered the same job, but with two different rates of pay. Drivers have little visibility or control over how their pay is calculated, only receiving offers they must rapidly decide to take or leave. If, for example, drivers wanted to understand how their personal data is collected and analysed by algorithms to set their pay, it would only be possible to do so by analysing that data collectively across the workforce to identify patterns.

This extends beyond the gig economy. Workers in [Amazon warehouses](#), for example, are highly monitored for the stated purpose of safety and security. Their data is used to set performance targets, which workers say they struggle to understand. The opacity of data collection and use by employers prevents workers from understanding how decisions are made around key aspects of their jobs, making those decisions difficult to challenge.

This should be a significant concern for the government. Ensuring workers can bargain on pay and conditions is fundamental to the goals of the government's Make Work Pay agenda. But where there is not transparency on how pay is set, as is the case with dynamic pay, workers are unable to bargain on their pay in practice.

Empowering workers through collective data rights

In this environment, it is crucial that workers have rights to data, protection from employer misuse of data and are informed about these rights. Trade unionism is premised on the idea that when workers can organise and bargain collectively, the power imbalance between workers and their employer starts to shift. Collective bargaining is [a proven mechanism](#) for tackling inequality, supporting productivity, and managing industrial change – including technological change. That same logic must now be applied to data rights in the workplace context.

Through expanded data portability rights, data intermediaries, in the form of not-for-profit data trusts, could enable individuals to better exercise their data subject rights in the workplace. [Data trusts](#) manage an individual's data rights on their behalf, and can

collect, store, aggregate and determine how to process their personal data. This would enable workers and their unions to access the personal data that they have 'provided to' their employer, such as their location data, search activities, or raw data from wearable devices.

This is more limited than the data provided in an SAR, which would include inferred or derived data produced through an algorithm. But it would provide workers with a better understanding of what data their employers collect on them, and through their unions, the opportunity to analyse this data and data collection at scale.

Unions are well-placed to steward this data, with permission from members and subject to defined purposes and governance obligations. They are used to representing workers at scale and could provide workers with access to the appropriate tools to understand and analyse their personal data. Unions are also best placed to leverage this data to benefit workers: to support better enforcement of data rights in the workplace, to identify patterns and potential bias, and for collective bargaining.

There is limited guidance on how to become a not-for-profit data trust. Therefore, unions will need support and resources, including guidance on becoming data intermediaries and funding to support the additional resources that developing and managing this type of programme would require.

Safeguarding workers' data

Extending rights to delegate personal data to an intermediary would come with significant risk, particularly in the workplace context. The use of data intermediaries in the employment context must be subject to strict safeguards that exclude use of commercial data intermediaries and prevent employer capture.

This should exclude commercial data intermediaries, who are primarily incentivised by generating revenue, from being able to operate in this context. Failure to do so risks creating a new market for worker data. This would enable commercial products to be built from that data without genuine control by workers, and risks strengthening employers' informational advantage.

Similarly, without clear safeguards, employers could steer workers towards a particular data intermediary, which may not be in workers' best interests. Individual employee consent should not be used as a mechanism for employers to circumvent this distinction, given the power dynamics in the workplace and the precedent on consent in the workplace context set by the Information Commissioner's Office.

Portability offers a route for workers and their unions to leverage some worker-generated data, but collective workplace data rights are needed to access the fuller range of data used in algorithmic decision-making. We set out below the policy changes needed to establish such a system.

Policy recommendations

- **Enable not-for-profit worker data trusts:** Government should support trade unions to act as trusted, not-for-profit data intermediaries that steward worker data in workers' collective interests.
- **Exclude employer-led or commercial misuse:** Any delegation framework should clearly distinguish worker-led not-for-profit data trusts from commercial intermediaries or employer-controlled data sharing models in the employment context.
- **Provide resource support and guidance:** Government should fund and guide unions and other not-for-profit worker organisations to build the legal, technical and governance capacity needed to operate as data intermediaries.

Wider reforms include:

- **Create collective workplace data rights:** Government should establish a legal framework allowing workers to exercise data rights collectively, not only through individual subject access requests.
- **Give unions a statutory right to member data:** Trade unions should have a clear legal right to access relevant anonymised worker data, particularly where it is used for algorithmic decision-making. For example, under Section 8 of the TUC's model [Artificial Intelligence \(Regulation and Employment Rights\) Bill](#), trade unions would have a statutory right to request and receive all data collected by an employer that is used (or proposed to be used) for AI-powered decision-making.
- **Introduce a right to data reciprocity:** Where employers collect and analyse worker data, workers and their unions should have reciprocal access so they can scrutinise decisions, challenge unfair outcomes, and bargain effectively.