LEWIS SILKIN

16 April 2024

Artificial Intelligence in the Workplace

Bryony Long

Bryony.Long@lewissilkin.com
+44 (0)20 7074 8435

Agenda

- The AI Act and How it Interacts with the GDPR and Health and Safety Legislation – Planning Your Approach
- Practical Impact of Platform Workers Directive

LEWIS SILKIN

The AI Act and How it Interacts with the GDPR and Health and Safety Legislation – Planning Your Approach

Ideas. People. Possibilities.

How AI is being deployed in workplace?

- Recruitment and selection (job descriptions, CV sifting)
- Performance Management (automating reviews, strength/improvement analysis, linking areas for development with skills)
- Skills matching (new opportunities, training, planning career progression)
- Access to resources
- DE&I (mitigate cognitive and algorithmic bias)
- Employee Engagement (gen AI to get short, regular responses)
- Recognition (image, speech)
- Detection (fraud, cyber incidents, employee welfare)
- Forecasting (workforce management)

Existing laws and guidance regulating AI in the workplace

- The Equality Act 2010
- GDPR/UK GDPR (especially Article 22)
- Common law (employment relationship)
- Caselaw
  - Facial Recognition tech – Uber Eats
- Guidance
  - DSIT – Responsible AI in recruitment
  - ICO - Guidance on AI and data protection
  - Alan Turing Institute and ICO - Explaining decisions made with AI

Legal developments on AI regulation - US, UK and EU

US

- US Executive Orders
- Blueprint for AI Bill of Rights
- NIST Framework
- NY Automated Employment Decision Tools (AEDT) Law 144 of 2021
- Illinois AI Video Interview Act (820 ILCS 42/1)

UK

- White Paper + response
- Light touch → guardrails
- Global Safety Summit - Bletchley Declaration
- ICO guidance
- DSIT guidance – Responsible AI in recruitment

EU

- EU AI Act
- EU AI Liability Directive
- EDPB?
- Local?

EU AI Act

“We finally have the world’s first binding law on artificial intelligence, to reduce risks, create opportunities, combat discrimination, and bring transparency.”

Brando Benifei, Internal Market Committee co-rapporteur

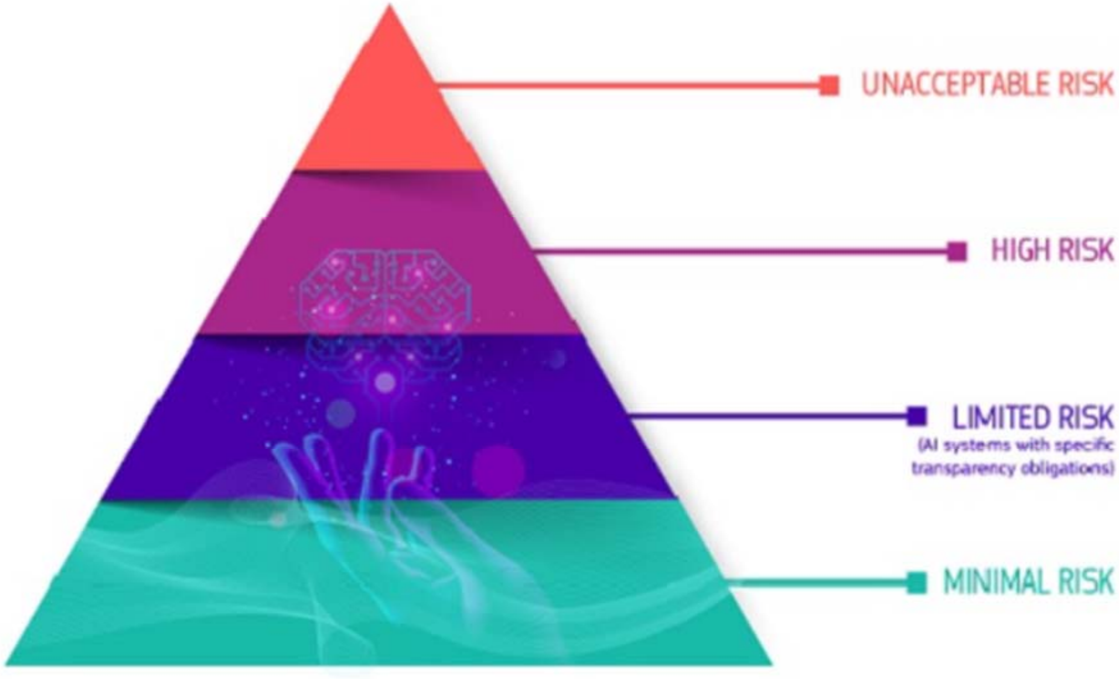
How will it be enforced?

- Member state authorities will lay down rules on penalties and other enforcement measures, e.g. warnings and non-monetary enforcement
- Individuals can lodge an infringement complaint with a national competent authority, which in turn can launch market surveillance activities
- No provision for individual damages

- Penalties
  - Prohibited AI violations, **up to 7%** of global annual turnover or **€35 million**
  - Most other violations, **up to 3%** of global annual turnover or **€15 million**
  - Supplying incorrect information to authorities, **up to 1%** of global annual turnover or **€7.5 million**

What does the Act say and how will it affect you?

- Risk-based approach
- 4 levels of risk



EU AI Act – Recital 36

“AI systems used in ***employment, workers management and access to self-employment****, notably for the* ***recruitment and selection of persons****, for* ***making decisions affecting terms*** *of the work related relationship* ***promotion*** *and* ***termination*** *of work-related contractual relationships for* ***allocating tasks*** *based on* ***individual behaviour, personal traits or characteristics*** *and for* ***monitoring or evaluation of persons*** *in work-related contractual relationships, should also be* ***classified as high-risk****, since those systems may appreciably impact future career prospects, livelihoods of these persons and workers’ rights.”*

High Risk – key obligations

Providers

- designing the systems to allow for **effective human oversight**
- designing the systems to ensure an appropriate level of **accuracy, robustness and cybersecurity**
- drafting and maintaining **technical documentation** for the AI system
- establishing, implementing, documenting and maintaining a **risk management system and quality management system**
- meeting **data governance** requirements, including bias mitigation
- **record-keeping, logging and traceability** obligations
- complying with **registration obligations**
- ensuring the relevant **conformity assessment procedure** is undertaken
- provider's **contact information made available** on the AI system, packaging or accompanying documentation
- drawing up the **EU declaration of conformity** promptly
- ensuring the "**CE marking of conformity**" is affixed to the AI system

Deployers

- **informing** workers representatives and the impacted workers that they will be subject to a high-risk AI system
- using information from the providers to **carry out a DPIA** (likely to be required for high risk system)
- undertake a **fundamental rights impact assessment** for certain deployers and high-risk systems, e.g. if evaluating the creditworthiness of individuals or establishing their credit score, or for life and health insurance when used for risk assessment and pricing in relation to individuals
- **human oversight** of the AI system must be assigned to a person with the necessary "*competence, training, and authority*"
- if the deployers control input data, ensuring that **the data is relevant and sufficiently representative**
- if a decision generated by the AI system results in legal or similarly significantly effects, the deployer must provide a c**lear and meaningful explanation** of the role of the AI system in the **decision-making process** and the main elements of the decision

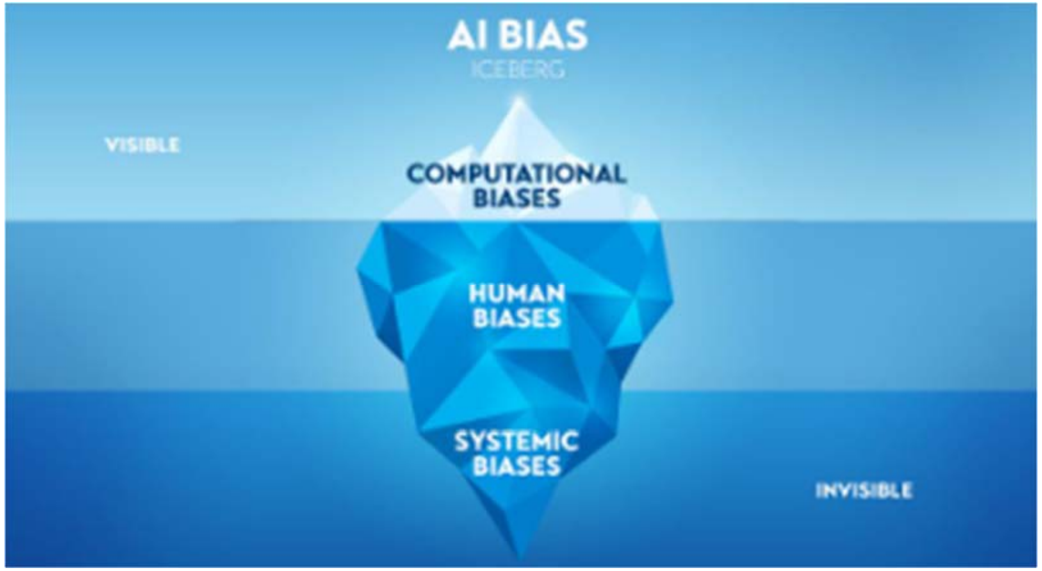
Some privacy considerations when using AI [1]

The key risk areas:

- Accountability & governance
  - DPIAs (use ICO’s ‘AI toolkit’ to identify and mitigate AI risks)
  - Controller(s) v processors
  - Outsourcing / 3rd party AI systems
- Lawfulness, fairness and transparency
  - Development v deployment; Consent v contract v LI; Special category data; A22 automated decision-making
  - Transparency (use ICO’s ‘Explaining decisions with AI’ when explaining AI decisions)
  - Fairness: is it statistically accurate? Does it avoid discrimination? What about reasonable expectations?

Discrimination and bias

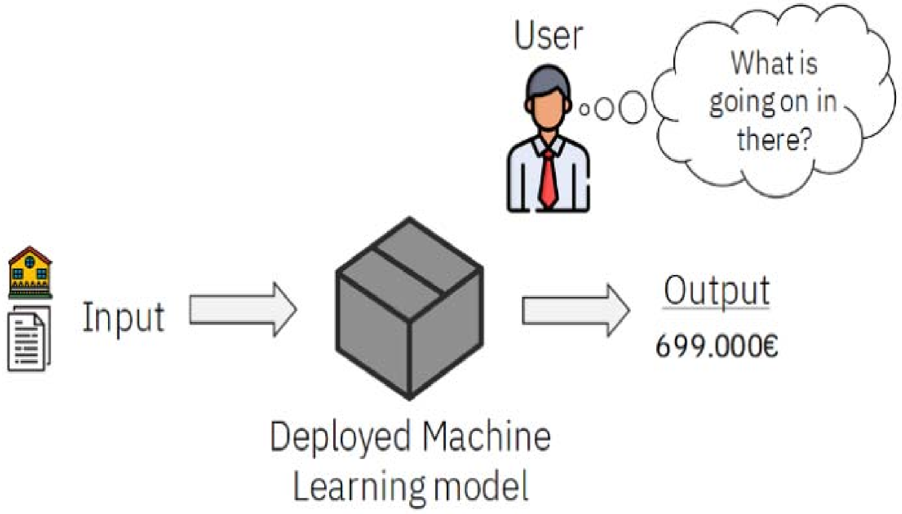
- Biases
  - historical bias
  - sampling bias
  - measurement bias
  - evaluation bias
  - aggregation bias
  - deployment bias
- Equality Act 2010



Some privacy considerations when using AI [2]

The key risk areas (cont'd):

- Ensuring individual rights
  - Information!
  - Human in the loop?
  - Article 22 UK GDPR/GDPR automated decision making
- Security and data minimisation
  - Large volumes of data
  - AI supply chain
  - Privacy attacks
  - PETs



LEWIS SILKIN

Other considerations when using AI

- Web scraping - Joint statement on data scraping and data protection | ICO
- Think about
  - Input data
  - Data licence restrictions
  - What is public data (data mining exemption)
  - Once input data – do you lose rights? (Samsung)
  - Creation of IP rights – can output data even be protected as not created by a human?
    - No in US/ Yes in UK
    - Stable Diffusion v Getty case
- Use of Output data – likely to be determined by terms

Other considerations when using AI

- Ethical/ESG considerations
- Contractual protections
  - Warranties, indemnities, rights of audit, data use restrictions

Health and Safety

- Interaction with health and safety laws
  - Reasonably practicable defence?

- AI used to monitor workplace efficiency and health and safety
  - Hours worked (lorry driving, air traffic control)
  - Correct loading and safety procedures followed (warehouse, logistics)
  - Monitoring and Control of Substances Hazardous to Health (COSHH)
  - Tracking batches of drugs (pharma and healthcare)
  - But a note of caution…
    - CNIL Amazon €32 million fine for "excessive" and "illegal" employee monitoring

© Alex Whittles

What can be done to mitigate against these risks around AI?

INTERNAL POLICIES

SUPPLIER CONTRACTS

AI DUE DILIGENCE

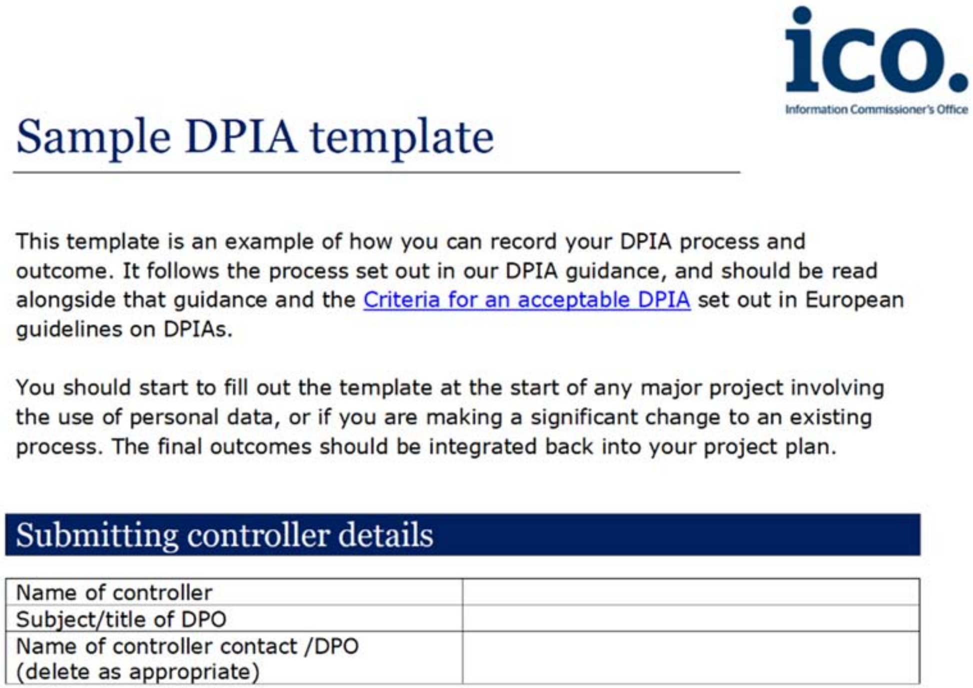
What is a data protection impact assessment (DPIA)?

- *'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'* – Article 35 UK GDPR.
- A DPIA sets out:
  - The reason why personal data is being processed,
  - The risks to data subjects, and
  - The steps being taken to mitigate those risks, to ensure the personal data is being processed as safely as possible.

When will I need a DPIA?

- High risk processing (and all AI projects!)
- Common examples of when a DPIA may be needed include:
  - Implementing a new type of monitoring, whether that is CCTV, covert monitoring, or performance monitoring using new technology,
  - Collecting sensitive types of personal data, e.g. Covid vaccination status, drug/alcohol testing, data for diversity monitoring, or undertaking blanket criminal background checks.
- DPIAs are useful documents to have should a data subject complain – they demonstrate to the ICO that you have considered the processing and taken steps to make it as safe as possible.

How do I do a DPIA?



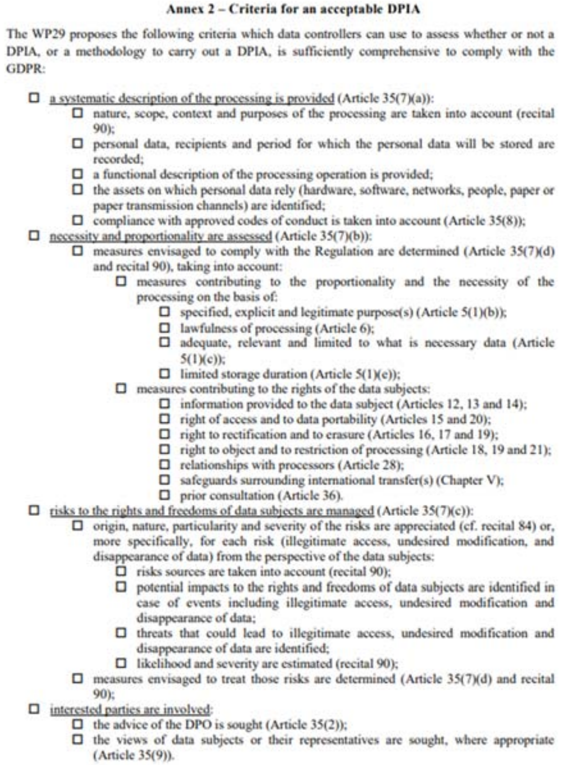
Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

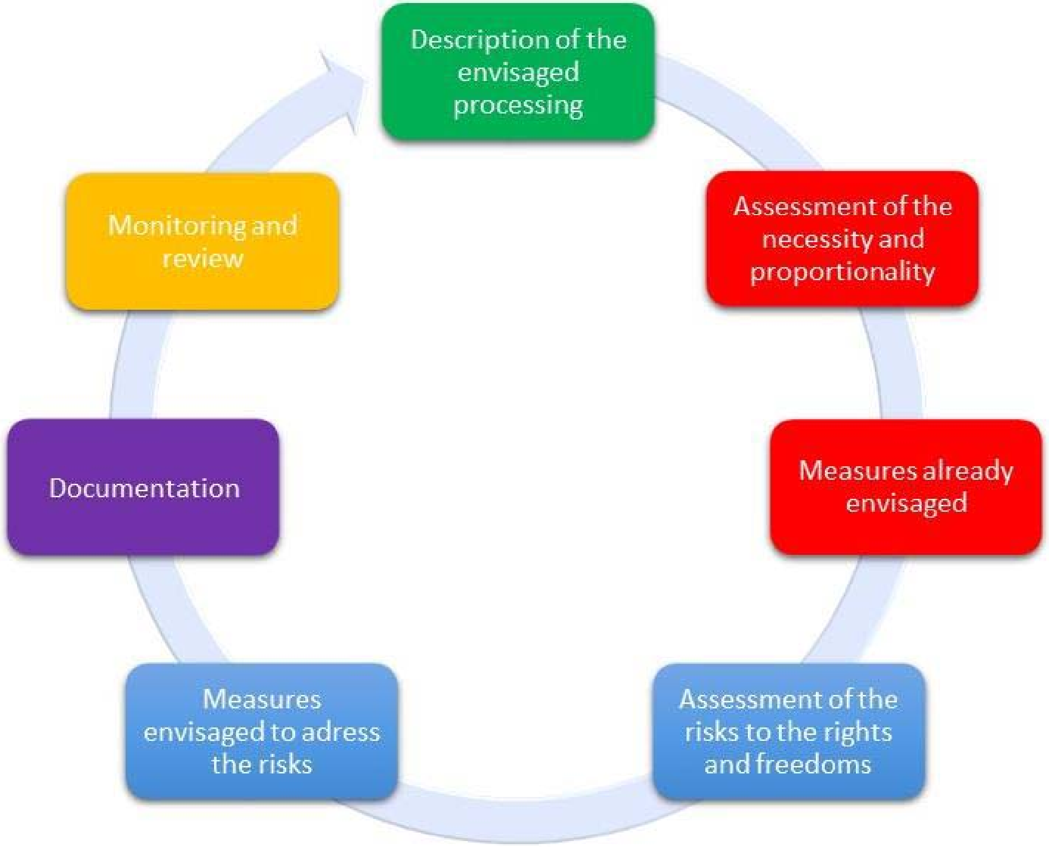


Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- □ a systematic description of the processing is provided (Article 35(7)(a)):
    - □ nature, scope, context and purposes of the processing are taken into account (recital 90);
    - □ personal data, recipients and period for which the personal data will be stored are recorded;
    - □ a functional description of the processing operation is provided;
    - □ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
    - □ compliance with approved codes of conduct is taken into account (Article 35(8));
- □ necessity and proportionality are assessed (Article 35(7)(b)):
    - □ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
        - □ measures contributing to the proportionality and the necessity of the processing on the basis of:
            - □ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
            - □ lawfulness of processing (Article 6);
            - □ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
            - □ limited storage duration (Article 5(1)(e));
        - □ measures contributing to the rights of the data subjects:
            - □ information provided to the data subject (Articles 12, 13 and 14);
            - □ right of access and to data portability (Articles 15 and 20);
            - □ right to rectification and to erasure (Articles 16, 17 and 19);
            - □ right to object and to restriction of processing (Article 18, 19 and 21);
            - □ relationships with processors (Article 28);
            - □ safeguards surrounding international transfer(s) (Chapter V);
            - □ prior consultation (Article 36).
- □ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
    - □ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
        - □ risks sources are taken into account (recital 90);
        - □ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
        - □ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
        - □ likelihood and severity are estimated (recital 90);
    - □ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- □ interested parties are involved:
    - □ the advice of the DPO is sought (Article 35(2));
    - □ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

How do I do a DPIA?



Description of the envisaged processing

Assessment of the necessity and proportionality

Measures already envisaged

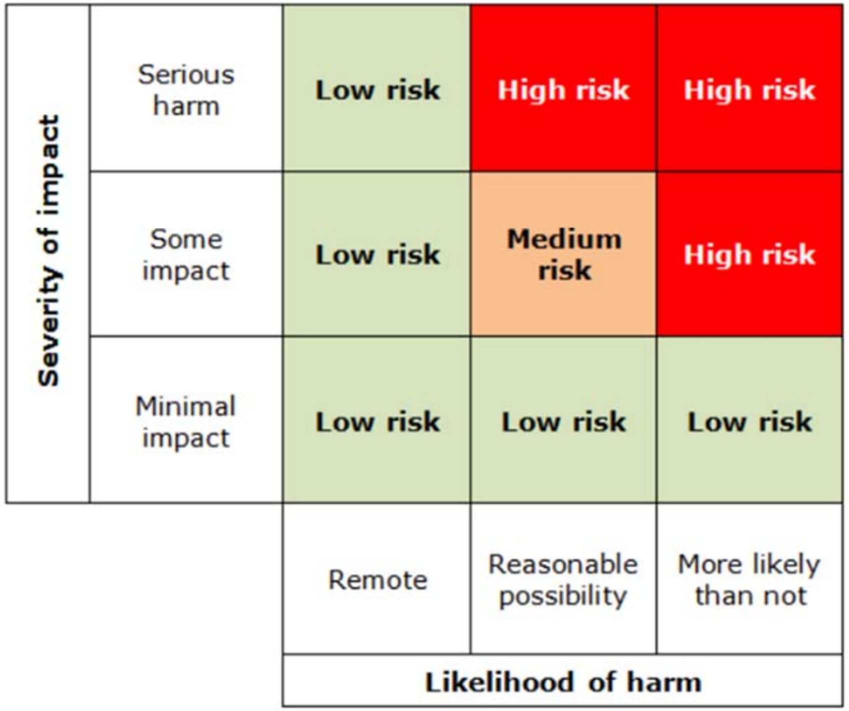
Assessment of the risks to the rights and freedoms

Measures envisaged to adress the risks

Documentation

Monitoring and review

Assess the risk



Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

© ICO How do we do a DPIA?

Mitigate the risks

ICO guidance suggests:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and manage
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- making changes to privacy notices;
- offering individual’s the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

Practical tips for deploying an AI solution

- Define the business need and purpose for such a solution – is it necessary?
- Make sure the legal team is involved from the start
- Consult with stakeholders (inc senior management and data subjects) and assess the impact to them
- Conduct a DPIA and use the AI toolkit to help identify and assess legal risks and mitigations
- If you are procuring AI, do your due diligence
- Ensure decisions made using AI are 'explainable'; i.e.
  1. Be transparent
  2. Be accountable
  3. Consider the context you are operating in
  4. Reflect on the impact of your AI system on individuals affected, and wider society
- Train any humans in the loop!
- Monitor, review and re-assess risk throughout the project lifecycle

AI in the workplace - scenario

- Your HR Ops team come to you saying they have just received a presentation from a vendor about a new monitoring tool.
- This tool is deployed as part of a data loss prevention (DLP) posture and involves continuous monitoring of words in emails via a semantic algorithm.
- The vendor believes this algorithm can identify when an employee is potentially going to compete/resign etc.
- The system would then alert HR, compliance and the relevant line manager.

❖ What are the key concerns here?

LEWIS SILKIN

The Status of Platform Workers Directive

Ideas. People. Possibilities.

EU Platform Worker’s Directive

- Final text adopted on 11 March 2024
- Purpose is to
  - Improve working conditions
  - Regulate the use of algorithms by digital labour platforms
- Stumbling block = workers’ rights (Spain) v business friendly, pro-platform (Sweden, Baltic States)
- Compromise – Member States will decide!

Removing the stumbling block – Employment Status

- Legal presumption the contractual relationship between "*digital labour platform*" and "*platform worker*" = employment relationship
- Presumption triggered when facts indicating "*control*" and "*direction*" are found
- Member States can use national tests and collective agreements, while "*taking into account EU caselaw*"
- Persons working in digital platforms, their representatives or national authorities may invoke legal presumption and claim they are misclassified
- Burden of proof falls on digital platform to prove there is no employment relationship
- Watch this space…guidance to follow!

Regulate the use of algorithms by digital labour platforms

- Transparency - workers must be duly informed about the use of automated monitoring and decision-making systems regarding
  - recruitment
  - working conditions
  - earnings etc.
- DPIA required and must be provided to worker representations
- Prohibition - bans use of automated monitoring or decision-making systems for the processing of certain types of personal data, e.g.
  - biometric data
  - emotional or psychological state of persons performing platform work
- Human in the loop - human oversight and evaluation are guaranteed as regards automated decisions
- Contestability - right to have those decisions explained and reviewed

LEWIS SILKIN

Find out more

Sign up for our data, privacy & cyber blog here

For our monthly newsletter and our In House Data Club invitations please contact our Events Team at events@lewissilkin.com

linkedin.com/company/lewis-silkin

x.com/lewissilkin

lewissilkin.com