BARNEA

Your Legal Guide to AI

How to implement AI in your business

Dr. Avishay Klein
Head of Privacy,
AI and Cyber Department

BARNEA

AI and Your Business

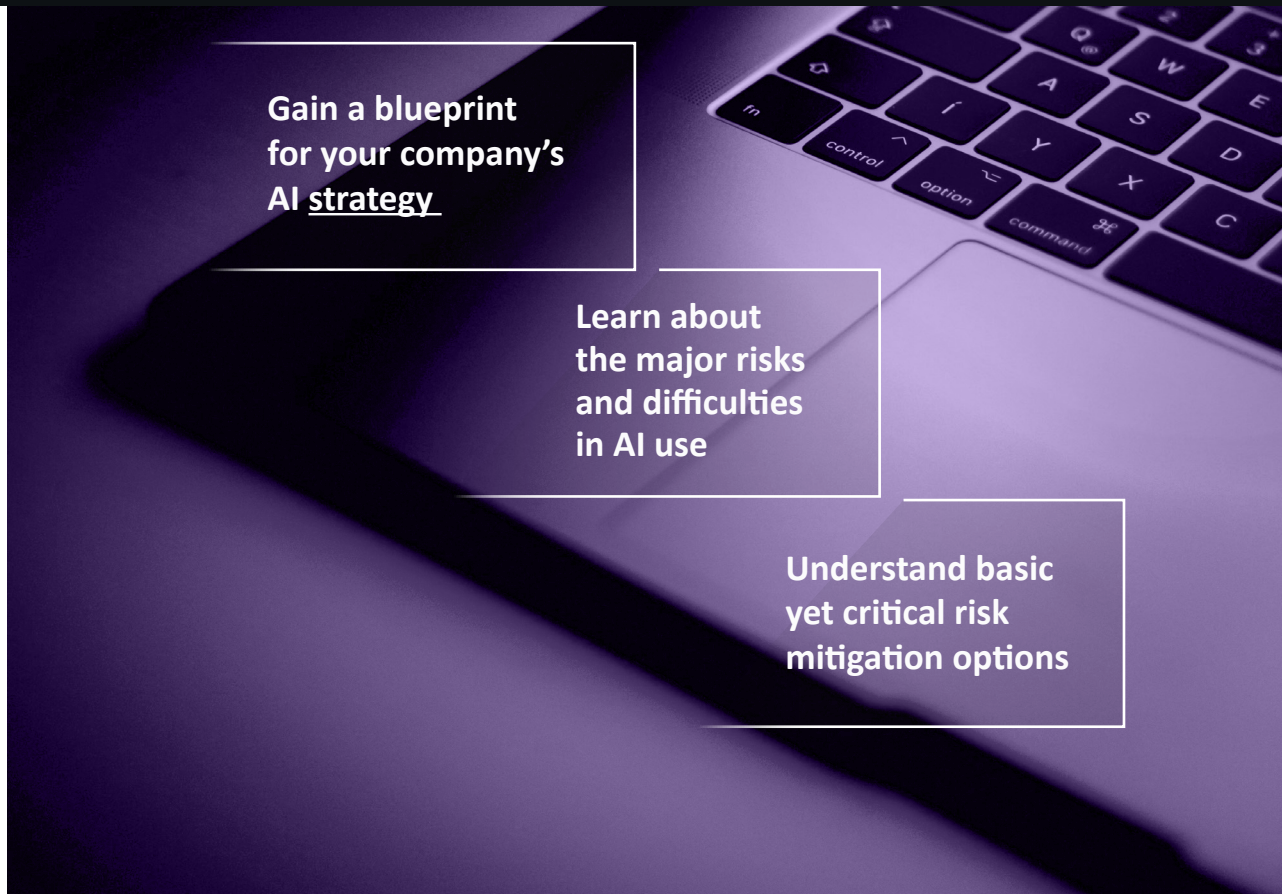
Artificial intelligence (AI) and machine learning (ML) are widespread and can play a major role in different aspects of your business.

HOW?

1. AI tools improve and optimize business processes and day-to-day tasks
2. Common and free tools (such as Bard, ChatGPT, etc.) provide employees a productivity boost
3. Commercial AI models can be customized for specific business purposes and benefits

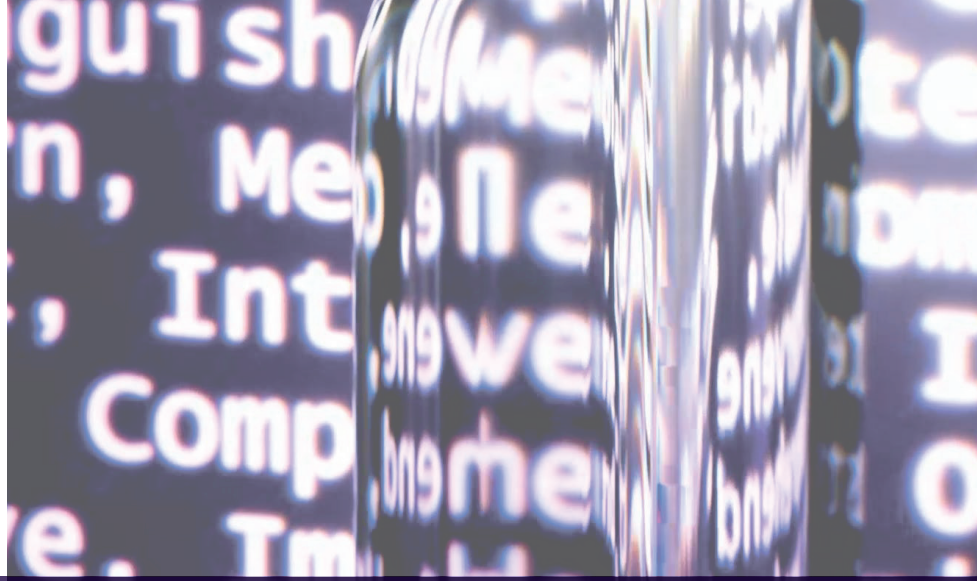
AI tools exist within a complex ecosystem

This legal guide will serve as a set of basic action points for using, acquiring, and integrating AI tools and systems into your business.



BARNEA

Identifying AI Tools and Risks



Managing AI risks requires first **identifying** the AI tools being used. This will enable you to consider the actual risks and decide what type of AI use is acceptable in your workplace.

How to identify the risk:

1. **Map** the relevant AI tools and the departments using them
2. Clearly **define the purpose** for each tool's use
3. **Classify the type of data** and its sensitivity as relevant to each tool
4. **Be aware** of the limitations and main fallacies regarding each AI tool you use

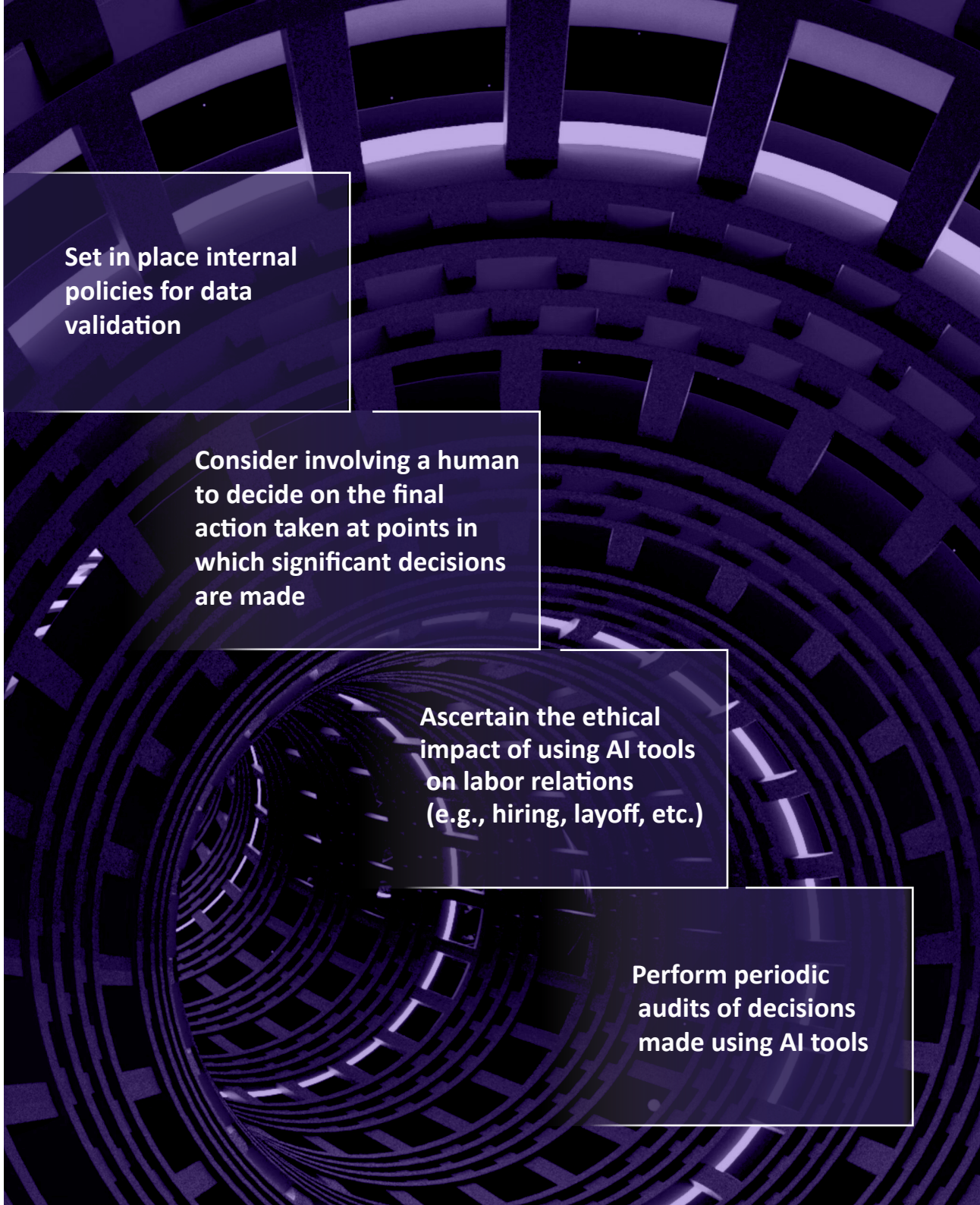
BARNEA

Human Oversight

AI tools can provide outdated and even erroneous and baseless results (AI hallucinations).

AI can also produce results that reflect a bias toward an individual, a group, or a collection of attributes.

Setting clear rules on human involvement when using AI tools can improve your ability to rely on their output and ensure an ethical approach to AI.



BARNEA

Keep Data Privacy in Mind

AI-based systems often require wide-scale use of personal information. The use of AI creates threats to such data, especially when utilized as training data for an AI tool.

It is important to remember that AI systems may be subject to privacy laws and regulations, and violations may result in significant enforcement measures.

How to mitigate privacy risks:

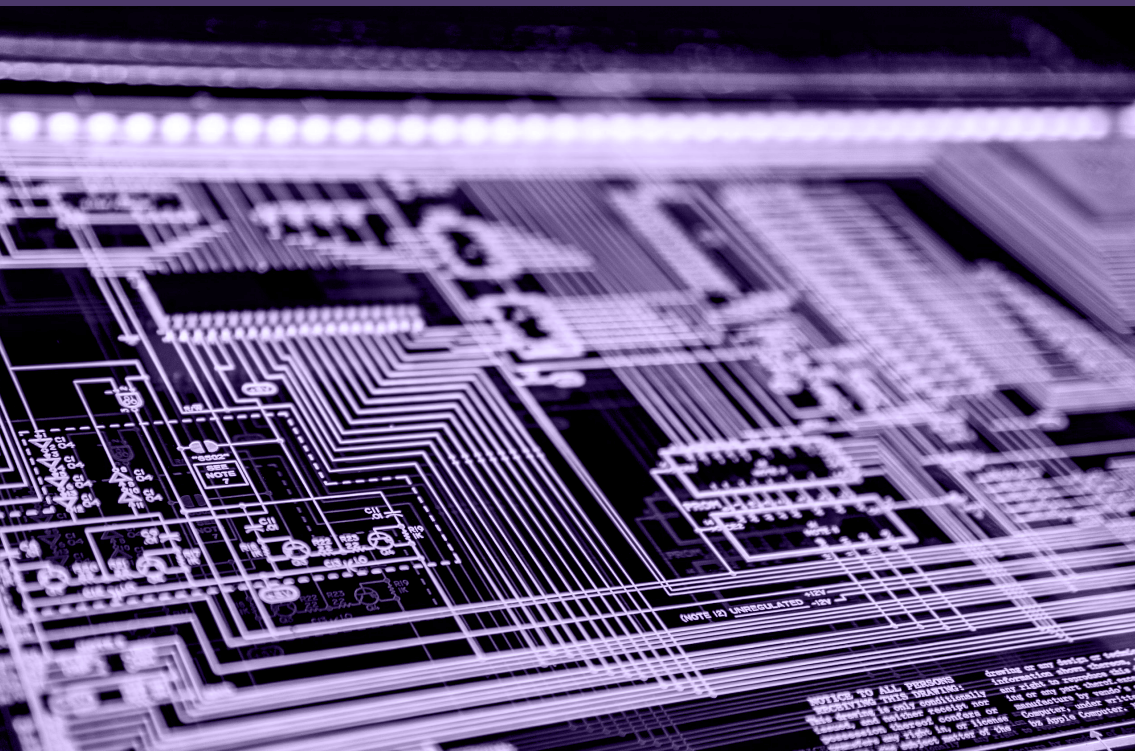
1. Only use personal data when it is necessary and relevant to the desired purpose
2. Limit the use of sensitive data, such as health information, financial data, etc
3. When possible, use anonymized or aggregated data
4. Conduct a data protection impact assessment **(DPIA)**

BARNEA

Secure Your Data

New technologies always create new security exposures. AI makes it easier for bad actors to undertake phishing attacks and spread deepfake videos, among other malicious activities.

Companies must take both organizational and technological security measures to avoid the loss of critical trade secrets and the leaking of personal information, as well as heavy fines.



How to ensure your data is secure:

1. Only the people who need to access the AI tools and have the proper credentials to do so should be able to access them
2. Protect the data sets used to train and improve AI tools. Consider encrypting such data sets
3. Certify that appropriate safeguards are used in the supply chain
4. Formulate a strategy to respond quickly and effectively to any breach of confidential data
5. Add clauses to employment agreements regarding the safeguarding of trade secrets and confidential data when using AI

BARNEA

Check Your Vendors

Ensure that relevant information about AI systems' operations and characteristics is available to you.

This will allow you to effectively choose the relevant vendors in view of the risks, possible misconceptions, and other issues with the tools.

To deal with the supply chain risks in AI systems, make sure **adequate contractual terms** and **a proper vetting process** regarding privacy and AI compliance are in place.

Your agreements with vendors should also contain express covenants of liability for compliance with legal and regulatory standards, as well as indemnity and liability obligations for damages resulting from reliance on the technology.

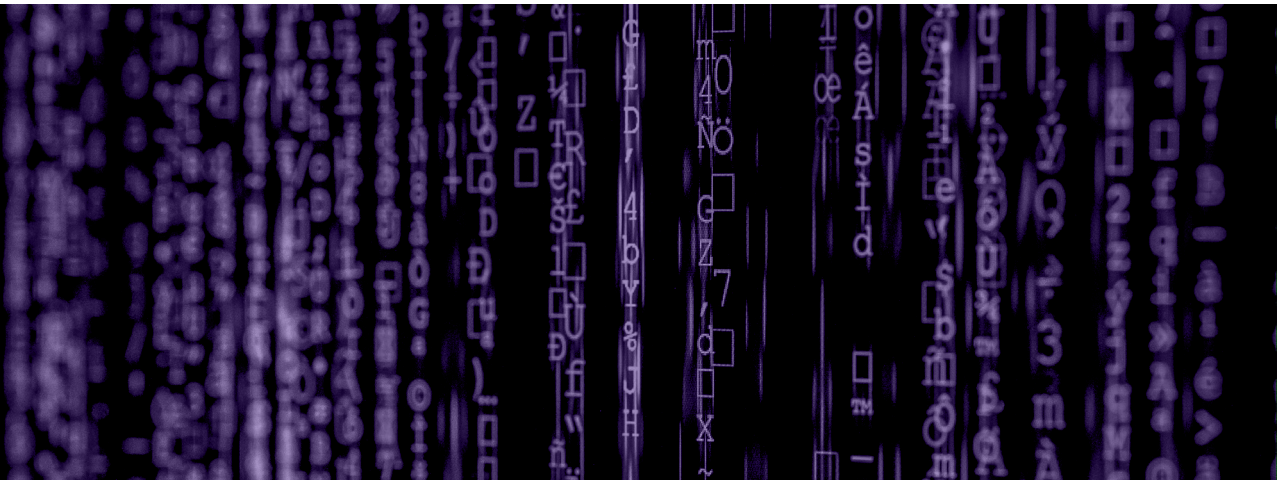
BARNEA

Familiarize Yourself with Evolving AI Regulations

AI laws and regulations are being developed all around the globe, including the European AI Act; the US Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence; and more.

Various legal frameworks in the fields of privacy, IP, consumer protection, financial regulation, and labor law are also applicable when using AI tools.

Compliance with such regulations and standards is important from a business perspective, but is also essential to avoid enforcement actions and heavy fines.



How to navigate this ever-changing legal field:

1. Closely **monitor** regulatory developments and consider their applicability to your business

2. **Consult** with privacy and AI professionals to assist you in “translating” the legal requirements to actual tasks

3. **Prepare** an action plan aided by legal advisors to ensure compliance with the emerging AI standards and regulations, as well as with other relevant regulations

BARNEA

Train and Inform Your Employees

Uninformed or unsanctioned use of AI tools may increase the risk to your company.

Employees using or developing AI systems or relying on their information must be educated on AI use and follow a company's internal guidelines.

We recommend that such education will include at least the following:

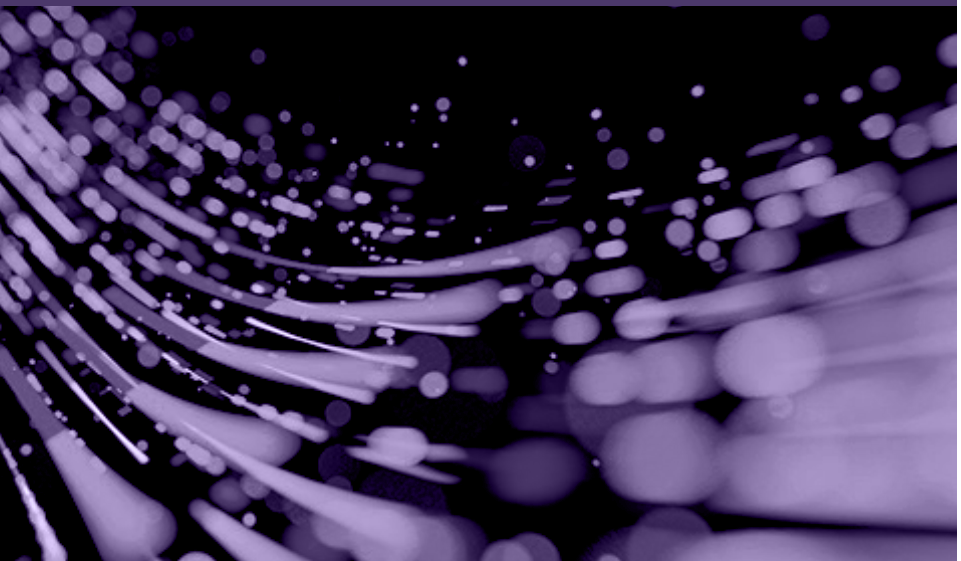
1. Stressing the importance of the separation between personal and professional uses of AI in the workplace
2. Examples of the common fallacies possible in the tools used, as well as the importance of effective human supervision
3. Do's and don'ts regarding the use of personal and proprietary information

BARNEA

Create an AI Policy

A comprehensive internal policy on AI use can serve as a powerful tool in an organization.

The policy will serve as a reference point for employees, as a basis for training material, and as proof of responsible use of the various AI tools.



Pillars of the policy:

1. The principles determining the AI policy
2. The type of data to be used (or not used) as input for AI systems (both proprietary and free-use systems)
3. An updated risk assessment of the AI tools used by the company
4. The procedures implemented to mitigate any relevant risks
5. An employee training plan
6. Vendor vetting and new AI system procurement guidelines
7. A review-and-update mechanism for the policy

BARNEA

Barnea Jaffa Lande's AI team

Contact Information

Dr. Avishay Klein
Head of Privacy,
AI and Cyber Department
aklein@barlaw.co.il

Adv. Masha Yudashkin
Privacy, AI and Cyber Department
myudashkin@barlaw.co.il

THANK YOU

Barnea Jaffa Lande & Co. Law Offices
barlaw.co.il
Electra City Tower, 58 HaRakevet St.
Tel Aviv, Israel. T. +972.3.6400600