

Large, overlapping circular shapes in shades of orange, blue, and green on the left side of the slide.

10 Steps towards AI Compliance

10 steps towards AI compliance: A practical guide for recruitment businesses

What's covered in APSCo's '10 steps towards AI compliance' and why you need it:

Using AI for innovation and process efficiency

Efficiency and innovation aren't just goals, they're necessities. That's why recruitment companies are turning to AI to revolutionise operations. AI offers unparalleled opportunities for automating tasks, enhancing decision-making and providing insightful analytics.

If you don't embrace AI, you may be left behind

The rapid adoption of AI is a clear signal: if you're hesitant to integrate AI into your processes, you risk falling behind competitors who leverage it to optimise their services and outreach.

AI is an asset when used compliantly

While AI can significantly enhance operational efficiencies and service offerings, its true value is realised when it's used within a compliance framework. Adherence to legal and ethical standards both safeguards your business and enhances your reputation.

The challenges and risks of AI need due attention

Implementing AI isn't without challenges and risks, particularly concerning data protection, privacy and ethical considerations. Recruitment companies must navigate these complexities to ensure your AI solutions don't inadvertently violate regulations or ethical norms.

Manage data protection when implementing AI solutions

APSCo's 10-step guide to AI compliance is designed to assist recruitment organisations in managing data protection risks. It offers a clear, actionable framework you can follow to ensure your AI implementations are both effective and compliant.

Be confident you're utilising AI compliantly

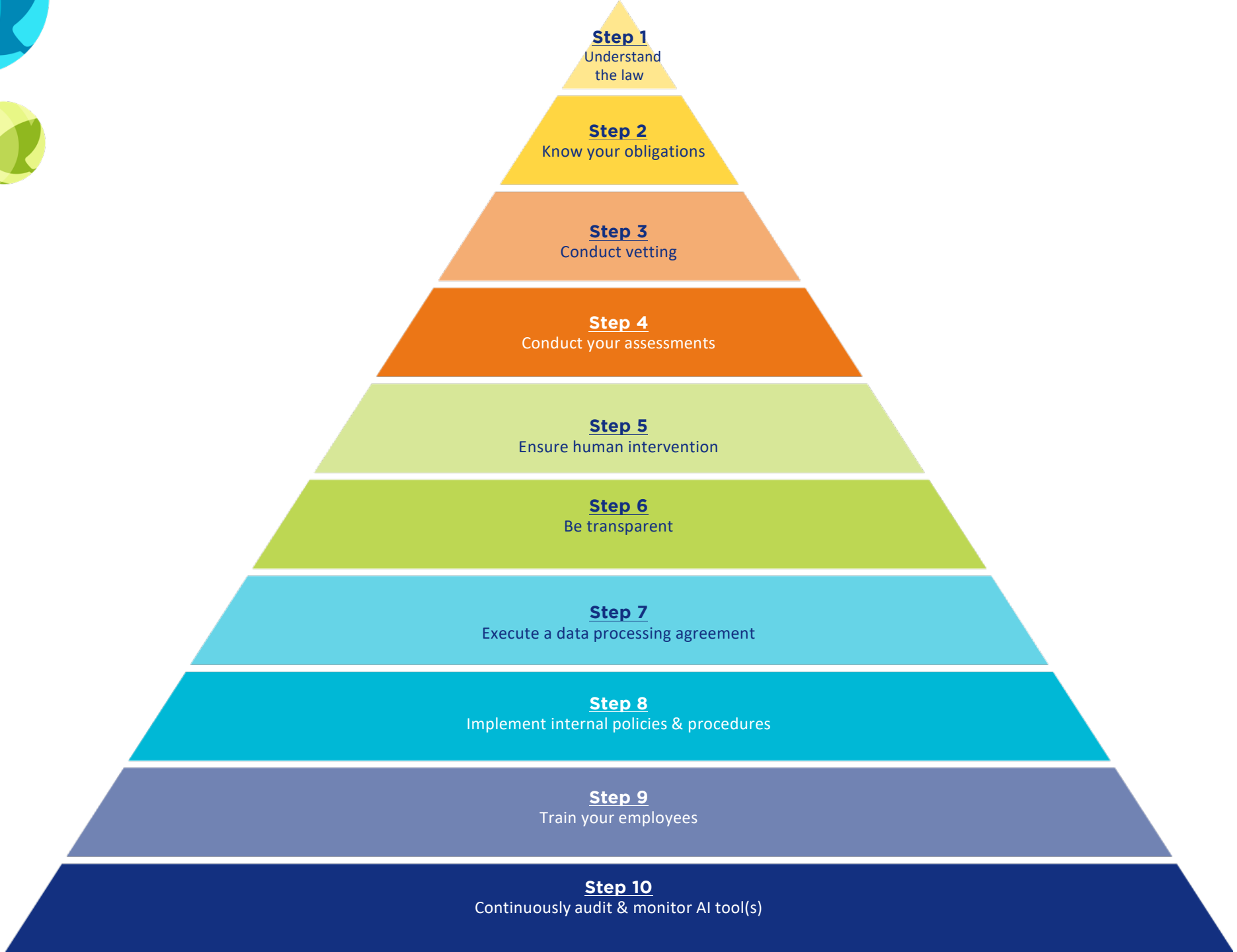
This guide provides detailed steps and tips, from understanding legal obligations to implementing robust vetting and assessment processes. Leverage AI's full potential without worrying about compliance breaches.


Understand key data protection considerations

By providing essential data protection considerations, you'll be well-informed about your responsibilities, the importance of transparency and the necessity of securing explicit data processing agreements.

Outlines checks and balances

With practical checklists and guidance, our 10-step guide outlines essential checks and balances, such as audits, training and internal policies. These measures are crucial for ongoing compliance and the ethical use of AI tools in recruitment processes.





“The world is one
big data problem.”

Andrew McAfee

“I’m increasingly inclined
to think there should be
some regulatory oversight,
maybe at the national and
international level just to
make sure that we don’t
do something very foolish.”

Elon Musk

“What all of us have to do
is make sure we are using
AI in a way that is for the
benefit of humanity, not to
the detriment of humanity.”

Tim Cook

“Just as electricity transformed
almost everything 100 years
ago, today I actually have
a hard time thinking of an
industry that I don’t think
AI will transform in the next
several years.”

Andrew NG

Step 1: Understand the law

The Law in the UK

The Law

There is currently no specific AI law in the UK.

However, in some respect existing data protection laws cover the use of AI when applied to employment ([Data Protection Act 2018](#) and [UK GDPR](#)).

As businesses will be processing personal data through their AI tools, they will need to comply with the [7 Principles of UK GDPR](#) under [Article 5](#):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage Limitation;
- Integrity and confidentiality (security); and
- Accountability.

Failing to comply with the 7 principles listed above would result in substantial fines, as [Article 83\(5\) of UK GDPR](#) classifies them in the highest tier of administrative fines: £17.5 million or 4% the businesses' total worldwide annual turnover, whichever is higher.

To comply with these principles, businesses should have a privacy notice in place and update it to include AI systems when needed.

Privacy Notice

Articles [12](#), [13](#) and [14](#) of the UK GDPR provide detailed instructions on how to create a privacy notice.

The privacy notice should include:

- Name and contact details of your organisation;
- Name and contact details of your representative, if any;
- Contact details of your data protection officer, if any;
- Purposes of the processing;
- Lawful basis for the processing;
- Legitimate interests for the processing, if applicable;
- Recipients, or categories of recipients of the personal data, if applicable;
- Details of transfers of the personal data to any third countries or international organisations, if applicable;
- Retention periods for the personal data;
- Rights available to individuals in respect of the processing;
- Right to withdraw consent, if applicable;
- Right to lodge a complaint with a supervisory authority;
- Details of whether individuals are under a statutory or contractual obligation to provide the personal data, if applicable; and
- Details of the existence of automated decision making, including profiling if applicable.

Privacy Notice Cont.

Businesses should review their privacy notice and privacy policy before using any AI tools and ensure that the privacy notice provides enough information to the individuals, such as:

- Being subject to AI tools and monitoring;
- Identifying the tools being used and their purpose; and
- Informing them about their right to object to solely automated decision making.

We have a [Privacy Notice template](#) available on our website and the ICO also have [guidance](#) and a [Privacy Notice template](#) available.

Regulatory Body

The [Information Commissioner's Office \(ICO\)](#) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It is an executive non-departmental public body, sponsored by the [Department for Science, Innovation and Technology](#).

The White Paper

In March 2023, the Government issued a [White Paper](#) on AI called "A pro-innovation approach", which details their plans for implementing a pro-innovation approach to AI regulation.

The White Paper identified 5 main principles:

- Safety, security and robustness;
- Appropriate transparency and explainability;
- Fairness;
- Accountability and governance; and
- Contestability and redress.

Further information on these principles can be found in [Annex A](#) of the White Paper.

It is important to note that the White Paper cannot be seen as a set of regulations, but simply as the Government's approach to regulating AI development and use.

The White Paper's 5 main principles echo those identified by other countries.

Practical Steps

Businesses should periodically review the law and regulations to ensure they keep abreast of any news and adapt their policies and processes accordingly.

The 5 principles covered by the White Paper should be followed.



The Equality Act 2010

Individuals are protected from discrimination under the [Equality Act 2010 \(EqA 2010\)](#), including any discrimination caused by the use of automated AI tools.

The private lives of individuals are also protected under this Act. Consequently, employers must consider the limit of the use of their AI tools when monitoring their employees.

When using an AI tool to assist in the recruitment process or the monitoring of its employees, businesses should ensure the tool is free of bias and discrimination in its decision making.

What are the main risks of using AI tools with regard to the EqA 2010?

There are 3 main risks to consider under the Equality Act 2010:

- **Fairness:** under the EqA 2010, employers are responsible for making reasonable adjustments if they are putting disabled people at a particular disadvantage. This extends to the systems used by employers.
- **Bias:** although AI systems are not human and are by extension free of all emotion, they have been created by humans and can reflect the same bias as their creator. It has been shown that some systems reproduced bias based on sex, ethnicity and disability due to how the system was trained and what information it was fed with.
- **Discrimination:** some systems can help businesses predict what would be the best relevant candidate for a specific role. However, depending on how the system calculates the outcome, it might advantage certain group of the population over others. Candidates with gaps in their CV might be less likely to be selected or ignored by the tool.

How to protect against discrimination when using AI tools

In a recruitment process which does not involve AI, it is easy to spot potential discrimination. However, when using AI in a fully automated process, potential discrimination can be less visible.

It is therefore important for businesses to conduct assessments before using AI, to ensure the AI tool is not biased and is accessible to anyone:

- **Equality Impact Assessment (EIA):** an EIA is an evidence-based approach which ensures that policies and processes are fair and free of any discrimination risks.
- **Algorithmic Impact Assessment (AIA):** an AIA will assess the data used to train the AI tool. Although an AIA does not solely assess discrimination in AI tools, this assessment will assist businesses in spotting potential bias and indirect discrimination.

Practical Steps

Businesses should complete an Equality Impact Assessment and an Algorithmic Impact Assessment to ensure the AI tool is not biased and does not risk potential discrimination.

Businesses can learn more about Equality Impact Assessments and Algorithmic Impact Assessments at [Step 4 “Conduct Impact Assessments”](#) below.

A specific process for individuals with disabilities should be in place to guarantee they have the same chances as any other candidates.

Outcomes provided by AI tools should be regularly checked to spot potential discrimination in the process and employees should be trained to recognise them.

It may be appropriate to stop using the tool to reduce the risk of discrimination when an issue has been raised. For instance, when an individual does not have access to the appropriate technology or when the individual cannot access the tool due to a disability.

The EU Artificial Intelligence Act

What is the EU AI Act?

It is important to note that although the UK does not have any AI Regulations as of yet, Europe has published the [EU Artificial Intelligence Act \(EU AI Act\)](#).

The EU AI Act adopts a risk-based approach and qualifies the use of AI tools in the Employment process as high- risk.

Under the Act, [high risk AI systems](#) must comply with the following requirements:

- Risk management system: processes should be put in place to evaluate and identify potential risks of using AI tools.
- Data and data governance: training, validation and testing data sets must be subject to appropriate data governance and management practices.
- Technical documentation: documentation must be drawn up by the AI tool provider confirming it complies with the EU AI Act obligations.
- Record-keeping: the system should record any decisions and keep a log of issues that arise.
- Transparency and provision of information to users: people must be informed they are subject to an AI tool to allow them to make informed decisions.
- Human oversight: to minimise the risk of bias and discrimination and to allow risk management.
- Accuracy, robustness and cybersecurity: AI systems should be robust and secure to ensure accuracy and prevent misuse.

As the UK is no longer a part of the EU, does this Act impact the UK?

Whilst the EU AI Act will not directly govern data subjects in the UK, UK businesses should comply with the EU AI Act when using AI Tools where the output of the tool is to be used in the EU and/or the data subject is based in the EU.

This is covered under [Title 1: Article 2 of the EU AI Act](#).

The Act

On 13 March 2024, the EU Parliament approved the EU AI Act.

The EU AI Act is now awaiting formal endorsement by the EU Council.

Once approved, it will enter into force 20 days after its publication in the Official Journal and will be fully applicable 36 months thereafter.

Certain provisions however, will apply earlier, such as:

- Bans on prohibited practices which will take effect six months after entry into force,
- GPAI rules will take effect 12 months after entry into force

Businesses should keep abreast of any changes that may be implemented.

The EU AI Act can be found [here](#).



Regulatory Body

Four new administrations will be created:

- [An AI Office](#): which will sit within the Commission and will monitor general-purpose AI systems (GPAIs);
- A scientific panel of independent experts: they will advise the AI Office about GPAI models and will monitor material safety risks;
- [An AI Board](#): which will include all EU member States' representatives and will assist in the implementation of the EU AI Act; and
- [An Advisory Forum](#): which will include a diverse panel of stakeholders, providing technical expertise to the AI Board.

It is important to know that each State Member will also decide what their own Local Authority will be.

Practical Steps

Keep abreast of development in the EU AI Act.

Ensure to regularly check the [Official Journal website](#) for the EU AI Act publication.

Identify your EU clients, candidates, suppliers and ensure compliant processes are in place regarding the use of AI.



Step 2: Know your obligations

Key Considerations

AI Tools

Consider the AI tools the business is going to use:

- What is the purpose of the tool? (sourcing tool/ scrapping tool/ online advertising...)
- What personal data will the AI tool be processing and why?
- What is the output of the AI tool you are seeking?
- Will the AI tool be reviewed?

It is important to clearly assess the need for an AI tool to distinctly identify the value the business is going to get from the tool to then be able to compare it to the potential risks attached to it. “Is the value worth the risk?” should be your motto.

Consider the impact of data protection laws when using the AI tool ([UK GDPR and the DPA 2018](#)).

Businesses must ensure they have taken into account the key considerations highlighted by the White Paper and have understood the risks and practical approaches they may need to consider.

[Guidance](#) aimed at employers and recruiters has been issued by the ICO to help them understand their obligations and how to comply.

Transparency & Explainability

Across all international guidance, Transparency is a key consideration when using AI.

The White Paper states: “Transparency refers to the communication of appropriate information about an AI system to relevant people (for example, information on how, when, and for which purposes an AI system is being used).”

Practical Steps

Businesses must inform the data subject that they are using AI tools and businesses must be transparent with them as this will allow the data subject to make informed choices or step back from being subject to the tool.

Read the ICO guidance on [Transparency](#) and on how to [explain the use of AI](#) within your business and externally.

Accountability & Governance

The White Paper addresses the accountability of AI tool providers and users for future regulations.

It is important for anyone using AI tools to be able to limit their responsibility by identifying and mitigating risks.

Practical Steps

Refer to the [Step 3 “Conduct vetting”](#) for more information on how to achieve this.

Safety, Security & Robustness

The AI tool should be resistant against risks connected to safety concerns (e.g. errors, faults, inconsistencies, unexpected situations) or reproduction of bias.

The tool should also be resistant to malicious action that may compromise the security of the AI system.

Practical Steps

Ensure that the AI tool provider has put in place appropriate cybersecurity measures to avoid the tool being misused or compromised and to protect against potential data breaches and corruption of the system. The AI tool provider should be asked for a security report for the tool.

Contestability & Redress

Using AI can result in different types of risks and concerns (errors, bias etc).

Practical Steps

Businesses should have processes in place allowing Individuals to contest decisions where their rights have been violated or they have been harmed.

Accuracy

AI accuracy is the degree to which an AI system produces correct outputs or predictions based on the given input or data.

The AI tools should be consistent throughout their lifecycle and meet an appropriate level of accuracy.

Practical Steps

The AI tool provider should supply businesses with the accuracy metrics.

Copyright & Confidentiality Infringement

Some AI tools may infringe confidentiality and copyright by generating outputs that resemble existing work. This is a particular risk for Generative AI, such as Chat GPT.

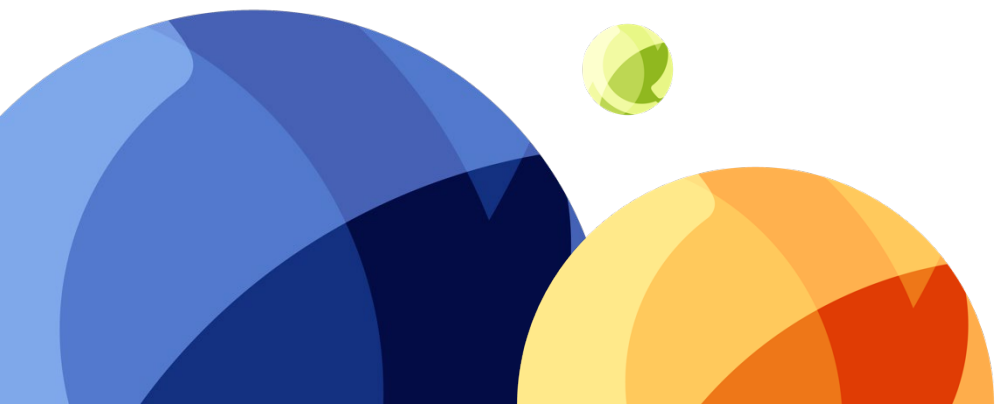
Practical Steps

Businesses should consider this before making use of the tool and read the Terms and Conditions of the tool.

Fairness

As defined in the White Paper, AI should not undermine the legal rights of individuals or organisations, discriminate unfairly against individuals, or create unfair market outcomes.

Businesses should have processes in place to ensure that AI tools are not subject to bias by requiring reports from the AI tool provider, conducting assessments, training the employees who will be using the tool, and allowing reviews of outcomes provided by the AI tool.



Step 3: Conduct vetting

Vet your AI Tool Provider

Both the [White Paper](#) and the [EU AI Act](#) place the responsibility on the businesses using AI tools to vet the AI tool provider before using the tool.

The AI tool provider as the developer of the tool, should be aware of the potential flaws, errors and bias of the tool and notify businesses of this risks.

Businesses should also be aware of their responsibilities when developing their own AI tools.

Practical Steps

Businesses should ensure compliance with the applicable laws and regulations.

[Article 2](#) of the EU AI Act for example makes it clear that any UK AI tool provider should comply with the EU AI Act if the individual subject to the tool resides in the EU. This means that by extension, any businesses who use an AI tool on an individual must comply with these rules.

Check for recognised certifications such as [ISO/IEC 23895:2023](#), which provides guidance on managing risks specifically related to AI and [ISO/IEC 42001:2023](#), which is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving AI Management Systems.

Vet the Tool

Once businesses have vetted the AI provider, it is time to vet the tool itself.

The vetting of the tool can take many forms and will most likely need to be assessed on a case-by-case basis. Below are some of the most common checks businesses would be expected to conduct:

- What is the purpose of the tool? (sourcing tool/scraping tool/online advertising)
- What personal data will the AI tool be processing and why?
- How long has the tool been in use (if applicable)?
- What do the error reports show?
- What do the security reports show?
- Is the tool accessible to any individual (does the tool consider disabilities, age gaps, language barriers etc?)

Practical Steps

Businesses should address the questions above and the questions set out in the ICO [guidance](#) on AI and data protection with their AI tool provider. Obtain reports from the AI tool provider. AI tool providers should have strong processes in place to identify issues, errors, and bias. AI tool providers should also have a full report available on how the tool was trained (the data used to train the tool and the process under which the AI tool arrives to a conclusion).

Business should obtain confirmation from the AI tool provider that the tool does not infringe any data protection laws and regulations.

Test the tool with hypothetical candidates to check the relevance of the outcome provided and identify any bias or potential access risks for disabled people.

For businesses developing an AI Tool, consider the Department for Science, Innovation and Technology (DSIT) [guidance](#) on AI assurance techniques.

Step 4: Conduct your assessments

Data Protection Impact Assessment (DPIA) & AI Data Protection Risk Assessment (DPRA)

Each AI system is different and will present different levels of data protection risks. DPIAs should be carried out for each of them and revisited on a regular basis throughout the lifetime of the AI system as the risks to data protection may evolve over time. DPIAs are required under [Article 35\(3\)\(a\) of the UK GDPR](#) if the business' AI tool involves:

- Systematic and extensive evaluation of personal aspects based on automated processing, including profiling, on which decisions are made that produce legal or similar effects; or
- Large-scale processing of special categories of data, such as health or genetic data.

The DPIA will:

- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals including risks of bias and discrimination; and
- Identify any additional measures to mitigate those risks before the introduction of any AI.

APSCo templates and guidance on DPIA can be accessed [here](#).

Additionally, businesses should conduct a DPRA to understand and assess some of the AI-specific risks to individual rights and freedoms, and how to mitigate, reduce or manage them.

The ICO have DPRA [guidance](#) and [templates](#).

Identify a Lawful Basis for Processing

Consider the 6 lawful bases for processing:

Under [Article 6 of the UK GDPR](#), businesses can only process the individual's personal data under:

- Consent;
- Contract;
- Legal obligation;
- Vital interests;
- Public task; or
- Legitimate interests.

Businesses can find more guidance on the lawful basis for processing [here](#).

Legitimate interests are usually the most flexible lawful basis for processing in the recruitment industry, however businesses cannot always assume it is appropriate when using AI tools.

Before using any AI tools, businesses wishing to rely on legitimate interests as their lawful basis for processing data, should apply the ICO's Legitimate Interest Assessment (LIA) three-part test:

- Identify a legitimate interest (the 'purpose test');
- Show that the processing is necessary to achieve it (the 'necessity test'); and
- Balance it against the individual's interests, rights and freedoms (the 'balancing test').

More detail on each part of the test can be accessed through the ICO's [LIA guidance](#).

The LIA does not have to take any specific form, although it is recommended to use the [ICO template](#) to keep a paper trail of the tests.

Algorithmic Impact Assessment

An Algorithmic Impact Assessment (AIA) mitigates the risks associated with the use of an automated decision system.

The AIA focuses on:

- Understanding the risks attached to the use of Algorithmic systems;
- The commitments the business should make;
- Identifying the individuals impacted;
- Undertaking an ex-ante risk and Impact analysis;
- Taking appropriate action following the analysis; and
- Evaluating to ensure assessment and appropriate action have been put in place.

As AIAs are derived from DPIAs, and to avoid businesses being overwhelmed with assessments, businesses can instead amend their DPIA to include the relevant assessment for Algorithmic Impact.

Further [guidance](#) has been provided by the Institute for the [Future of Work \(IFW\)](#), an independent research and development institute exploring how new technologies are transforming work and working lives.

Equality Impact Assessment

An Equality Impact Assessment (EIA) is an assessment carried out by businesses to ensure that the policies, practices, services and decisions taken are fair and do not discriminate against any one group of individuals.

Considering the impacts AI tools may have on decision making and their potential for errors, misuse, and bias. It is important for businesses to conduct such assessments prior to using the tool.

Trained employees on diversity & inclusion should assist in conducting the assessment and the EIA must be made fully available to whoever requests it.

The UK Research and innovation (UKRI) provides an [Equality Impact Assessment Guidance and template](#) businesses can use.

Practical Steps

Each of these assessments should be carefully considered and carried out.

When a business does not see the need of conducting these assessments, they should document why.

Step 5: Ensure human intervention

Human Oversight (Article 14 EU AI Act)

[Title 3: Article 14 of the EU AI Act](#) defines Human Oversight as the means by which an AI tool can be effectively overseen by natural persons during the period it is in use. Human Oversight aims to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used.

The individual in charge of overseeing the AI tool should:

- Fully understand the capacities and limitations of the AI system to monitor its operation;
- Remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias);
- Be able to correctly interpret the high-risk AI system's output;
- Be able to decide on a particular occasion, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;
- Be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

Businesses should ensure the individual is trained to carry out this task.

Will the AI System be Solely Automated?

[Chapter 3: Article 22\(1\) of the UK GDPR](#) states:

"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her."

Solely Automated can be defined as a decision-making process that is totally automated and excludes any human influence on the outcome. It would still be considered automated, even with the human inputs of data if the system carries the decision-making.

Businesses can only carry out this type of processing if they are able to rely on one of the three exceptions set out in [Article 22\(2\)](#):

- When the decision is necessary for a contract;
- When the decision is authorised by law; or
- When the decision is based on the individual's explicit consent.

The ICO has issued some guidance on Solely Automated systems in the recruitment process which you can access [here](#).

Practical Steps

Businesses should consider partially automated systems, which could include human intervention.

This could for example be the case where the system pre-selects candidates for a role, but only the business can manually assess each pre-selected candidate and move them to the next stage of the recruitment process.

If businesses wish to rely on fully automated systems, it is important for businesses to ensure the AI tool and processing data is in line with [Article 22 of the UK GDPR](#).

Step 6: Be transparent

Communicate

Communication is key to ensure an appropriate use of AI whether internally or externally.

Businesses should ensure that each employee using or overseeing the AI tool has been appropriately trained, including to report any misuse or errors by the system. Businesses wishing to use AI tools to manage their employees (see [Monitoring your employees at work](#) below), should ensure their employees have been informed of their rights.

Businesses should ensure appropriate transparency and explainability is provided to individuals that are subject to the AI tool.

Contestability & Redress

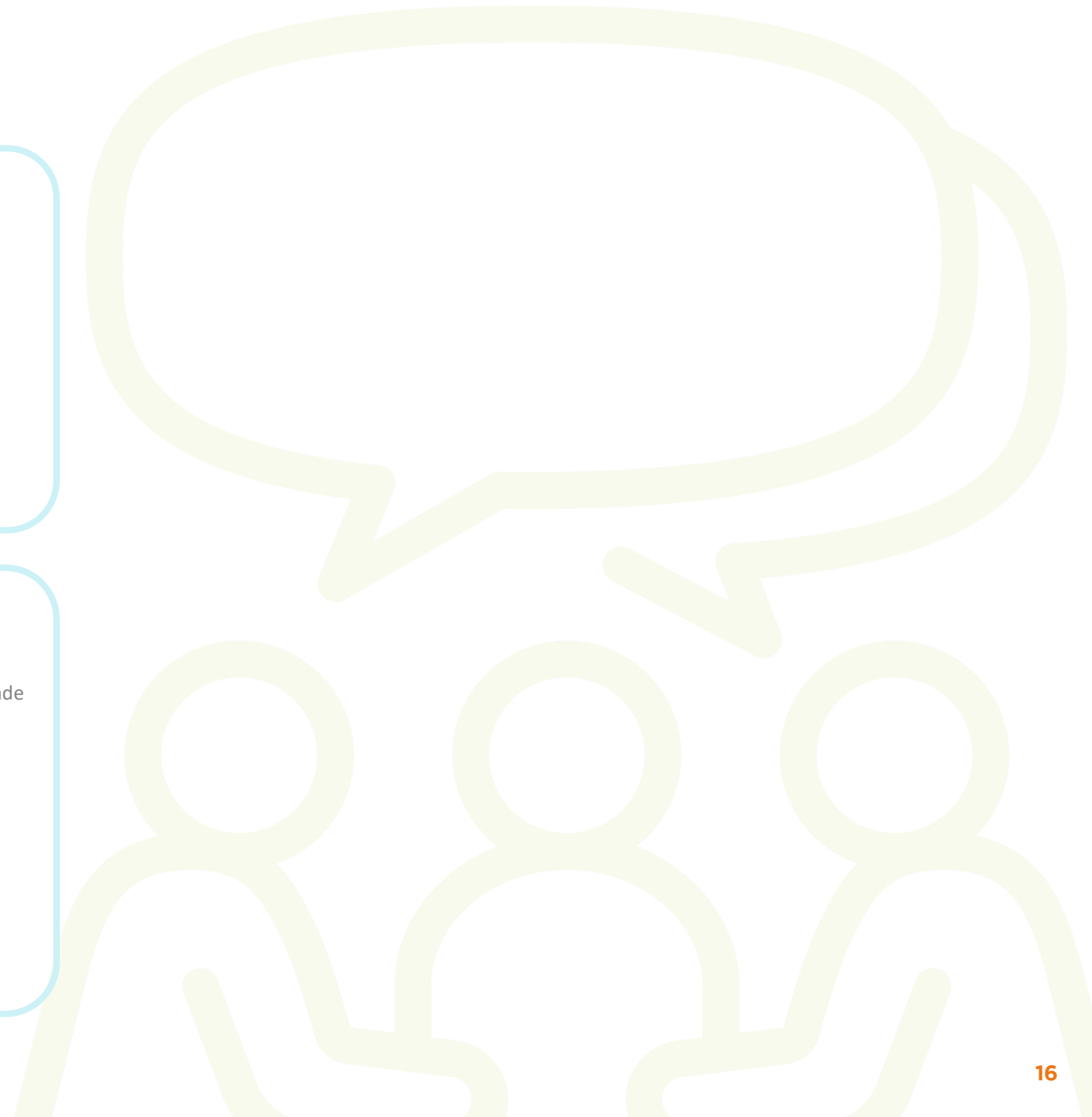
As specified in the [White Paper](#), and in order for individual to exercise their rights under Data Protection laws and the Equality Act 2010, businesses will be expected to have policies and processes in place for individuals to challenge the decisions made by the AI tool.

Individuals subject to AI tools should be able to report and contest potential malfunctions, bugs and bias resulting from the tool.

Businesses are recommended to put in place a feedback and contest process.

Running tests before the use of the tool and during its use as set out at [Step 10 “Continuously audit and monitor AI tool\(s\)”](#) should also assist in preventing such issues.

Obtaining Reports from the AI developer will also assist towards preventing bias and errors.



Step 7: Execute a data processing agreement (DPA)

Under Article 28(3), the UK GDPR requires data controllers and data processors to enter into a contract

“Processing by a processor shall be governed by a contract or other legal act under domestic law, that is binding on the processor with regard to the controller...”

To comply with this obligation, businesses should consider whether a separate Data Processing Agreement (DPA) is required to ensure that the AI tool provider and its tool are complying with all relevant data protection laws and regulations.

What should be included in the Data Processing Agreement?

[Article 28\(3\) UK GDPR](#) states that the following 8 provisions must be present in a business' contract as a minimum:

- Processing only on the documented instruction of the controller (Article 28(3)a): under which a data processor can only process the data in accordance with the data controller's instructions.
- Duty of confidence (Article 28(3)b): under which the data processor is bound by to keep the data it processes confidential.
- Appropriate security measures (Article 28(3)c): under which the data processor must take all measures necessary when processing the data.
- Using sub-processors (Article 28(3)d): under which the processor cannot sub-contract the processing of data to a third party without the prior consent of the data controller.
- Data subject's rights (Article 28(3)e): under which the data processor is required to put in place measures allowing data subjects to exercise their rights.
- Assisting the controller (Article 28(3)f): under which the data processor must assist the controller in meeting its obligations.
- End-of contract provisions (Article 28(3)g): under which the contract must state that, at the end of the contract, the data processor will destroy all the personal data the data processor has been processing.
- Audits and inspections (Article 28(3)h): under which the data processor must provide all information relevant for Article 28(3) and allow the data controller to conduct audits showing compliance with this article.



Practical Steps

A specific DPA should be entered into between the business and the AI tool provider to ensure that all UK GDPR obligations are met by the AI tool provider when processing the data submitted to the tool, standard contractual clauses can also be used.

Standard contractual clauses may provide simple solutions to ensure that the AI tool provider and the way the tool processes data complies with data protection laws. Due to the nature of AI, and the risks associated with such tools, it may be advisable to get in touch with a lawyer who specialises in Data Protection law to assist businesses in the drafting and negotiating such clauses, or to assist them in building a Data Processing Agreement.

Should businesses require legal assistance, a list of APSCo's Legal Trusted Partners can be accessed [here](#).

The ICO has further guidance available on DPAs which you can access [here](#).

Step 8: Implement internal policies & procedures

Appropriate policies and procedures should be put in place to safeguard individuals subject to AI tools.

Policies

Businesses should ensure policies are in place to control the use of AI tools within their business, and to comply with the [White Paper](#) principles which aim to safeguard individuals.

Businesses should create a policy that:

- Restricts the use of AI tools to only the AI tools vetted and approved by the business;
- Provides employees with an understanding of their role when using these tools;
- Explains how the tool operates;
- Describes what and how data will be collected;
- States if the tool is automated and what part of the automation is submitted to human input; and
- Explains what the contest processes are for employees and individuals.

The appropriate stakeholders should be consulted to assist on the drafting of the policy such as a Data Protection Officer, and your business' IT, legal and HR departments.

Alternatively, a lawyer specialising in GDPR should be consulted. You can access APSCO's Legal Trusted Partners list [here](#).

Procedures

To comply with their obligations and responsibilities, businesses should ensure processes are in place before using AI tools.

Such processes should include:

- A vetting process (auditing and testing the tool before it is used (DPIA, AIA, EIA and LIA) – Please see [Step 4 “Conduct your Assessments”](#);
- Monitoring and reporting on the use of the tool and potential errors and misuses – Please see [Step 10 “Continuously Audit and Monitor AI Tool\(s\)”](#); and
- Contest and redress (responding to contest of individuals subject to the tools) – Please see [Step 6 “Be Transparent”](#).

If businesses have a Data Protection Officer, they should be involved in the end-to-end process and undertake the latest AI training.

Ideally, all parts of the business who will be using the AI tool or will interact with individuals subject to the tool should be trained on the process.

“By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.”

Eliezer Yudkowsky

Step 9: Train your employees

When it comes to IT systems and cybersecurity, it is often said that employees are the first line of defence. This is also true when using AI tools.

As the employees will be the ones in direct contact with the AI tools, interacting with them on a daily basis, it is crucial that they are trained to prevent any misuse but also to spot any potential risks.

Who should receive AI Training?

- Anyone involved in the selection and vetting process of the tools must be trained to understand the potential risks for the business to use or develop such tools. They should have knowledge to help them navigate Data Protection Law and Discrimination Law, and how to comply with them.
- Any employee using the AI tools. As these employees will most likely be interacting with the tools the most or providing human intervention, they should be trained to identify misuse, bias and discrimination in the recruitment process.

Practical Steps

Training should be tailored for each of the AI tools being used by the business. Although the compliance part of the training is likely to be similar between AI tools, the way the tools will be used and how employees interact with them might differ. It is important for businesses to identify the training needs of their employees, before and during the use of the tools.

The AI tool provider may have training material and documentation at hand to assist the business. Alternatively businesses can also consider getting AI training providers.

Step 10: Continuously audit & monitor AI tool(s)

Auditing & Monitoring

As explained earlier, [Robustness, Accuracy and Security](#) are three of the main considerations when using AI.

The [EU AI Act](#) and the [White Paper](#) both emphasise the responsibility of the developers and users of these systems.

Businesses should ensure they periodically conduct tests and monitor the results of the AI tools they use prior to using the tools and also during their use:

- Prior to the first use of an AI tool, businesses should test the tool with data previously used to see if the tool provides the same outcome.
- During the use of the AI tool, businesses should conduct similar test(s) and require reports from the AI tool developers to ensure the outcomes are not provided with errors and there is no bias.

Record-Keeping

In order to show to the relevant authority that businesses have complied with their legal obligations, it may be useful to keep a record of their use of AI tools and their compliance with all obligations.

The [EU AI Act](#), which covers record-keeping, suggests that such record-keeping should, at a minimum, provide:

- A data log of each use of the AI tool such as start and end date and time for each use;
- The reference database against which input data has been checked by the system;
- The input data for which the search has led to a match; and
- The identification of the employee involved in the verification of the outcome.

Practical Steps

Businesses should ensure they can justify each of the outcomes provided by the AI tool.

Obtain regular reports from the AI tool developer and provider, identifying the AI tools errors, misuses and any identified bias.

AI when Monitoring your Employees at Work

Key Considerations

The White Paper does not differentiate between external individuals subject to AI tools and employees of businesses who are using them. Neither does it make a distinction between the purpose and use of the AI tools.

Therefore, employers should follow the same considerations highlighted by the [White Paper](#):

- **Human Intervention:** decisions provided by AI tools in the recruitment process, any decision taken by the AI tools to assist management of the workforce should require a human intervention to confirm that decision.
- **Transparency:** workers must be informed they are subject to AI tools. Put in place an AI policy at work that would cover the use of AI tools for tasks allocation and performance management.
- **Fairness:** AI should not undermine the legal rights of employees and unfairly discriminate against them.
- **Contestability and Redress:** each employee must have the right to contest a decision issued by the AI tool and employers should consider and investigate each employee's request.
- **Safety, Security and Robustness:** the same types of safety and security should be expected for an AI tool used for the business' employees as it would for an AI tool used.
- **Accountability and Governance:** the White Paper addresses the accountability of AI tool providers and users for future regulations.

It is important for anyone using AI tools to be able to limit their responsibility by identifying and mitigating risks.

Practical Steps

AI tools should not be used to replace human interaction but should be used to assist them in their tasks.

Follow the practical steps below to ensure the use of the tool is not infringing any of your employees' rights:

- Think about the goal you want to achieve and what the different ways are to achieve it. Is the AI tool really necessary?
- What type of data will the AI tool collect on your employee?
- What would be your lawful basis for processing their data? If consent is required, employees should not be influenced or threatened to accept it as they could potentially claim unfair or constructive dismissal.
- Ensure a DPIA, LIA (if applicable), DPA (with your provider if needed) is conducted.
- Consult your employees to seek their views on AI tools to manage them.
- Ensure a human manager actively check the outputs provided by the tool and that the tool provides you with accurate and non-biased outcomes.
- Allow your employees to contest the outcome of the tool.
- Be transparent when producing reports from the tool used to monitor your employees. Your reports and the one provided by the AI tool provider should be shared. Ideally, all your assessments (DPIA, LIA etc) should also be accessible to your employees.

ACAS has an evidence-based policy paper which can be accessed [here](#).

The report forms a view of the opportunities and risks that algorithmic management present. It also provides businesses a responsible and ethical approach when considering AI management's tools.

Case Law

ICO v Snapchat – October 2023

Overview

In April 2023, Snapchat launched its own generative AI chatbot called “My AI” in the UK. The tool, which appeared at the top of the user’s feed acts as a virtual friend individuals can interact with. In October 2023, the Information Commissioner’s Office (ICO), which is the independent supervisory authority for data protection in the UK, issued Snapchat with a preliminary enforcement notice over the potential failure to properly assess the privacy risks posed by its generative AI chatbot. Upon investigation, the ICO found that Snapchat failed to adequately identify and assess the risk to several million “My AI” users in the UK, including children aged 13 to 17. Although Snapchat conducted a risk assessment, the ICO found that Snapchat did not adequately assess the risks posed by the AI tool. If a final enforcement notice were to be issued, Snapchat may be required to stop processing data in connection to the AI tool and may have to pay a substantial fine.

Impact

This case confirms that although no AI specific regulation exists in the UK, existing data protection laws protect individuals whose personal data is being processed by AI tools. The ICO is actively enforcing these laws for AI technologies by applying the data protection laws to AI tools.

Action

[Data Protection Risk Assessments \(DPIAs\)](#) should be conducted before the use of any AI technologies. Businesses are also recommended to conduct an [AI Data Protection Risk Assessment](#) and a [Legitimate Interest Assessment \(LIA\)](#). Each assessment should be conducted seriously and in good faith.

Harber v HMRC – December 2023

Overview

Mrs Harber, disposed of a property and failed to notify her liability to Capital Gains Tax (CGT). HMRC, issued her with a failure to notify penalty of £3,265.11, to which Mrs Harber appealed claiming she had a reasonable excuse because of her mental health condition, and because it was reasonable for her to be ignorant of the law. Mrs Harber provided the Tribunal with the names, dates and summaries of nine First-tier Tribunal (FTT) decisions in which the appellant had been successful in showing that a reasonable excuse existed. After reviewing the information, HMRC’s solicitor was unable to identify these cases on the FTT website. It appeared during the hearing that the respective appellant(s) used an AI Generative Chatbot to provide the cases and she did not know how to check their validity on the FTT website. The Appeal was dismissed as the FTT did not find the Appellant to have a reasonable excuse for failing to notify liability to HMRC and accepted that Mrs Harber did genuinely not know the cases used were made up.

Impact

This case highlights that AI tools may be subject to errors, and any outcomes should be reviewed. The FTT identified that there was American spelling in some sentences, and the frequent repetition of identical phrases.

Action

Businesses must have [processes](#) and [training](#) in place to ensure their staff using AI tools are aware of these risks. Regular reports should also be requested from the AI provider highlighting any errors, faults and inconsistencies.

Mata v Avianca INC (USA) – June 2023

Overview

Mr Mata introduced a claim against Avianca INC, after being injured when a metal serving cart struck his left knee during a flight from EL Salvador to John F. Kennedy Airport. Mr Schwartz had been the attorney listed on the state court complaint, but as the case was moved from one court to another, Mr LoDuca filed a notice of appearance on behalf of Mr Mata, while Mr Schwartz continued to perform all substantive legal work. On 13 January 2023, Avianca filed a motion to dismiss. On 1 March 2023, Mr LoDuca filed an Affirmation in Opposition to the motion to dismiss. The Affirmation in Opposition cited and quoted several case law which were said to be published in the relevant Legal case law reporter. Above Mr LoDuca’s signature the Affirmation in Opposition stated, “I declare under penalty of perjury that the foregoing is true and correct”. Avianca filed a reply memorandum on 15 March 2023 which stated that they were unable to locate most of the cases brought forward by the Mr Schwartz and Mr LoDuca. The Court conducted its own search for the cited cases and was also unable to locate them. Mr Schwartz had used ChatGPT which fabricated cases, although Mr Schwartz produced screenshots evidencing that he asked ChatGPT confirmation the cases were real. The Court found that both Mr Schwartz and Mr LoDuca violated rule 11 imposing a gatekeeping role on Attorney and both lawyers were sanctioned to a joint penalty of \$5,000.

Impact

This case emphasises the risk of using AI for certain types of work, and that outcomes produced should also be checked and cross referenced manually by a human.

Action

Ensure a [process](#) exists for each AI tool and that the process is appropriate for the service required from the AI. Ensure your employees are [trained](#) to review the output of the tool and to recognise any “hallucinations”, incorrect or misleading results produced by the AI tool.



Disclaimer: This guidance document is intended for use by APSCo members only. The facts, information, and opinions contained herein are correct to the best of APSCo's knowledge as at time of publication. This document is intended to provide general information only and does not constitute advice. It is not an exhaustive and complete reference document on this subject. APSCo can take no responsibility or liability for the use of or reliance on the information contained within this document or for any decisions or the consequences of any such decisions made by APSCo members.