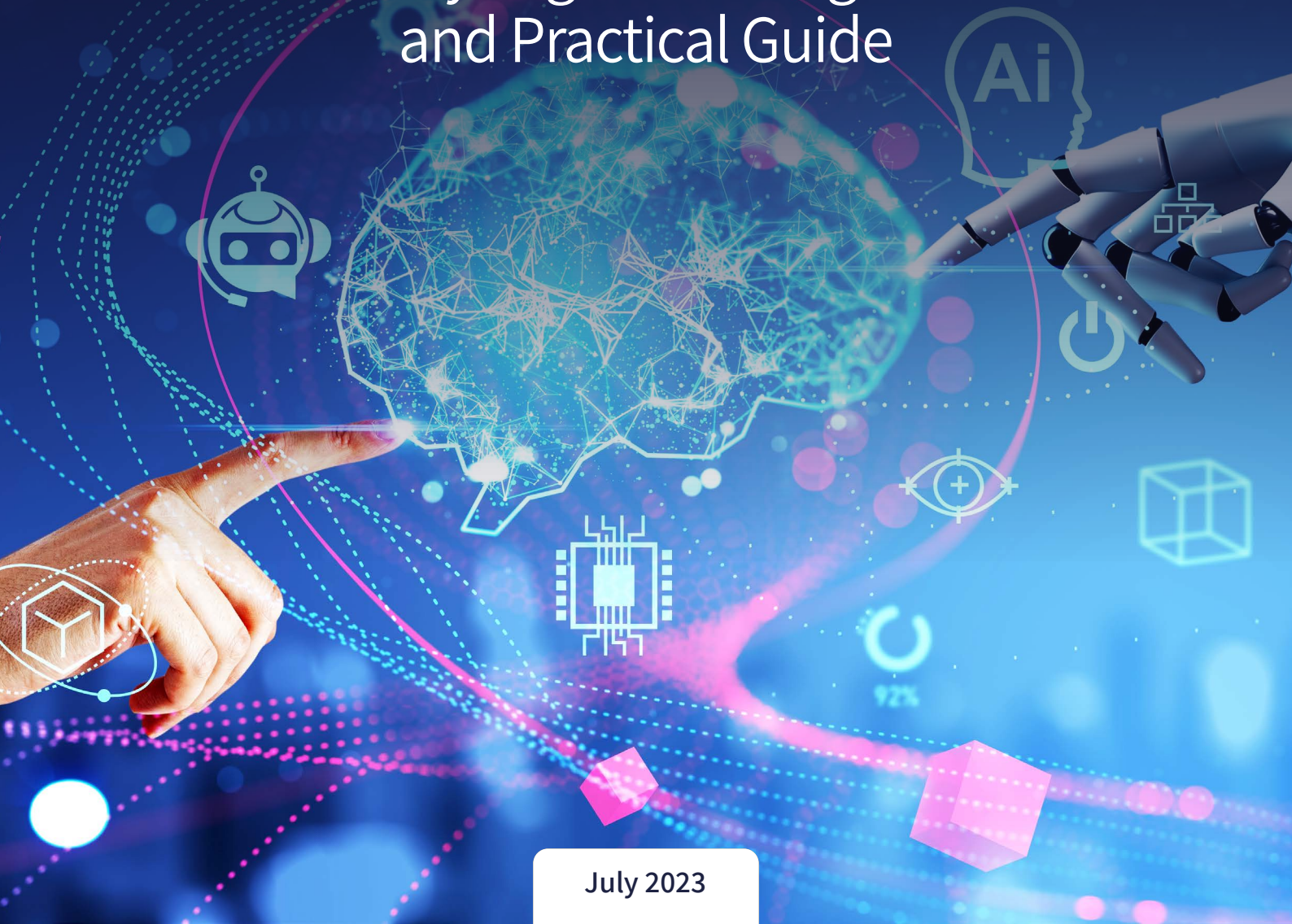
HERZOG

HERZOG FOX & NEEMAN

Using Artificial Intelligence Systems in Organizations

Key Legal Challenges and Practical Guide



July 2023

The use of Artificial Intelligence (AI) systems is becoming more common in businesses, product development and commerce contexts.

Following questions raised by many clients in a **variety of industries,** we have put together this guide, which provides an **initial overview** of the **key legal risks** associated with **using AI systems in your organization,** together with some **initial recommended actions** and **precautions** to mitigate such risks.

This guide is intended to be part of a series of publications, each focusing on a different segment of practices and business sectors, and providing practical tips and insights, while addressing the evolving regulatory regimes in the field of AI (such as the draft European AI Act).

FACTUAL INACCURACIES IN OUTPUTS AND INPUTS

AI systems often operate as "black boxes". They arrive at conclusions or decisions without providing any explanations as to how they were reached. Such systems rely on the data used for training, which may include biases or inaccuracies. Even when training the model on your own organization's data, biases and inaccuracies unintentionally included in the input data may **adversely affect the accuracy of output**. In addition, even without biased or erroneous input data, AI processing results may be wrong or contain fictitious outputs sometimes referred to as "hallucinations".

Such concern is demonstrated by the recently published case of a New York lawyer who has been fined $5,000 due to a court filing that referenced **nonexistent legal cases** based on "case law" provided by an AI-based chat system. In this case the judge noted that "technological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But **existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings**".

Similarly, it is **paramount for organizations relying on AI systems to verify both the input and the output**, and to never blindly rely on AI's processing results.

Do:

- ✓ Implement rigorous data quality checks and frequent validation processes.
- ✓ Keep a human in the loop for decision-making processes involving material consequences for the business, its employees and clients.

Don't:

- ✗ Rely solely on AI outputs for important decisions without human oversight. Neglecting to check the AI's data source or its algorithmic logic could lead to errors in judgment based on false information.

PRIVACY AND CONFIDENTIALITY

Another concern arises when using AI systems (especially conversational AIs or ones that require users to enter "prompts", e.g., ChatGPT or Bard), as the data uploaded or made available to these services may contain personal or confidential information. These services might **store and utilize the data provided by your organization** to improve their offerings and train their algorithms, often under extensive, perpetual, and irrevocable licenses.

From a privacy perspective: Providing personal data collected by your organization to AI systems can pose significant legal risks, including under various privacy laws, which restrict the sharing of personal data with third parties without addressing various requirements. Those include limitations concerning the purpose of such data sharing, the legal grounds of the processing, limitations on the location to which the personal data is shared, as well as additional procedural and contractual requirements.

Furthermore, sharing personal data with AI systems can be risky and expose your data to various security threats. For example, a bug discovered in an AI chat earlier this year allowed some users to see other users' personal information, including their name, email address, payment address, the last four digits of their credit card number, and credit card expiration date.

In addition, existing laws may restrict some organizational processes from being implemented on personal data with the use of AI. For example, according to Article 22 of the EU General Data Protection Regulation, data subjects have the right not to be subject to decisions made solely based on automated processing of their data if these decisions produce legal effects or similarly significantly affect them (for example, see below in the context of employment-related automated decisions). In such cases organizations may be required to implement measures such as informing data subjects about the use of AI in decision-making, obtaining their explicit consent, and providing the right to obtain human intervention or contest the decision. If not handled correctly, this could lead to enforcement actions and lawsuits.

Confidentiality: Uploading confidential information into AI systems can potentially lead to legal liability if the information is protected under confidentiality agreements, trade secret laws, or other similar legal restrictions. Furthermore, it exposes your (or your client's) confidential data to security risks, which could result in confidentiality of data being compromised. For instance, an improperly trained AI system might inadvertently expose confidential information to other users.

Do:

- ✓ Prior to implementing AI features or initiating organizational use of an AI system, assess the risks and the legal framework applicable to your intended use and ensure the existence of required compliance measures.
- ✓ Before sharing or granting access to any personal data, ensure that such sharing is compliant with data protection laws and doesn't violate any contractual obligations your organization might have. This includes (but not limited to) ensuring a solid legal basis for sharing, verifying the existence of organizational and technical safeguards, performing an assessment of the data recipient (the AI provider), and executing applicable data protection agreements.
- ✓ Regularly educate your team on the importance of data privacy and confidentiality, and the risks associated with disclosing personal or confidential information to AI systems. Awareness is the first line of defense.
- ✓ Develop clear, comprehensive policies outlining the types of information that should never be disclosed to AI systems.

Don't:

- ✕ Upload or make available to AI services any personal information unless it is done in accordance with the organization's data protection policies and procedures.
- ✕ Upload or make available to AI services any confidential information unless it is compliant with the organization's legal and contractual confidentiality obligations.

EMPLOYMENT

Using AI systems in recruitment and employment contexts may have **specific legal implications**. Current laws in the US, including anti-discrimination laws, require that you use hiring AI systems carefully. In the EU, employers should also consider implications under the GDPR, particularly those related to automated individual decision-making (as mentioned above), and which may apply in certain cases.

For example, NYC Local Law 144 provides that employers using automated employment decision systems must conduct an independent bias audit and publish a summary of the results. These employers are also required to notify applicants of the use of such systems, and provide an alternative selection process upon request.

Moreover, under the Illinois AI Video Interview Act employers using AI analysis of applicants' video interviews must notify applicants of the use of AI and provide an explanation of how it functions; obtain the applicant's consent before conducting the AI-powered video interview; upon an applicant's request, destroy all copies of the applicant's videos and instruct any service providers involved in the hiring process to do the same; provide an annual report that includes a demographic breakdown of the applicants as well as statistics regarding the number of rejections versus hires; applicant videos should only be shared with relevant vendors or parties involved in the hiring process.

Failure to comply with these requirements may result in claims and lawsuits.

Do:

- ✓ Be transparent about how you use AI in hiring or other employment decisions. Candidates and employees have a right to know if AI systems are being used and how they impact decision-making processes.
- ✓ Regularly train those working with AI on anti-discrimination laws and practices. This includes educating them on how unconscious bias can impact AI use, even unintentionally.

Don't:

- ✗ Rely solely on AI for critical employment decisions; AI should augment, not replace, human judgment. When you do use AI in employment, keep looking for patterns that may suggest certain demographic groups are being disadvantaged or discriminated against. Such a pattern, even if unintentional, could still be legally significant.
- ✗ Overlook feedback from candidates or employees about their experiences with AI systems. These insights can highlight potential issues or areas of concern that may not be immediately apparent.

INTELLECTUAL PROPERTY

Ownership

The use of generative AI systems may result in the creation of works or inventions. While works of authorship (e.g., source code) and inventions are generally protected under applicable copyright and patent laws, AI-generated works and inventions might not be entitled to such protection since no natural person authored or invented them.

For instance, in 2022, the US Copyright Office denied a copyright application for a visual work described by the applicant, Dr. Stephen Thaler, as “autonomously created by a computer algorithm running on a machine.” Consequently, in March 2023, the US Copyright Office released guidelines regarding works containing material generated by AI. According to the guidelines, copyright can only protect material that is the result of human creativity, as the term "author" in the US Constitution and the US Copyright Act excludes non-humans. As such, in all cases where the work contains AI-generated content, the applicant must demonstrate that the traditional elements of authorship were created by a natural person and not by AI.

The same Dr. Thaler has also attempted to challenge the patent laws around the world by filing international and national patent applications that mentioned his AI machine, DABUS, as an inventor. As of today, these applications were refused in most of the jurisdictions, including the US, the UK, the EU, and Israel, on the basis of the human inventor requirement. In contrast, Thaler's applications were granted by both the South African IP Office and the Australian Federal Court.

Even if AI-based creations may be protected in some jurisdictions under copyright or patent laws, the terms of use of certain AI systems provide that the company which owns the tool also owns the AI system's output; they often grant a broad, royalty-free, and irrevocable license to use and even prepare derivative works of the output (see, for example, the Midjourney and Copy.ai Terms of Service).

Furthermore, the terms of use of most AI platforms include a broad license to the user’s input as well. The upshot is that the user's IP may be included in the platform and portions thereof may ultimately be used by third parties without the original user's knowledge or consent.

Do:

- ✓ Ensure that there is human involvement in the creation of the company's material IP and, to the extent possible, in the creation of the output itself (e.g., the arrangement and structure).
- ✓ Carefully review the ownership and license provisions of each AI system's terms of use.
- ✓ Enable any filters or purchase paid/pro subscriptions, which limit the scope of the license granted to the AI platforms.

Don't:

- ✗ Use generative AI systems to generate core or material portions or elements of your code.
- ✗ Use portions of your organization's proprietary code as part of the input unless the AI platform.

Infringement

Generative AI systems train their models on a variety of different datasets; therefore, it is possible that the generated content may infringe upon third parties' IP rights, such as copyrighted images or code and trademarks. This might bring about claims of IP infringement, particularly if the generated content closely resembles existing protected works.

While recent lawsuits in the US target the generative AI platforms rather than the users for copyright infringement claims (see, for example, the Stable Diffusion class action and the GitHub Copilot class action), the risk for users who exploit the output remains significant. In addition, most generative AI platforms do not include any non-infringement warranty or IP indemnification.

Lastly, as previously stated, the ability to copy and paste information and submit queries into a freeform text field increases the likelihood that larger sets of sensitive data will be entered into the AI platforms. Such use increases the risk of trade secrets misappropriation.

Do:

- ✓ Implement a control mechanism, requiring approval prior to certain uses of AI-generated content (e.g., in the front-end).
- ✓ Immediately remove any infringing content upon receipt of notice of IP infringement.
- ✓ Depending on the AI platform and its terms of use, and to the extent possible, modify/revise the output.

Don't:

- ✗ Enter any confidential information into the generative AI platforms including any material proprietary code.
- ✗ Depending on the AI platform and its terms of use, avoid using generated output as-is.

Open Source

Since generative AI systems such as GitHub Copilot and ChatGPT are trained, in part, on open source libraries, there is a risk that the output may be subject to copyleft licenses.

A copyleft license may require, for example, that any code incorporating the open source code to which it applies be distributed in source code form, licensed for the purpose of preparing derivative works, or redistributed without charge. A prime example of such copyleft open source license is the GNU General Public License.

Although the issue is still under debate (see the GitHub Copilot class action referenced above), if generative AI output is determined to be a derivative work of the training materials, users might be required to comply with the open source licenses governing the use of such materials, some of which might be copyleft licenses. Most other open source licenses also impose conditions on the use of the open source code, most notably, a requirement to provide copyright notices (also known as attribution requirements).

Do:

- ✓ Consider implementing a tagging system in order to distinguish between the human-created code and AI-created code.
- ✓ Use AI scanning tools that detect open source components in your code.
- ✓ Enable platforms' features such as Github Copilot's duplication detection filter (which filters code suggestions that resemble public code on GitHub).
- ✓ If possible, use AI systems that use open source code with permissive licenses (e.g., Tabnine).

Don't:

- ✗ Use AI systems that train on open source code without enabling filtering tools or implementing scanning tools.
- ✗ Use AI systems that train on open source code without implementing a policy limiting use of the output to certain elements or sections of the proprietary code.

CONTRACTUAL RISKS

Taking into account the foregoing, it is important to note that the terms of use of the AI systems place the responsibility for all risks, including the outputs, on the users of the systems. These terms often provide no indemnification or protection; instead they protect the developers against infringement claims arising from **user** input and system output. As a result, **users bear the entire risk associated with the outputs generated by AI systems.**

Do:

- ✓ Conduct thorough due diligence before integrating any AI system into your organization.
- ✓ Educate your employees about the potential risks associated with AI usage.
- ✓ Establish an internal procedure for implementing new software.

Don't:

- ✗ Use random or unverified software in your organization without seeking professional legal or technical advice.

The rapid emergence and adoption of AI systems necessitate a heightened level of caution and due diligence. While AI holds immense potential, users must be aware of the risks associated with its use, as well as of the evolving regulatory frameworks around the technology.

In this document we presented a general overview of the typical risks associated with using AI systems. This is not an exhaustive legal opinion or regulatory overview of all applicable regulatory requirements regarding the topics presented. **We encourage you to contact our AI team for further insight into the specific risks related to your business practices and industry.**

Herzog's Artificial Intelligence and Intellectual Property Practice

Artificial Intelligence ("AI") technologies are reshaping familiar industries and bring them to new exciting frontiers which raise novel fascinating legal and regulatory challenges. AI has recently come to the forefront of the regulatory and legislative trends globally, and are now subject to the increased of focus of legislators and regulators in a wide array of jurisdictions. Alongside the emerging **bespoke regulatory frameworks,** AI systems are also subject to various **existing general and sector specific legal and regulatory regimes**, as well as self-regulatory guidelines which lie at the intersection of law and technology.

Our unique Artificial Intelligence law practice, supported by our IP experts in Herzog's IP Department, is led by top legal experts and professionals with deep legal, regulatory as well as technical understanding and hands-on background in AI, machine learning, deep learning and neural networks technologies. This enables us to offer tailor made and practical solutions for often complex situations, and to assist in the **development, implementation, management and use of** adequate and compliant **AI technologies,** thereby mitigating legal and business risks.

Our team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in **a myriad of jurisdictions, digital platforms** and leading **self-regulatory** guidelines. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks

---

Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Michal Kra | Associate
Technology Regulation
kram@herzoglaw.co.il

Oded Kramer | Associate
Technology Regulation
kramero@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Dima Zalyalyeyev | Associate
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Eden Lang | Associate
Technology Regulation
lange@herzoglaw.co.il

Or Noy | Associate
Technology Regulation
noyo@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Mai Arlowski | Intern
Technology Regulation
arlowskim@herzoglaw.co.il

Liron Adar | Intern
Technology Regulation
adarl@herzoglaw.co.il

Karen L. Elburg | Partner
Head of Intellectual Property
elburgk@herzoglaw.co.il

Adar Bengom | Partner
Intellectual Property
bengoma@herzoglaw.co.il

Nadav Lev | Associate
Intellectual Property
levn@herzoglaw.co.il

Chen Arobas | Associate
Intellectual Property
arobasc@herzoglaw.co.il

Adi Golding | Associate
Intellectual Property
goldinga@herzoglaw.co.il

Orit Lissak | Associate
Intellectual Property
lissako@herzoglaw.co.il

Hadas Weinblut | Paralegal
Intellectual Property
weinbluth@herzoglaw.co.il

Barak Vardi | Intern
Intellectual Property
vardib@herzoglaw.co.il

Shahar Shwartzman | Intern
Intellectual Property
shwartzmans@herzoglaw.co.il

Ron Morad | Intern
Intellectual Property
moradr@herzoglaw.co.il

Eden Sasson | Intern
Intellectual Property
sassone@herzoglaw.co.il

Neriya Rettig | Intern
Technology Regulation
rettign@herzoglaw.co.il

Kobi Plotkin | Intern
Technology Regulation
plotkiny@herzoglaw.co.il