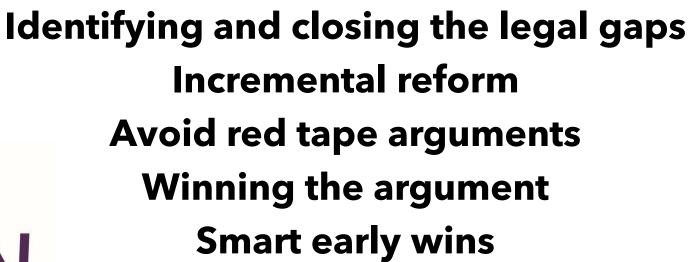
- Employers harnessing new technologies to create data on employees to drive up production, mangement and business planning but without balancing workers' rights
  - Miss match& imbalance with business ahead and Labour behind

eform employment and equality laws with Al and data protections



Digitalisation and AI in the employment cycle: recruitment, promotion, disciplinary issues, time keeping monitoring, surveillance, productivity monitoring, facial, speech and drone recognition, contact control, bonuses, pay rewards, orm rights, working from home, teleworking ermination of contracts of employment





- Trade Union and Labour Relations (Consolidation) Act 1992
- Human Rights Act 1998 European Convention on Human Rights ("ECHR")
  - Employment Rights Act 1996
    - Equality Act 2010
  - Public Sector Equality Duty 2011
  - GDPR Data Protection Act 2018



**Employers should generally conduct an Equality Impact Assessment (EIA) before** introducing digital and AI systems that determine the impact on access to work, direct and indirect discrimination, on the terms and conditions of work, employees with protected characteristics, job losses and re-skilling, apprenticeships, changing nature of work and job roles to fit around the introduction of new technology etc.



**Employers should generally conduct an Equality Impact Assessment (EIA) before** introducing digital and AI systems that determine the impact on access to work, direct and indirect discrimination, on the terms and conditions of work, employees with protected characteristics, job losses and re-skilling, apprenticeships, changing nature of work and job roles to fit around the introduction of new technology etc.



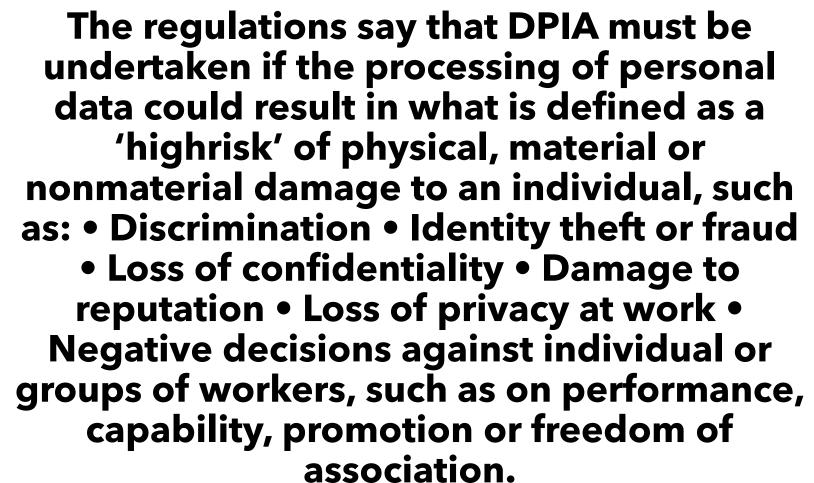
Article 35 of GDPR lays out the scope for Data Protection Impact Assessments (DPIAs).

It states that workers' representatives (which includes unions) should be consulted by employers before the introduction of new data processes, including surveillance technology



**Data Protection Impact Assessments (GDPR** Article 35): "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."







A DPIA should: 1. Describe the proposed processing of the data and explain why the processing is taking place. 2. Provide the legal basis for the processing. 3. Give 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. 4. Consult with all relevant stakeholders - including trade union and/or workforce representatives



5. Identify and assess the risks to the personal data of individuals. 6. Provide mitigation of risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulations. 7. Detail recommendations to be signed off by project managers - the outcomes should be incorporated into the project plan.



Data processing must comply with Article 5

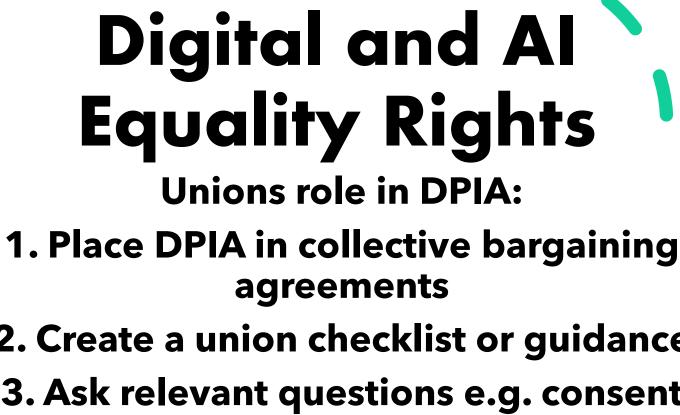
- 1. Data is processed lawfully, fairly and in a transparent manner.
- 2. Data is collected for a specified, explicit and legitimate purpose.
- 3. Data is adequate, relevant and limited to what is necessary in relation to the purpose.
- 4. Data is accurate, and where necessary kept up to date.



Data processing must comply with Article 5

- 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







- 3. Ask relevant questions e.g. consent
- 4. Propose alterantive risk mitigations
  - 5. Monitor and review the DPIA with employer for compliance and risks



Challenges to securing digital equality rights

1. Two assessments EIAs and DPIAs - be better to have a new umbrella assessment which would also include binding human and ethcical rights

. Defne 'high risk' and 'low risk'and streghthen targetted regualtion

3. Precuationary Principle - how do we prevent harmful applictions from the beginning



Challenges to securing digital equality rights

- 4. Business wants to 'self-govern' their use of high-risk data need a statutory duty that they must consult on AI and Automated Descion -Making (ADM) technology
- 5. Change employment law so that workers have a statutory right not to suffer any detriment on the grounds of inaccurate data processing.



Challenges to securing digital equality rights



7. Strengthening the principle of non-discrimination in all stages of the employment relationship - a new statutory Code of Practice supplying guidance on avoiding discrimination in an age of digitalisation. Example human oversight in ADM mandatory



Challenges to securing digital equality rights

- 8. Amend GDPR to state that fully automated discriminatory data processing is always unlawful.
- 9. Rewrite burden of proof in discrimination claims that challenge "high risk" Al and ADM, so that the business or undertaking using such systems have the full burden of explaining how they have worked and that they are not discriminatory.



Challenges to securing digital equality rights



11. Remove trade agreements global ecommerce protections of IPRs - trade secrets and patenets - in algorithms and source codes





Challenges to securing digital equality rights

12. See inside the 'black box'

- intentional opacity, where the system's workings are concealed to protect intellectual property
  - illiterate opacity, where a system is only understandable to those who can read and write computer code
  - intrinsic opacity, where a system's complex decision-making process itself is difficult for any human to understand

Challenges to securing digital equality rights



13. Strengthen GDPR obligations under 3 key articles 21, 6,22 as it only says that the data provider must provide an explanation that is meaningful about the logic involved but is not obliged to give a complex disclosure of the full algorithms

**Caimpaigning Tool Kit for unions** 

- 1. Prevent costly work tribuanals
  - 2. Set the pace of change
- 3. Put workers' rights at the heart of new Allaws
  - 4. Promote workers voice and put trade unions on the AI table

