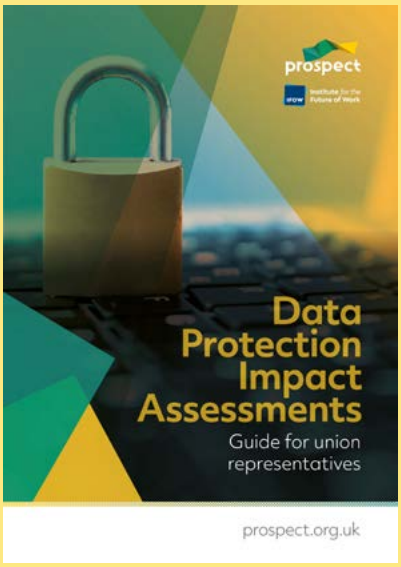
prospect

IFOW Institute for the Future of Work

Data Protection Impact Assessments

Guide for union representatives

prospect.org.uk



Acknowledgements

This briefing is part of Prospect's Future of Work activity. We'd like to thank staff, members and all those union and data specialist colleagues who have assisted in its production, in particular Anna Thomas and the Institute for the Future of Work, Ravi Naik, Cassie Roddy-Mullineaux and Eric Kind of AWO, Dr Christina Colclough, Ian Brown and Dr Phoebe Moore.

If you have further questions about the DPIA process or would like advice on how you can raise these issues please contact andrew.pakes@prospect.org.uk

Published by Prospect
New Prospect House,
8 Leake Street, London SE1 7NN
T 0300 600 1878

PRO-20-0015/NOV20-PDF

Introduction

Technology is transforming the way we work and the way employers interact with their employees. You might have heard of 'automated decision-making' where, say, job applications are filtered for words and phrases before they reach a human. And you might have heard about tracking tech which monitors colleagues' working patterns and activity - for example, when you're logged onto your email or when you're out in your company car.

With every tech interaction, data is gathered which helps businesses and organisations understand who their employees are and how they behave. The trend of monitoring and data gathering by employers has been growing at pace over the past few years. The move to remote working has led to a greater use of digital platforms - you may have a work email address, Zoom account, Slack account, WhatsApp group which can be analysed for activity.

This guide sets out workers' rights to be consulted about how our data is used through GDPR. Employers should be involving workers and their unions about how our data is used. The basis for consultation is set out in the General Data Protection Regulations (GDPR) and the Data Protection Act (2018). This guide is designed to help you make use of these rights.

The use of our personal data at work is covered by the GDPR. This is about our standing at work, how we are treated and whether employers make judgements about our work based on the information collected. Given the use of that data may impact the relationship between us and our employers – and our employment more generally – the processing of such data may be "high-risk" and result in "significant affects".

When employers introduce a different way of using our data that could present high risks to our rights and freedoms or produce significant affects to us, they need to conduct a Data Protection Impact Assessment (DPIA). Union reps and workers should be involved in a DPIA.

This is not just what we are saying as a union. The UK's official data regulator - the Information Commissioner's Office (ICO) - is also clear that workers and their representatives should be consulted as part of a DPIA. This guide is to help representatives ensure that meaningful consultation happens on a regular basis.

This is about safeguarding our rights at work – and ensuring safeguards for the use of our data.

1: Data is transforming work

Digital monitoring and data gathering by employers has been growing at pace over the past few years.

Examples include location tracking, human resource tools for hiring or deciding who to fire, keystroke monitoring, wearable sensors, CCTV, voice recordings and social media trawls.

There is already evidence that some workers are unaware of, or intentionally excluded from, decisions about workplace surveillance, the information that is gathered about them and how this information is used.

The workplace is a critical arena for testing the relationship between digital transformation and employment rights.

Our own research[1] at Prospect shows that most workers are unsure what data is currently collected about them by employers.

Covid-19 has sharpened many of these issues with remote working and the widespread adoption of digital solutions. Video conferencing and other online networking platforms, like CrowdCast webinars or Slack messaging, have become central to many people's work and an almost constant presence in their homes.

But there is also another side to this discussion with employers examining how to use technology to monitor homeworkers. Just look at some of the headlines during lockdown:

"Bosses are panic-buying spy software to keep tabs on remote workers" [2]

"The boss in your bedroom: as workplace surveillance spreads, what are your rights?" [3]

"Creepy technologies are invading European office spaces as people go back to work" [4]

Even with the best of intentions, employers may be failing to take precautions and care over how this information is handled, stored and used in a way that employees would wish, and that the law requires.

Ensuring unions are involved: what does good practice look like?

We believe that the introduction of new data processes and technology should be:

- openly undertaken in consultation with unions and the workforce
- transparent so that workers can identify and be informed about what data is being collected about them and why
- clear on the uses of the data collected
- governed by employers in cooperation with the union on the use/future use of the data, data storage, and offboarding (deletion and/or selling)
- subject to scrutiny by unions to make sure data is handled in line with GDPR principles
- understood in terms of implications for privacy, equality and potential discrimination.

Prospect would like to see employers and unions work together on how data is used at work. Regular, formal discussions along with shared governance on the use of data give the best protection for employers, as well as employees, against the legal and reputational risks that new technologies and data-processing techniques may bring.

1 https://prospect.org.uk/future-of-work-technology-and-data/
2 https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers
3 https://mimicnews.com/the-boss-in-your-bedroom-as-workplace-surveillance-spreads-what-are-your-rights
4 https://theprint.in/world/creepy-technologies-are-invading-european-office-spaces-as-people-go-back-to-work/426174/

2: GDPR

GDPR rules were incorporated into UK law by the Data Protection Act 2018 to provide a framework for considering workers' views when new data processes are introduced. The rules provide scope to:

- check if an employer is fulfilling their obligations under the law
- ensure that the union is appropriately informed and involved as representative of its members
- provide visible evidence on what data is being collected, how and why.

Personal data

Personal data is the foundation of GDPR. Every person whose data is collected - or processed - is called a "data subject", whether you are identified directly in that data or "identifiable". Since personal data about you is collected by your employer, you are a "data subject".

Personal data can be any information that relates to an identified or identifiable individual - for example your unique staff number, your telephone, credit card, number plate, home address, personal email address. Personal data can even include data which indirectly identifies you, like unique GPS co-ordinates. It also includes data which could reveal special characteristics about you like trade union membership, religious, philosophical and political preferences, health concerns, biometric and genetic data – and there are additional restrictions around how employers can use these 'special category data'.

Legal basis for consultation

1. When is a DPIA required?

The GDPR sets out the legal requirements for Data Protection Impact Assessments (DPIAs). Article 35 GPDR states that a DPIA will be required where the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Recital 75 of the GDPR says that such "high-risk" processing

> *may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*

This includes cases involving "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or

similarly significantly affect the natural person."[5]

Official guidance about when processing is likely to need a DPIA expressly includes employee / employer relations

> *because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management.*[6]

Taken together, the use of personal data to monitor employees' activities should require a DPIA as such monitoring involves (i) systemic monitoring and (ii) data concerning vulnerable data subjects, owing to the "power imbalance between" the employer and employee.

2. High-risk use of workers' data: When should an employer carry out a DPIA?

The systematic collection of workers' data presents an inherent high-risk to individual employees as it could affect or impact on the employment relationship. This could include the risks of:

- Loss of data or poor security in how employers collect, store and use the data.
- Damage to workers standing or reputation
- Material damage through decisions made using the data, such as promotion opportunities, pay or performance management
- Discrimination based on decisions made using the data.

The burden is not on the union or employees to demonstrate what the risk is before a DPIA is carried out, just that the risks exist.

Moreover, employees are in a "vulnerable" position because of the power imbalance inherent in the introduction of such new technology.

Taken together, it is very likely that the introduction of any technology to monitor, assess or evaluate employees will require a DPIA. That DPIA should be conducted by the employer as the data controller. It is not appropriate for the employer to rely on any DPIA conducted by, for example, the manufacturer of the technology. The burden is on the employer as the data controller to assess the risks through a DPIA.

Any such DPIA must be conducted before the processing occurs, to guard against risks.

Example: If an employer is thinking about changing how workers' data is used, for example through new monitoring or tracking software, then they should carry out a DPIA. The

5 Article 35(3)(a) GDPR

6 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Adopted on 4 April 2017) (as endorsed by the EDPB). See also, ICO Guidance on DPIAs: https://bit.ly/ico-dpia-when9

UK Information Commissioners Office (ICO) has stated that consultation with data subjects is a key part of this process.

A DPIA should not be a tick-box exercise. It needs to be objectively and meaningfully conducted. It should be seen as a real chance to consider and weigh the risks of data processing to employees against the benefits to the technology. Such an analysis cannot sensibly be conducted without the involvement of the employees.

Failure to undertake a DPIA when it is required is a breach of the GDPR and may result in unfair processing, in breach of the basic principles of data processing in Article 5 GDPR.

3. Consultation over the DPIA

Article 35.9 confirms that "the controller shall seek the views of data subjects or their representatives on the intended processing." Thus, workers' representatives (which includes unions) should be consulted by employers before the introduction of new data processes, including surveillance technology. As such, employers should engage in consultation and the involvement of workers (as data subjects) when new high-risk data processing is introduced at work. .

What does consultation mean?

According to the ICO, employers must, where appropriate:

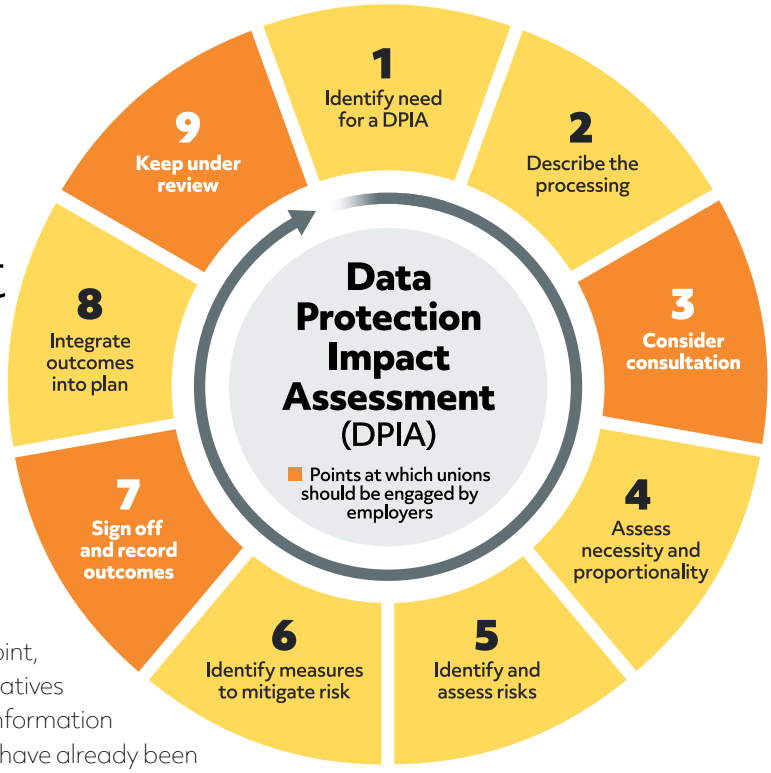
- **seek and document the views of individuals or their representatives, unless there is a good reason not to;**
- **consult all relevant internal stakeholders;**
- **consult with your processor, if you use one;**
- **and consider seeking legal advice or other expertise.**

The ICO also states employers should describe what is proposed in a way that those they consult can understand.

Source:
ICO, Guidance on AI and data protection (2020) – https://bit.ly/ico-gai-2020

The ICO guidance on DPIAs also explicitly mentions consulting employees – https://bit.ly/ico-dpia-how7

3: Undertaking a Data Protection Impact Assessment



Source: ICO – Steps for conducting a DPIA annotated by Prospect https://bit.ly/ico-dpia-check

The ICO has produced UK guidance on how a DPIA should be undertaken. They have set out a framework involving nine steps for what should be included. This should involve consultation with affected individuals, in this case workers directly affected, and their representatives, through a union or other representative forum.

In terms of a DPIA, the focus should be assessing the risk of harm to an individual's rights and freedoms if data is collected and processed in a certain way. This can also include an impact on their economic or social position.

We would argue that where a trade union is recognised there is an established process through collective bargaining for consultation.

As a starting point, union representatives should ask for information on what DPIAs have already been conducted and on how the union will be involved in future DPIAs.

The ICO has produced detailed guidance on the different steps in the DPIA process. See: **https://bit.ly/ico-dpia-qas**

Equality Impact Assessments

We would argue that the collection and use of our data should be assessed for equality impacts. Prospect is working with the Institute for the Future of Work[7] to examine how Equality Impact Assessments should be used as part of a DPIA in order to assess and protect the right and freedoms of data subjects. This is also looking at the Public Sector Equality Duty and how it applies to data. This will promote best practice and help employers demonstrate legal compliance.

7 Equality Impact Assessment, Institute for the Future of Work:https://bit.ly/ai-hire-equality

What must be included in a DPIA?

As union representatives, you can scrutinise your employer's DPIA to make sure it:

- **Provides a description of the proposed processing of the data, and the reasons why the processing is taking place.**
- **Explains the legal basis for the processing.**
- **Provides an assessment of how necessary the processing of the data is in relation to the reasons for the processing – employers should only be collecting the minimum amount of data needed.**
- **Consults with the relevant stakeholders – this should include trade union and/or workforce representatives**
- **Identifies and assesses the risks to the personal data of individuals.**
- **Identifies the measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulations.**
- **Details recommendations to be signed off by project managers - the outcomes should be incorporated into the project plan.**

4: What should unions be looking for?

Unions should be consulted as part of an organisation's overall approach to our data, as well as under the scope of GDPR. Given the high-risk to workers in how our data is collected, stored and used, union reps should be made aware and more importantly consulted when:

- new processes are being introduced;
- there is a change to an established process; or
- when new technology is introduced.

The DPIA isn't about protecting the personal data per se (although that is part of it); it's about protecting the rights and freedoms of data subjects; including privacy, but also freedom of expression, equality, etc).

These are some of the questions that unions should consider asking of employers:

- What DPIAs have you already undertaken in relation to the processing of any employee personal data?
- When and how have you consulted workers or union representatives – as data subjects – in relation to the processing of employee data?
- What is your policy around who to consult in the conduct of a DPIA and will you share that with the union?
- Will you involve union reps and the workforce in the DPIA process?
- What regular checks are you putting in to review how the data is being used?
- What data processes or new technology are you thinking about introducing?
- What systems do you have in place for new technology that is self-learning or adapting in relation to review processes for risk, rights and legal compliance?

Safeguarding workers' rights and interests

Once the risks have been identified the DPIA should consider how to mitigate them. The law acknowledges that not all risks can be eliminated entirely but there may be actions that can be taken to reduce them to an acceptable level. This could include:

- Consultation as part of the procurement process.
- Higher levels of consultation in design and deployment of the system.
- Decide not to collect certain types of data.
- Reduce the scope of the processing.
- Reduce the retention period.
- Taking additional technological security measures.
- Training staff to ensure risks are anticipated and managed.
- Anonymising data where possible.
- Writing guidance or process procedures.
- Using different technology.
- Ensuring sharing agreements are in place.
- Making changes to privacy notices.
- Giving individuals the chance to opt out.

Six Principles of GDPR

Article 5 of GDPR sets out six principles on the collection and use of personal data. These principles are important and should be used to help inform discussions with employers and in consultation as part of a DPIA.

1. Data is processed lawfully, fairly and in a transparent manner.
2. Data is collected for a specified, explicit and legitimate purpose.
3. Data is adequate, relevant and limited to what is necessary in relation to the purpose.
4. Data is accurate, and where necessary kept up to date.

5. Data is kept for no longer than is necessary for the purposes for which the data is processed.
6. Data is processed with appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Keeping DPIA under review

Risks over data can change over time, so the DPIA process is designed to be ongoing. The ICO says the initial DPIA is not complete unless it is signed off and its outcomes recorded. We would argue that it also needs to be reviewed on a periodic basis to assess if the risks have changed, such as the technology is used in a different way, or material contextual changes have occurred, like a global health pandemic or significant change of employees.

In recording the outcomes of the DPIA, employers should record:

- What measures an employer plans to take;
- Whether each risk has been eliminated, reduced or accepted;
- The level of 'residual risk' after taking additional measures;
- If a high level of risk still exists, consult with the ICO.

Unions, as representatives of affected data subjects, should expect to be informed and involved.

The ICO says that the findings or assessment of a DPIA should be kept under review. Unions should be asking under what period a DPIA will be reviewed, and how they will be involved in checking that the original outcomes are still accurate and appropriate.

What questions should be asked during a DPIA?

The role of the consultation in a DPIA is to enable the union/workers to question the new process:

- **How is the data going to be used?**
- **Why is the personal data being collected?**
- **What are the sources of these data?**
- **How have you identified risks arising from the use of individual personal data and the rights/ freedoms of the collective group of employees?**
- **What are these risks and how can they be reduced?**
- **If you have decided not to consult with union reps, can you disclose the reasons why?**
- **What will be the review process?**
- **How will data breaches be shared with the union?**

Appendix A: Examples of how this may affect workers

An employer must undertake a DPIA for new projects involving personal data or look to changing existing use of personal data. These are some examples of what this may mean for your work.

Use systematic and extensive profiling which produces a significant effect	Data on an employee's performance at work, sickness absence, time-keeping or behaviour impacts on performance-related pay.
Systematic monitoring: processing used to observe, monitor or control individuals on a large scale	Employees are monitored through internal CCTV or their access to buildings or rooms are controlled by passes.
Process special category or criminal offence data on a large scale	Data is collected on or may reveal an employee's special characteristics - as outlined by Article 9 of GDPR - ie trade union membership, race or ethnic origin, political opinions, religious or philosophical beliefs, health, sex life or sexual orientation, genetic data, and biometric data.
Use of innovative technology	An employer plans to use: artificial intelligence, machine learning, smart technologies, or plans to collect information captured by physical systems in one place. A DPIA is also required if existing technology is used in a new way.
Processing biometric or genetic data	Biometric data could include fingerprints, facial recognition, and voice pattern recognition. Genetic data could include DNA testing.
Matching data or combine datasets from different sources	Integrating two databases.
Collecting personal data from a source other than the individual without providing a privacy notice (invisible processing)	Data on an individual is collected from a non-work website and added to their work record without consent.
Tracking individual's location or behaviour	Company cars may also be used for private purposes, and location-tracking features might allow managers to monitor movement and whereabouts of employees at all times.

Appendix B: Checklist for unions

- [ ] Ask your employer if they are aware of their responsibilities to conduct DPIAs and to confirm the existence of any DPIAs relating to the processing of workers' personal data. Ask if they will undertake to inform and involve you as and when future DPIAs are undertaken.
- [ ] Check when and how your employer has consulted workers on the use of personal data in any relevant changes to technology at work. Ask them to provide information about who they have consulted before the change took place.
- [ ] Ask for a review of the consultation process for how new data/technology uses are introduced to ensure that workers are named. Negotiate for union reps to be included in the consultation process as representatives of data subjects.
- [ ] Ask for information about how your employer undertakes assessment of risks and safeguards.
- [ ] Consider how you communicate or consult with members and other workers about the DPIA and the union's involvement in it.
- [ ] Ensure the employer knows the union's views about the issues, potential risks, and possible ways of reducing or mitigating these.
- [ ] Seek to be informed about how the DPIA will be recorded and its outcomes signed-off. Seek to union involvement in agreeing this.
- [ ] Ask about how and when the DPIA will be reviewed, and how the union will be informed and involved.
- [ ] Seek to establish an ongoing dialogue with the employer about data, data-processing and new technology.
- [ ] Ensure union members and other workers are aware of how the union is working on their behalf to ensure they are informed, involved and their rights protected.

prospect

IFOW Institute *for the* Future of Work

prospect.org.uk