

AI IN THE WORK OF AN ATTORNEY-AT-LAW



NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW

WARSAW, 2025

AI IN THE WORK OF AN ATTORNEY-AT-LAW

RECOMMENDATIONS ON
HOW ATTORNEYS-AT-LAW
SHOULD USE AI-BASED TOOLS

1st edition
Warsaw 2025



NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW



Microsoft



SOŁTYSIŃSKI
KAWECKI
& SZLĘZAK

Publisher: Krajowa Izba Radców Prawnych,
ul. Powązkowska 15, 01-797 Warszawa

© Copyright by Microsoft sp. z o.o., 2025

ISBN 978-83-972004-5-6

English translation: Sołtysiński Kawecki & Szlęzak - Kancelaria Radców Prawnych
i Adwokatów SP. K.

Typesetting and layout: Aleksandra Snitsaruk

Printing: Wiedza i Praktyka sp. z o.o.



Foreword

The development of tools based on artificial intelligence (AI) is a phenomenon that radically changes the way many industries, including the legal world, operate. The use of AI in the work of an attorney-at-law has ceased to be a matter of choice and has become a natural direction for the development of the profession. There is no one-size-fits-all approach to the use of AI in the work of a lawyer – the scope and manner of using these tools will always depend on the specific needs of a given law firm or attorney-at-law.



Regardless of whether AI will be used occasionally as a support in the analysis of documents or case law, or will become an important part of everyday work, it is necessary to learn the principles of its safe and informed implementation. This publication not only introduces the subject of generative AI, but also helps to address possible concerns and provides practical tips on how to use new technologies without violating the principles of professional ethics and legal security of clients. A conscious approach to AI allows you to fully use its potential while minimizing the risks associated with it. With the rapid development of AI technology, lawyers have to face new challenges, such as issues related to data protection, professional secrecy or liability for content generated by artificial intelligence.

It is worth noting that the presented recommendations are not final – as AI develops, they will be subject to further evolution and clarification. We are only at the beginning of the road related to the implementation of this technology in legal practice. In the coming years, there will be case law that will begin to shape practical standards for the use of AI, and regulations concerning this technology will become more systematic and precise. Therefore, this publication should be treated as a “living document”, the content of which will be updated and adapted to the changing legal and technological environment.

We hope that the presented recommendations will prove valuable in the daily work of attorneys-at-law. Their main goal is practical usefulness – to provide specific tips that will help to safely and effectively use AI tools in the daily activities of attorneys-at-law.

Włodzimierz Chróścik
President of the National Bar Council of Attorneys-at-Law

RECOMMENDATIONS PREPARED IN COOPERATION WITH:



NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW

The National Council of Attorneys-at-Law

- Damian Flisak PhD – attorney-at-law, KIRP
- Paweł Kowalski PhD – attorney-at-law, attorney-in-fact of President of The National Bar Council of Attorneys-at-Law concerning New Technologies



Microsoft

Microsoft sp. z o.o.

- Renata Zalewska – attorney-at-law, Senior Commercial Attorney
- Tomek Kasprzyk – Legal Program Manager
- Paweł Wróbel – Technical Architect Innovation Hub | Central Europe



SOŁTYSIŃSKI
KAWECKI
& SZLĘZAK

Sołtysiński Kawecki & Szlęzak Kancelaria Radców Prawnych
i Adwokatów Spółka Komandytowa

- Agata Szeliga – attorney-at-law, Partner
- Sylwia Macura-Targosz – attorney-at-law, Senior Associate
- Katarzyna Paziewska-Młodawska – attorney-at-law, Senior Associate
- Anna Tujakowska – advocate, Senior Counsel

..... INTRODUCTION

In November 2022, the generative AI tool, Chat GPT, was made available to the public for the first time. AI became available to everyone, including lawyers. Soon, the first reports emerged of the tool being used without verification, in particular, by pointing out non-existent court rulings. This sparked discussions about whether lawyers can use AI solutions. However, this is not a new discussion – a similar question arises with every new technology. As the example of cloud computing shows, lawyers can legally and ethically use new technologies. However, proper preparation and competence are necessary.

Of the new technologies, it is AI that is indicated as the technology that could have the most significant impact on the legal profession. Already at this moment, standard tools allow materials previously prepared by trainees attorney-at-law or junior lawyers to be generated in minutes. There is no longer any doubt that AI will bring about significant changes in the way the profession is practiced, from training through the manner and scope of counseling to client’s billing. These recommendations aim to help attorneys-at-law and lawyers prepare to use AI in a responsible and compliant manner.

These recommendations consist of two parts. The first contains basic concepts and general information about regulations on using AI. The second contains recommendations divided into three groups:

- Recommendations for preparing to use AI tools,
- Recommendations for implementing AI tools, and
- Recommendations for using AI tools.

..... TABLE OF CONTENTS

Section I	7
ARTIFICIAL INTELLIGENCE – BASIC ISSUES	
1. What is AI?	7
2. Examples of available AI tools	11
3. Basic concepts – generating and using (training) data	13
4. AI vs. cloud computing	15
5. Examples of applications of generative AI tools in the work of an attorney-at-law	15
Section II	17
PROVISIONS OF LAW – BASIC REGULATIONS	
1. Personal data	17
2. AI Act	20
3. Copyrights	21
4. General regulations on contractual relations	23
5. Liability for defective products	24
6. Cyber Security	24
7. Regulations for attorneys-at-law	25
8. Criminal proceedings	26
Section III	27
USE OF AI TOOLS BY LAWYERS – BENEFITS, CHALLENGES, AND RISKS	
1. Benefits	27
2. Challenges	28
3. Ryzyka	30
Section IV	33
FOREIGN BAR ASSOCIATIONS’ GUIDELINES ON USING AI TOOLS	
Section V	34
RECOMMENDATIONS	
Appendices	58
1. Tips for best prompting	58
2. Examples of AI applications (using Microsoft 365 Copilot as an example)	59

ARTIFICIAL INTELLIGENCE – BASIC ISSUES



1. What is AI?

1.1. STATUS QUO

Artificial intelligence, particularly generative AI, is extensively utilised across various sectors, including healthcare, e-commerce, and manufacturing. Today, it primarily allows organizations using AI tools to become more efficient but also has the potential to accelerate or advance innovation.

Solutions using AI are also useful in the legal counseling profession. They can be used to perform a variety of tasks, such as analyzing documents, generating contracts or searching for large data sets. This allows attorneys-at-law to save time and focus on more complex aspects of work that require human judgment and creativity. AI development is dynamic. With the emergence of so-called “agents”, we can independently create solutions that are more tailored to the needs of specific lawyers.

The development and rapid spread of AI has accelerated work on defining legal rules for using AI. On 13 June 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act), also referred to in these Recommendations as the AI Act was adopted. The Regulation will be supplemented by national regulations to ensure proper implementation and supervision within EU member states (the Artificial Intelligence Systems Act). Additionally, it will be accompanied by guidelines, clarifications, and codes of practice.

1.2. PREDICTIVE AND GENERATIVE AI

AI is a field of science that aims to build systems to act intelligently.

AI can be categorized into predictive and generative types, which primarily differ in their data processing methods and result generation. In doing so, AI systems can combine both approaches.

Predictive AI is a type of AI that analyzes historical data to predict future events or outcomes. A key component of predictive AI is machine learning (*Machine Learning*) and statistical models. Machine learning involves creating algorithms that allow computer systems to perform tasks without instructions, relying on patterns and inference, then allows that information to be used to predict future events or outcomes. The goal of machine learning is to analyze data to find patterns and make predictions. This approach is utilized to forecast weather, predict machine failures, or assess credit risk.

Generative AI (GenAI) is a type of AI that can create new content (such as text, images, music, and computer code) based on training data. A key component of generative AI is large language models (LLM), neural networks or transformers which process and generate human-like text based on learned patterns. Examples of generative AI solutions include ChatGPT, which produces text based on provided data; Dall-E, which is utilized for image generation; and GitHub Copilot, which generates computer code or verifies existing code.

1.3. HOW DOES AI WORK?

The researchers' end goal is to create a general AI (*general AI*), that is a system that is supposed to be able to reason and draw conclusions at the same level or even better than a human. Such general AI will learn on its own how to draw conclusions, solve complex problems and evolve, even without human input.

At the current stage of AI development, we can distinguish the following stages in the operation of AI:

- collecting data and preparing it for further use;
- data processing and learning (model training);
- model construction;
- testing and refining the AI model; and
- AI system development.

The first step is to collect large data sets which can come from a variety of sources, including the Internet or the resources of specific entities (e.g. books, newspaper archives). This data forms the basis on which AI will learn and later

Section I

take further actions. At this stage, the data should also be verified for accuracy and potential risk of discrimination (e.g. by removing erroneous data).

The next step is processing and analyzing the collected data and learning. The primary methods for developing AI models are machine learning-based techniques, which use data to achieve specific objectives, and logic and knowledge-based techniques, which use encoded information or symbolic representations to solve tasks.

Machine learning encompasses various approaches, such as supervised learning, unsupervised learning, self-supervised learning, and reinforcement learning (rewarding and punishing to develop an optimal solution). Examples of AI models based on supervised learning include image classification systems, medical device diagnostic systems and fraud detection systems. In the context of unsupervised learning, the AI model is trained on unlabeled data utilizing methods such as clustering, dimensionality reduction, association rule learning, anomaly detection, or generative models.

Logic and knowledge-based approaches include models that infer based on coded knowledge or the symbolic representation of a task. Medical diagnosis systems are created by incorporating the expertise of numerous medical professionals.

The next step is to build the model based on the developed patterns. The most common way to do this is to use advanced algorithms (including neural networks) or deep learning methods (which use multilayer neural networks and could independently extract information from data) so that the model recognizes complex patterns and relationships.

The next step is to refine the model. AI models are continuously improved based on, among other things, new data, and feedback. Validating the AI model, i.e. checking its accuracy, is also conducted at this stage.

The last step is to use the AI model to create an AI system.

1.4. AI SYSTEM VS. AI MODEL

According to Article 3(1) of the AI Act, an “**AI system**” is defined as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.

To clarify this concept, the European Commission has approved guidelines for the definition of an AI system.¹ In particular, the guidelines indicate cases where a specific IT solution will not constitute an AI system. The EC guidelines are not mandatory and will be updated when needed, based on practical experience, new questions, and emerging use cases.

The concept of “AI system” should be distinguished from the concept of an “AI model”. The AI Act does not contain a definition of an “AI model”, but according to recital 97 of the AI Act “AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems”. An AI system is a more complex structure that can include one or more AI models, as well as additional elements such as a user interface or databases.

In doing so, the AI Act distinguishes a “general-purpose AI model” which is an AI model capable of performing a wide range of different tasks (Article 3 (63) of the AI Act). According to recital 99 of the AI Act: “large generative AI models are a typical example for a general-purpose model”.

In contrast, a “general-purpose AI system” should be understood as “AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems”.² An example of a general-purpose AI system is, for example, ChatGPT.

1.5. DIVISION OF AI SYSTEMS BY THE AI ACT

The AI Act classifies AI systems into four categories according to the level of risk they may pose to users.

1.5.1. AI SYSTEMS OF UNACCEPTABLE RISK

These are systems whose use is prohibited. The technologies mentioned in Article 5 of the AI Act encompass those that can, for instance, manipulate or mislead individuals, exploit their vulnerabilities, utilize social scoring, or infer emotions in workplaces and educational institutions, with certain exceptions.

¹ The EC guidelines are available here: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>.

² Article 3 point 66 of the AI Act.

Section I

The European Commission has approved detailed guidelines on prohibited AI practices.³ The guidelines are not binding.

1.5.2. HIGH-RISK AI SYSTEMS

Are systems that may pose significant risks to health, safety or fundamental rights. High-risk systems are delineated in Article 6 and Annex III of the AI Act. They include systems used in healthcare, transportation, education and employment. They require implementing and maintaining risk management systems, high-quality training data to minimize the risk of discriminating against results, transparency of operations, and using appropriate human oversight measures, high levels of accuracy, robustness, and cybersecurity.

1.5.3. LIMITED-RISK AI SYSTEMS

Those include technologies that can affect users but do not pose a serious threat, such as chatbots and recommendation systems. They require only minimal transparency measures, such as informing users that they are dealing with AI. and

1.5.4. MINIMAL RISK AI SYSTEMS

These are systems that pose no risk to users. They include most AI applications, such as spam filters. They do not require special regulations or precautions⁴.

2. Examples of available AI tools

AI tools can be classified into various categories based on their functionalities and applications.

2.1. STANDARD

Standard AI tools are AI systems that require no special configuration and are available off-the-shelf. They use AI to support users in a variety of daily tasks, increasing user creativity and productivity. These tools help generate and edit

³ The EC guidelines are available here: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

⁴ For more information on the division of AI systems, see, for example, here: <https://digital-strategy.ec.europa.eu/pl/policies/regulatory-framework-ai>.

Section I

content, automate tasks, analyze data, create presentations, and manage email and calendars. An example of such tool is Microsoft 365 Copilot which works with Microsoft 365 applications such as Word, Excel, PowerPoint, Outlook and Teams.

2.2. DESIGNED FOR LAWYERS

AI tools for lawyers are solutions tailored to the specific needs of lawyers that help analyze legal documents, manage cases, due diligence and automate office processes. An example of such tool is the Harvey application.

Tools for legal professionals can be developed using conventional applications, such as: Microsoft PowerApps or Copilot Studio allow building tools to embed AI models.

It is also possible to create with this application or M365 Copilot so-called “agents” to perform specific tasks, depending on your needs. M365 Copilot agents allow you to precisely define source materials, configure the agent with a prompt, add actions and autonomous functions.

Example applications: facilitating access to information made available by the legal department to the company’s employees, automatically preparing the first version of the bulletin on changes in legislation and parliamentary discussions of the previous week, identifying and evaluating specific clauses in contracts, or creating agents specialized in a specific issue used to deepen the knowledge of employees and prepare for meetings.⁵

2.3. ASSISTANTS RELYING ON SHARED AI MODELS

AI assistants are AI-based tools that use large language models to interpret natural language, carry out conversations and perform tasks. They support users in natural language processing tasks across various applications and systems. Examples include chatbots on websites.

⁵ Examples of using M365 Copilot Agents in Microsoft’s legal department: Specialized agent for DORA Regulation materials: https://www.linkedin.com/posts/jeff-bullwinkel-a01a259_microsoftcopilot-genai-dora-activity-7285213763962568705-7LYv; Preparation of Regulation newsletter: https://www.linkedin.com/posts/activity-7289592679540174848-o-75?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAgtOMB9bZ4-CaP-cH3AcYwKF57_IBX5Q; Facilitating access to information provided by the legal department: <https://www.microsoft.com/insidetrack/blog/boosting-efficiency-with-sharepoint-agents-how-our-microsoft-legal-team-is-helping-clients-find-answers-faster/>.

2.4. FINE-TUNED MODELS

Fine-tuned models are advanced AI tools that are customized to meet your specific needs through additional training on your data. Fine-tuning involves adapting a previously trained AI model to specific tasks or new data sets (such as contracts). This makes the model more precise and tailored to specific customer requirements.

3. Basic concepts – generating and using (training) data

3.1. DATA GENERATION

Below are key concepts in this area:

- **Prompt** – user-directed command to initiate output content creation in large language models and generative AI.
- **Meta prompt** – is a system-applied prompt (coded instructions) that applies to each prompt sent (“prompt for prompt”). A prompt for a service to generate output data, e.g. “be creative” or “be strict.”
- **Grounding** – is the addition of context to the input data to increase the relevance of the output data (e.g. taking additional information from customer resources, from the Internet, from other services).
- **Input data / input content** – is the input information for the generative AI system (e.g. text, image, or sound). It is a command that the user provides to the generative AI system to generate a response (output). A prompt is a specific example of input data that applies to large language models and generative AI.
- **Output data / output content** – is the outcome created by the AI system as a result of input processing. It can take various forms, for example, text, images, sounds or decisions.

3.2. TRAINING AI MODELS

As we indicated above, creating an AI model requires that it learns from data. Using standard solutions, an attorney-at-law will usually not be involved in the process of training AI models. However, when creating so-called fine-tuned models, the attorney-at-law may already be involved in the process, including providing data to better train the model. Content from attorneys-at-law and

trainees attorney-at-law on the Internet is frequently used to train models, evidenced by links to data sources in generated output.

The possibility of training models, especially on copyrighted data, is controversial. The following legal grounds for such activities are indicated:

- **Text and data mining (TDM)** refers to an automated analytical technique for analyzing text and digital data to generate information including patterns, trends and correlations.
- As part of an amendment to copyright law, implementing Article 4(3) of Directive 2019/790 of the European Parliament and of the Council (EU) of April 17, 2019 copyright and related rights in the digital single market and amending Directive 96/9/EC and 2001/29/EC, **a new type of permitted use in the form of text and data mining (TDM)** was introduced in Article 26³(1) of the Act on Copyright and Related Rights. This provision allows users to reproduce already distributed works for content and data analysis unless the right holder has stipulated otherwise (opt-out clause). For works accessible to the public at any time and place of their choosing, the disclaimer is provided in machine-readable format. However, the lack of clear guidelines on the methods and means of making a disclaimer and the lack of a technical standard for making a disclaimer currently creates a sense of inability to make a viable use of the opt-out. It is unclear when a disclaimer can be made (before exploration begins or, for example, while the AI model is already in operation) and how it should be done to be effective.

Article 53(1)(c) of the AI Act requires manufacturers of general-purpose AI models to comply with European copyright standards during the process of training AI models, including adhering to the opt-out clause.

- **The fair use principle** is a concept developed under U.S. law that allows the use of a copyrighted work without the need to obtain permission from the eligible entity (author, publisher/producer) under certain conditions, such as for research, education, or criticism. The use of this exception to train AI models is under disputes in the US.

3.3. TIPS FOR PROMPTING



APPENDIX NO. 1

In **Appendix no. 1** of the Recommendation, you will find practical tips for proper prompting.

4. AI vs. cloud computing

Cloud computing is a customer-provided digital service that enables ubiquitous on-demand network access to a shared set of configurable, scalable and flexible computing resources of a centralized, distributed or highly distributed nature that can be rapidly allocated and released with minimal effort in terms of management or interaction with the service provider (“data service” in the Data Act).⁶

Cloud computing thus allows access via the Internet, with minimal interaction with the service provider to specific computing resources. The basic models of cloud services are platform as a service (PaaS), infrastructure as a service (IaaS) or software as a service (SaaS).

Cloud computing plays a key role in developing and implementing AI tools. With cloud computing, organizations can evaluate and use advanced AI tools without investing in expensive infrastructure (to install or train models in their own data centers) and without lengthy implementations. For standard tools (e.g. M365 Copilot), the service can be fully available to the user, at most, a few hours after ordering.

The cloud computing service also facilitates the process of training or fine-tuning AI models. This often requires significant computing power to process and analyze large amounts of data.

Analyses conducted by attorneys-at-law for cloud computing can be applied when implementing cloud computing-based AI tools. Previous analyses should only be supplemented with specific requirements related to AI tools, as described in these Recommendations, which will significantly speed up and simplify the entire implementation process.

5. Examples of applications of generative AI tools in the work of an attorney-at-law

5.1. IN EVERYDAY WORK OF AN ATTORNEY-AT-LAW

AI tools can be utilized in nearly every aspect of an attorney-at-law’s work to:

- analyze or compare documents, prepare document summaries or document templates;

⁶ Article 2 (8) Regulation (EU) 2023/2854 of the European Parliament and of the Council of December 13, 2023 (Data Act).

Section I

- support in managing the email inbox and communication with clients;
- create transcriptions of video conferences;
- create presentations;
- translate text and presentations;
- analyze arguments and counterarguments;
- prepare offers and communicating with clients (e.g. preparing periodic case reports);
- automatically create summaries and categorize documents for databases; and
- find information relevant to a particular issue in internal and external sources.

It is worth remembering that AI solutions can be particularly important support for attorneys-at-law practicing alone or in smaller teams, using these tools can make it easier for them to quickly increase the quality of their services and customer service.

5.2. DETAILED EXAMPLES OF THE APPLICATION OF GENERATIVE AI TOOLS



APPENDIX NO. 2

In **Appendix no. 2** of the Recommendation, you will find detailed examples of the application (using Microsoft 365 Copilot as an example) of generative AI tools in the work of attorney-at-law.

PROVISIONS OF LAW – BASIC REGULATIONS



Attorneys-at-law using AI tools is subject to both general laws, such as data protection or copyright laws, and laws that regulate the practice of the profession, including protecting professional secrecy.

1. Personal data

From the point of view of data protection law, an attorney-at-law – depending on the form of practice of the profession – may have the status of a data controller (an entity that decides on the purposes and means of data processing), or will act under the authority of the controller referred to in Article 29 of the GDPR and in accordance with the controller’s instructions. If an attorney-at-law practices their profession in the form of a Law Firm of Attorney-at-Law / the attorney-at-law is the controller of the personal data processed during their profession. If an attorney-at-law practices the profession in a partnership, civil partnership, based on an employment relationship or under a civil law contract, the data controller is either the partnership or the employer, and the attorney-at-law processes the personal data under the authority of the controller and in accordance with the controller’s instructions.

General regulations on the processing of personal data, including the provisions of the GDPR⁷ or sector regulations, apply to using AI tools. The scope of the application of these regulations will depend on whether the attorney-at-law engages in creating and training the AI model (or adjusting it – *fine tuning*) using information containing personal data, or is a user of the AI system.

In the case of construction and training, an attorney-at-law will have more responsibilities, including, first and foremost, properly identifying the legal basis for processing the personal data contained in the training data. A detailed

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Section II

explanation of how the GDPR is applied at this stage can be found in the Opinion of the European Data Protection Board (“EDPB”) on certain data protection aspects of processing personal data in the context of AI models.⁸

In practice, however, the attorney-at-law will most often be a user of the AI system. In such a situation, personal data processing can potentially occur at three levels:

- processing personal data contained in the input content (prompt);
- processing personal data contained in the output content (output); and
- processing user data when using the AI model (e.g. what services are used, when, and for how long).

1.1. PROCESSING PERSONAL DATA IN THE INPUT CONTENT

If an attorney-at-law wants to process personal data in the input content, they should, as the controller or a person authorized by the controller, verify that they have an appropriate legal basis for such processing and what the purpose of the processing is.

Additional data processing regulations should also be examined, such as:

- their adequacy;
- securing confidentiality;
- issues of data transfer to third countries, i.e. whether data will be transferred outside the European Economic Area (EEA);
- whether it is necessary to enter into a data processing agreement (it is necessary to analyze in which role the AI system provider is acting – in the role of controller or joint controllers or in the role of processing entity);
- whether a Data Protection Impact Assessment (DPIA) is required;
- whether the realization of data subject’s rights is ensured;
- the necessity and extent of updating internal documentation, including records of processing activities and privacy policies, must be evaluated;
- furthermore, for personal data protected by attorney-client privilege, it is essential to ascertain whether such data can be included in the input content (refer to [Section II.7](#)).

⁸ European Data Protection Board Opinion 28/2024 on Certain Data Protection Aspects of the Processing of Personal Data in the Context of Artificial Intelligence Models, 17 December 2024 Opinion available here: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl.

Section II

1.2. PROCESSING PERSONAL DATA CONTAINED IN THE OUTPUT CONTENT

Attorneys-at-law should note that personal data in the output is based on statistical predictions and may be inaccurate. For example, the generated data may be “made up” in part or in whole (so-called hallucinations, see [Section III.3](#)). The attorney-at-law should consider that personal data might be inaccurate what could impact decisions based on it. Failure to do so with “limited confidence” in the personal data generated, may mean that the data processing does not comply with the principle of fairness. Uncritical reliance on such data may also be incompatible with the principle of data minimization as personal data, including applications, must be relevant and appropriate to the purpose.⁹

Some commentators propose that AI-generated data might be classified as statistical forecasts rather than personal information. Proponents of this approach argue that because AI generates data based on patterns and probability rules derived from large data sets, the output data is more like statistical forecasts than personal data. This thesis is controversial. The primary concern is whether AI-generated data can be associated with an identifiable individual. In such case, the data can be considered personal data, even if it is inaccurate. EDPB’s opinion confirms that this will be particularly true if the AI is to provide conclusions (e.g. personal data) about individuals whose personal information was used for training.¹⁰

1.3. PROCESSING USERS’ PERSONAL DATA, INCLUDING REGARDING THEIR INTERACTION WITH THE AI SYSTEM

Attorneys-at-law should bear in mind that AI may also collect its own personal data and that of other users including data such as, name, surname, username, contact information; and in addition, input content, output content, and so-called user engagement data, e.g. pseudonymized identifiers randomly assigned

⁹ Information Commissioner’s Office publication: How to use AI and personal data appropriately and lawfully, p. 9, <https://ico.org.uk/media2/migrated/4022261/how-to-use-ai-and-personal-data.pdf>

¹⁰ European Data Protection Board Opinion 28/2024 on Certain Data Protection Aspects of the Processing of Personal Data in the Context of Artificial Intelligence Models, December 17, 2024, paragraphs 29, 36-37; Opinion available here: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl.

to the user, usage time, activity history, encryption information, error information. This data is typically encrypted and sometimes users can delete it themselves. The input and output content is typically used for providing the service and not stored, though it may be temporarily kept in the application's memory until cleanup occurs.

The controller of user data may be either the attorney-at-law or the company/employer, depending on the form of practice, while the AI system provider usually process user data as a processing entity. An AI system provider may also be a data controller if, for example, it processes data to improve the AI system's performance, conducts research, or detect abuse – this will typically involve processing input and output content and user engagement data. To determine the role of the provider, it is necessary to review the contractual documentation for using the AI system.



RECOMMENDATIONS

Recommendations **7** and **8** contain specific suggestions on this matter.

2. AI Act

The AI Act entered into force on 1 August 2024. Most provisions will apply from 2 August 2026. From 2 February 2025, the general provisions, the provisions on prohibited practices, and the provisions on AI literacy (Article 4) are applied. As of 2 August 2025, provisions on AI Act supervisory authorities, penalties for violations, and management rules and responsibilities for general-purpose AI models will begin to apply. As of 2 August 2026, the AI Act will be mostly applicable – regulations on high-risk systems will begin to apply, including in recruitment, finance, or critical infrastructure management. The regulations on high-risk AI systems referred to in Article 6(1) of the AI Act will apply from 2 August 2027.

The AI Act imposes obligations on various entities involved in developing, implementing, and using AI systems. The AI Act also applies to various entities: providers of AI systems,¹¹ importers, distributors, authorized representatives

¹¹ An entity that develops an AI system or general-purpose AI model, or commissions the development of an AI system or general-purpose AI model, and that, whether for a fee or free of charge, markets or puts into service an AI system under its own name or its own trademark (Article 3(3) of the AI Act).

Section II

and deployers.¹² Most of the responsibilities lie with AI system providers, while the delineation of these roles for some AI systems, such as embedded or fine-tuned systems, may require deeper analysis.

As a rule, attorneys-at-law will be entities using AI systems. AI system deployers have limited obligations unless they use general-purpose AI classified as high-risk.

When using high-risk AI systems, attorneys-at-law may have additional obligations, including those indicated in Articles 26 and 27 of the AI Act, such as the obligation to implement technical and organizational measures to enable use in accordance with the user's manual or to conduct an impact assessment of the AI system. In addition, if a deployer changes the purpose of an "ordinary" AI system so that it becomes a high-risk AI system, it will also become a provider of that system under the AI Act, making the obligations of a provider of a high-risk AI system applicable to it (Article 25(1)(3) of the AI Act).

Above all, the deployer has obligations to build AI literacy (Article 4 of the AI Act), considering their technical knowledge, experience, education and training, and the context in which the AI systems are to be used, as well as considering the individuals or groups of individuals against whom the AI systems are to be used. In addition, the deployer has transparency obligations under Article 50 of the AI Act in certain cases, which include, among other things, the need to inform people about interacting with AI systems or the generation or modification of so-called deepfake. Further, where the AI system is used to generate graphics, audio, video and text material, the obligation to design the AI system so that it automatically marks the generated material as artificially generated or manipulated. A contracting authority may not use a general-purpose AI system to implement prohibited AI practices (Article 5 of the AI Act).

National AI regulations aim, among other things, to ensure AI implementation and supervision at the national level.

3. Copyrights

Polish copyright law recognizes only human beings as creators, and copyright protection is granted to a work, i.e. any manifestation of creative activity of an individual character, established in any form, regardless of value, purpose and

¹² An entity that uses an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity (Article 3(4) of the AI Act).

manner of expression.¹³ However, not every manifestation of human activity is considered a work. For example, legal acts and their official drafts, discoveries, ideas, procedures, methods and principles of operation, and mathematical concepts are not copyrightable works (Article 4 of the Act).

Legal and copyright issues in the context of AI primarily concern the following areas:

- the basis for using AI systems (e.g. under a license);
- model training and possible claims against users for model training on copyrighted data;
- input content rights; and
- rights to the output content and the ability to use it.

3.1. BASICS FOR USING AI SYSTEMS

As defined in the AI Act, an AI system is a machine system that includes a software component and the hardware on which such software runs. As a result, we apply analogous rules to contracts for using AI solutions like those for software. Typically, AI systems are offered under licenses, such as subscription licenses for those provided through the software-as-a-service (SaaS) model.

License agreements govern specific issues related to AI solutions, such as:

- obligations of the deployer, including the need to comply with the principles of responsible use of AI;
- input and output content rules;
- commitments by providers on using output and input content (e.g. regarding rules for using this data to train their models);
- restrictions on use, e.g. filtering input and output content, possibility of human verification, possibility of limiting or disabling access to AI systems;
- responsibility for claims on AI system and output content.

3.2. AI MODEL TRAINING AND CLAIMS RELATED TO MODEL TRAINING

As the question of whether models can be trained on copyrighted data under the aforementioned exemptions (see [Section I.3.2](#)) is not yet settled, contracts

¹³ Article 1(1) of the Law on Copyright and Related Rights.

Section II

for using AI systems may also regulate the provider's liability to the user in the event of such claims by third parties (e.g. authors of training data) raised against the user, such as claims for abandonment of use or compensation for infringing their copyrights.

3.3. RIGHTS TO INPUT CONTENT

Human-created input can be considered a work (e.g. fragments of computer code inserted into a prompt). Furthermore, prompts often encompass complete documents or images that may be protected by intellectual property rights. It is necessary to determine whether using such content in this way will not infringe on third-party copyrights.

3.4. RIGHTS TO OUTPUT CONTENT

In Poland, AI-generated content is not considered a work and thus is not protected by copyright, as only human activity is subject to such protection. However, the difference between human-generated output **using AI** and **AI-generated** output is emphasized.¹⁴ When AI is used solely as a tool to assist the author in the creation process, copyright protection of the results of such creativity is potentially possible (analogous to the digital processing of photographs). In addition, in the case of human reworking of the output content in such a way that the result meets the criteria of a work, such reworking can potentially be the subject of copyright protection.

Video or audio output may be protected under related rights, specifically video and phonogram rights.

4. General regulations on contractual relations

Applicable general regulations on contractual relations, such as the Civil Code in the case of contracts governed by Polish law, will also apply to using AI tools. In this respect, the provisions on liability for non-performance or improper performance of a contract, for example, will apply.

¹⁴ European Parliament resolution of 20 October 2020 on intellectual property rights in the development of artificial intelligence technologies (2020/2015 (INI)).

5. Liability for defective products

The new **Directive** of the European Parliament and of the Council (EU) 2024/2853 of 23 October 2024 **on liability for defective products** and repealing Council Directive 85/374/EEC, which entered into force on 8 December 2024, and should be implemented in the Polish legal order by 9 December 2026, extends liability for defective products in relations with consumers to digital products (software, including software provided in the SaaS model) or data, when compared to the existing legislation. The provisions implementing the Directive may find application in the case of, for example, attorneys-at-law offering AI chatbots to consumer clients.

6. Cyber Security

AI systems are machine systems and, as a result, are susceptible to cyber threats. The most important Polish act in the field of cyber security is the currently amended **Act on the National Cyber Security System**,¹⁵ which is tasked with implementing the provisions of the NIS-2 Directive into Polish law.¹⁶ According to the NIS-2 Directive, the previous division into essential service operators and digital service providers has been replaced by a division into essential entities and important entities, while imposing a number of new obligations on them. More industries will need to implement these provisions. This will be important especially for attorneys-at-law using AI systems within companies in these industries.

Among the most important obligations imposed on essential and important entities are the obligations to put in place appropriate technical, operational and organizational measures to manage security risks to the networks and information systems these entities use to conduct operations or provide services, and to prevent the impact of incidents on the recipients of their services, including

¹⁵ The bill is available here: <https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055217-#13055217>.

¹⁶ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security within the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS Directive 2). The directive should be implemented in the Polish legal order by 17 October 2024.

Section II

ensuring the security and continuity of the supply chain of ICT products, ICT services and ICT processes on which the provision of the service depends.¹⁷

AI systems may be subject to AI-specific risks (see III.). According to the AI Act, high-risk AI systems must be designed and developed to achieve suitable levels of accuracy, robustness, and cybersecurity, and to perform reliably in these aspects throughout their lifecycle.¹⁸

In addition to the NIS-2 Directive, sector-specific regulations may be applicable in certain instances, such as the **DORA Regulation**,¹⁹ which aims to make the financial sector more resilient to cyber-attacks and other technological threats. This regulation introduces new digital security requirements for financial institutions and their IT service providers. In contrast, the **CER Directive**²⁰ is designed to increase critical entities' resilience to incidents (events) that can significantly disrupt the provision of a critical service, including when they affect national systems that protect the rule of law, such as natural disasters, terrorist attacks, insider threats or sabotage.

7. Regulations for attorneys-at-law

An attorney-at-law is obliged to keep secret what they have learned when providing legal assistance,²¹ i.e. all information concerning the client and their affairs, disclosed to the attorney-at-law by the client or otherwise obtained when performing professional activities, regardless of the source of such information and the form and manner of its recording (professional secrecy). Professional secrecy also extends to all documents the attorney-at-law creates, and the attorney-at-law's correspondence with the client and people involved in the case that is created to provide legal assistance.²²

¹⁷ Article 8 of the draft law on the national cyber security system.

¹⁹ Regulation (EU) 2022/2554 of the European Parliament and of the Council 14 December 2022 on the operational digital resilience of the financial sector and amending Regulations (EC) No1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011. The regulation is effective as of January 17, 2025.

²⁰ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. The CER Directive should be implemented in the Polish legal order by 17 October 2024.

²¹ Article 3(3) of the Law of 6 July 1982 on attorneys-at-law.

²² Article 15 of the Code of Ethics for Attorney-at-law.

Section II

Maintaining professional secrecy is an attorney-at-law's duty.²³ An attorney-at-law is obliged to protect any information covered by professional secrecy from unauthorized disclosure²⁴ in a manner adequate to the nature, type and scale of their activity, environment and the type of information constituting professional secrecy and the risk of its disclosure.²⁵ An attorney-at-law must perform professional activities conscientiously and with due diligence considering the professional nature of the activity.²⁶

The obligation to respect professional secrecy implies the need for an attorney-at-law to provide appropriate technical and organizational measures to safeguard against disclosure. An attorney-at-law should exercise the due diligence required of a professional in providing a secure AI tool, including by selecting a dependable AI tool provider, as well as considering whether they should take additional measures in the client relationship.



RECOMMENDATIONS

The attorney-at-law's regulations are addressed in Recommendations **2, 4, 8, 12, 16** and **22**.

8. Criminal proceedings

An attorney-at-law is required to keep confidential the details of pre-trial proceedings and court hearings conducted privately. Article 241 §1 of the Criminal Code states that information obtained during criminal proceedings is protected and cannot be publicly shared without authorization before being disclosed in court. Unauthorized dissemination of such information is subject to penalties. Likewise, public dissemination of news from a court hearing held in camera is prohibited and is subject to a penalty.

²³ Article 9 of the Code of Ethics for Attorney-at-law.

²⁴ Article 23 of the Code of Ethics for Attorney-at-law.

²⁵ Par. 3 of the Rules of Practice for Attorneys-at-law .

²⁶ Article 12 of the Code of Ethics for Attorney-at-law.

USE OF AI TOOLS BY LAWYERS – BENEFITS, CHALLENGES, AND RISKS



AI offers many benefits, but it also comes with certain challenges and can generate certain risks. The risks associated with using AI tools are not specific to the legal industry but are general in nature. Proper regulation, transparency, and regular monitoring of AI systems’ performance can mitigate and minimize these issues.



RECOMMENDATIONS

Ways to mitigate the risks associated with using AI tools are included in the Recommendations ([Section V](#)).

1. Benefits

The most cited benefits of using AI tools include:

- **Increasing competitiveness:** Attorneys-at-law who use AI tools in their daily work can serve clients faster and more efficiently, allowing them to stand out in the market and attract new clients. The use of modern technology can also attract clients to look for innovative and cutting-edge legal solutions.
- **Saving time and accelerating legal processes in the organization:** AI tools can significantly reduce the time required for certain projects and processes. AI tools can significantly ease the burden on the legal department by allowing the legal department to prepare information more efficiently for internal clients regarding routine issues, processes and policies.

As a result, attorneys-at-law can more quickly prepare first drafts of documents, prepare summaries, search databases, and analyze large amounts

Section III

of information, allowing for more efficient case management. Therefore, companies employing attorneys-at-law can serve more clients in less time, making them more efficient and competitive in the market.

- **Improving the quality of work:** AI not only speeds up an attorney-at-law's work, but also reduces the risk of human error translating into a higher quality of legal services. It also makes it possible to improve communication between an attorney-at-law and clients (legal language becomes clearer).
- **Automating Routine Legal Tasks to Aid Lawyers:** AI tools are capable of automating various time-consuming tasks, including document analysis and information retrieval. By automating routine tasks, lawyers can focus on more complex and strategic aspects of their work, increasing their efficiency and professional satisfaction.

2. Challenges

The most cited challenges in using AI tools include:

- **Protecting confidentiality and professional secrecy:** Using AI tools incorrectly, including those that do not guarantee confidentiality or permit AI models to be trained on input and output content, can risk the disclosure of professional secrets and data.
- **Adapting to AI-induced changes:** Standard tools available on the market already allow the generation of materials whose quality often matches the work product of younger lawyers at a much lower cost and faster. Therefore, lawyers face the challenge of how to train younger lawyers. Moreover, the demand for younger lawyers may be less than it is today. AI may also force a change in client billing and reduce demand for legal services, especially those with little added value (e.g. simple contracts, analysis).
- **Copyright Considerations:** The permissibility and conditions for training AI models on copyrighted material are subject to debate, which creates a lack of legal clarity for users. Attorneys-at-law should anticipate that similar prompts will produce similar or identical responses for multiple users. It is essential to consider the manner in which AI-generated materials are disseminated to others, including clients.
- **Liability:** Liability for using AI solutions can be considered on several levels which requires analysis and appropriate regulation. The deployer

Section III

may incur administrative liability under the AI Act or the GDPR, including being liable to pay financial penalties to regulators if they breach these regulations. The contract for using AI systems will govern liability in **the provider-ordering party** relationship (e.g. an attorney-at-law or law firm). According to market standards, most often the provider's liability, both under contract and in tort, is contractually limited, e.g. in amount to the provider's remuneration, or excluded, e.g. with respect to the deployer's lost profits. From the perspective of the deployer, it is crucial to use the AI system in accordance with the instructions and its intended use. The legal services contract and the regulations for attorneys-at-law will apply to liability in the **AI-applying attorney-at-law-client** relationship. At this level, attorneys-at-law may also introduce limitations on their liability indicated above, but they should also consider informing the client that part of their work has been generated by the AI system, e.g. this may include an illustration for a legal opinion, or an excerpt or element of a presentation. This matter is important from a copyright perspective (refer to [Section II.3](#) above) because such a portion of the work may not be copyrighted or might have been independently created by another individual. Thus, the failure to provide adequate information could at the very least jeopardize the attorney-at-law's reputation if the client arrives at a similar work. Attorneys-at-law may also face disciplinary and criminal liability for violating professional secrets.

- **Liability to third parties** which on general principles may arise under the Civil Code (tort liability), liability for property and non-property damage suffered by an individual for processing their personal data in violation of the regulations (Article 82 of the GDPR), or liability to customers under the Defective Products Liability Directive (see [Section II.5](#) above), cannot be excluded either.
- **Distinguishing AI-generated** content from original content: Given the ease of manipulating materials with AI, assessing the authenticity of evidence or content becomes challenging. Regardless of AI being used in legal practice, it will be necessary to implement solutions to identify AI-generated or AI-modified materials as part of the procedure for evaluating evidence to avoid relying on evidence that is false but generated by AI (e.g. a deepfake with a photo of a damaged object presented as evidence in proceedings for payment of an insurance contract claim). The lack of uniform standards for marking AI-modified content poses a challenge to current efforts.

3. Risks

The use of AI tools, like any technology, can involve risks. The most cited risks of using AI tools include:

- **Hallucination risk**²⁷ – this refers to situations in which AI systems generate results that are inaccurate, outdated, out of context or even false and without basis. One of the causes of hallucinations is imperfect training data. If the training data set is incomplete or loaded with biases, the system learns incorrect correlations and patterns, leading to producing false content. Another cause of hallucinations can be so-called model overfitting, a situation where the algorithm matches the training data set too precisely. As a result, the model loses the ability to generalize and correctly recognize new, previously unknown patterns.
- **Risk of Overreliance on AI**²⁸ – this refers to the situation in which a person using AI tools relies excessively or exclusively on the results generated through AI which can lead to the loss of certain competencies, one’s own intuition, expertise, critical thinking ability or independent problem solving. Additionally, AI often acts as a “black box” and there is a lack of clear information regarding its operation (risk of lack of transparency). This means that users do not have a full understanding of AI’s decision-making processes. Overusing AI can also lead to the loss of human competence realized by AI.
- **Discrimination risk (bias)** – this involves replicating patterns expressed in training data. If the training data contains historical biases or reflects social inequalities, the algorithm may learn these biases and will replicate them, resulting in biased or discriminatory decisions by AI. AI results will also be incorrect if the training data is not sufficiently diverse. For example, if the datasets used to train the AI model do not include

²⁷ An example of AI hallucination can be seen in the case of American lawyers who used ChatGPT to prepare a pleading. As it turned out, AI included fictitious quotes from court decisions and non-existent legal precedents in the letter. The lawyers claimed that they were unaware of ChatGPT’s ability to generate false information. The court fined the lawyers \$5,000. https://storage.courtlistener.com/recap/gov.uscourts.nysd.575368/gov.uscourts.nysd.575368.54.0_3.pdf.

²⁸ Examples of over-reliance on AI include: (i) developers’ use of AI tools (e.g. GitHub Copilot) to generate code; or (ii) recruiters’ use of AI to check candidates’ resumes and the subsequent failure of the recruiter to verify resumes selected by AI when candidates hide “employment” commands (commands written in white font) in the text.

sufficiently diverse demographic groups, the system may perform less accurately for those groups.²⁹

- **Risk of disclosing confidential / secret information** – this refers to the situation where a person using AI tools places information that is confidential or secret in the input content, in a situation where there are no contractual or technical safeguards against the disclosure of this information. Such actions can lead to violations of applicable laws (e.g. on protecting professional secrecy) or contractual provisions obliging to keep certain information confidential. They can also result in severe damage, for example, if the data of an invention is disclosed before it is filed for patent protection, making it impossible to obtain patent protection.
- **Risk of lack of timeliness** – this concerns static models that are not updated after the training process and, consequently, do not contain information about the latest rulings, events or cases. As a result, the results generated may be erroneous or incomplete.
- **Legal and reputational risks** – this may involve client claims of violating professional secrecy or third-party claims of infringing proprietary copyrights in connection with using AI systems trained on such data without the authorized party's consent. Complying with the law and protecting client interests are of utmost importance to lawyers, and often the mere rise of allegations of such violations can lead to a loss of client confidence.
- **Cyber risks (e.g. identified by the Open Worldwide Application Security Project – OWASP)³⁰** – this refers to specific AI-related security risks being identified, such as: altering prompts to influence generated responses (*prompt injection*); poisoning (altering) data used to train AI models (*training data poisoning*); and failing to verify output for potential vulnerabilities. OWASP has outlined various methods to mitigate the identified risks.
- **Risk of blocking access to services based on the terms and conditions of a particular provider** – this refers to situations where a particular provider may block a client's access to a service in certain situations

²⁹ Examples include: (i) an algorithm using AI for recruitment that discriminated against women <https://businessinsider.com.pl/firmy/strategie/amazon-zrezygnowal-z-algorytmow-w-rekrutacji-dyskryminowaly-kobiety/pp233ev>; or (ii) a facial recognition system that was trained primarily on photos of light-skinned people may have difficulty correctly recognizing the faces of darker-skinned people, leading to unfair and discriminatory results.

³⁰ <https://owasp.org/www-project-top-10-for-large-language-model-applications/>

Section III

(e.g. violations of permitted use rules specified in the contract). In such cases, switching to another provider usually requires paying additional fees – a minor risk for the legal profession at this stage of AI implementation.

FOREIGN BAR ASSOCIATIONS' GUIDELINES ON USING AI TOOLS



Foreign bar associations encourage lawyers to stay abreast of technological changes relevant to their practice, including solutions based on generative AI.³¹ According to the guidelines/recommendations of these associations, lawyers should understand these changes and their consequences although they do not have to be AI experts. They should, however, understand the opportunities afforded by using AI tools, the legal implications of their use, and the limitations of these technologies. At the same time, lawyers should use AI tools responsibly and in accordance with the rules of the profession.

Recommendations and guidelines worth noting are:

- Formal Opinion 512 of the American Bar Association (ABA) (29.07.2024);³²
- The Future is Now. Artificial Intelligence and Legal Profession; International Bar Association (IBA) (19.09.2024);³³
- European lawyers in the era of Chat GPT, FBE, Guidelines 2.0, 09.2024;³⁴ and
- The Law Society (LS) Guide (11.2023 – updated: August 2024).³⁵

In addition to considering issues of professional secrecy and confidentiality, the aforementioned recommendations and guidelines examine issues of informing clients about using AI tools, cases where obtaining client consent to use generative AI tools will be necessary, issues of verifying source materials used by the AI tool, or issues of billing clients in connection with using AI tools.

³¹ The International Bar Association's report "Future of Legal Services - White Paper 2024" (2024) shows that many lawyers still view AI as a "problem for next year" and not one that requires priority attention. However, there is an apparent increase in lawyers' interest in AI challenges. Lawyers see the need to focus on AI issues especially in the areas of change management and staff training to respond to upcoming challenges (first on the list). Implementing AI to improve the delivery of legal services was also identified by lawyers as an area of concern (second on the list).

³² https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf

³³ <https://www.ibanet.org/document?id=The-future-is%20now-AI-and-the-legal-profession-report>

³⁴ <https://www.fbe.org/nt-commission-guidelines-on-generative-ai/>

³⁵ <https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials>

RECOMMENDATIONS



A. Recommendations for preparing to use AI tools

RECOMMENDATION 1: DETERMINE THE PURPOSES IN WHICH THE ATTORNEY-AT-LAW WILL USE THE AI TOOL

Why: Identifying purposes for which an attorney-at-law will use an AI tool is crucial for several reasons: (i) it will allow an AI tool to be selected that addresses the attorney-at-law's specific needs (e.g. universal, specialized for litigation); (ii) it will identify the regulations that need to be taken into account to ensure lawful use of the AI tool, including ensuring appropriate security and data protection measures (e.g. whether the intended purpose of use does not constitute a prohibited practice or high-risk system); and (iii) it will allow the best cost-effective solution to be selected.

How: An attorney-at-law should identify the areas where AI can bring the most benefit to their work, e.g. improve the speed or quality of work or provide new opportunities. The attorney-at-law should therefore answer the question of why they want to use AI tools. Do they need support in preparing draft proposals, emails, calendar management, or meeting transcriptions? Or do they need a tool for drafting contracts and analyzing court cases?

Answering these types of questions will help identify why an attorney-at-law will want to use an AI tool, and consequently, selecting an appropriate AI tool and its provider.



RECOMMENDATION: Before selecting an AI tool, identify the purposes in which the attorney-at-law wants to use AI in their work (e.g. universal or more specialized support).

RECOMMENDATION 2: IDENTIFY THE INFORMATION UTILIZED BY THE AI TOOL, ASSESS THE QUALITY OF THAT INFORMATION, AND UNDERSTAND ITS PROCESSING METHOD, INCLUDING HOW THE AI TOOL OPERATES (E.G. WHETHER IT IS A CLOUD-BASED SOLUTION, WHETHER AND HOW IT FILTERS INPUT AND OUTPUT CONTENT)

Why: When choosing the right AI tool, it is important to determine how the AI tool works, specifically:

- how the data contained in the prompt is processed, including whether this input/output data is subject to grounding and, if so, how (e.g. whether data from the Internet is also obtained or only data in certain internal resources of the attorney-at-law) → a mere connection to the Internet or other systems does not necessarily increase the risk; ideally, the attorney-at-law should be able to choose and limit such grounding;
- in certain systems, the extent to which prompt and output data is filtered varies. Additionally, both the filtered input and output content may be stored for human verification purposes;
- where the input and output content is transmitted and processed, where the AI model is located (EEA, vendor, or third-party infrastructure). The AI system may be in the IT infrastructure (e.g. on servers) of the attorney-at-law or their organization (on-premises) – but, in practice, this will be an extremely rare situation. In most cases, AI tools are provided in a cloud service, and use will be based on a prepared application (SaaS model). Some providers of AI systems used for business purposes declare that the input and output content is not stored in the AI model’s memory, their processing is done only in real time, and the storage in the application’s memory is only temporary, until the application runs the memory cleaning function.

The above information is necessary to assess the compliance of such a solution with regulations (e.g. on protecting personal data or maintaining the attorney-at-law’s confidentiality) and for making a risk assessment.

How: An attorney-at-law should review the contract for using a particular AI tool, along with related technical documentation the AI tool provider provides (e.g. on websites), in particular:

- rules for processing data contained in output and input content (e.g. whether this information is utilized for model training and what security responsibilities are associated with the AI tool);
- information on how the data is processed (e.g. whether the processing takes place only within the EEA or also outside the EEA; if the data is processed outside the EEA, what mechanisms apply to the transfer of data; whether the solution provider is a processing entity or (joint)controller).

The attorney-at-law should also verify how the AI tool works from the technical side, e.g. in the instructions or materials available on the AI provider's website.

The attorney-at-law can also enlist the help of a developer or technology partner in this regard.



RECOMMENDATION: Before choosing an AI tool, it is important to review contractual and technical documentation to understand the rules for processing information in input and output content, including the establishment of data flows.

RECOMMENDATION 3: ESTABLISH A PROPER CONTRACT FOR USING THE AI TOOL

Why: Determining which contract, including which version of the contract, will apply to using a particular AI tool is important to accurately identify the AI tool provider and the terms of use of the AI tool. In practice, a contract may include several documents (e.g. the main provisions of contracts, licensing provisions or product use rights, and data protection provisions). It is therefore necessary to collect these documents so that the attorney-at-law can be sure that it is a complete agreement. In addition, especially in the case of larger contracts and entities, framework agreements may already be in place and the version that will apply must be determined. We may face such a situation, in particular, if the AI tool is one of the products offered as part of the cloud services of a given provider.

How: The attorney-at-law should first identify the provider of the AI tool in question. Then identify the relevant contract and terms and conditions applicable to the AI solution under consideration. The provider's websites that host technical information, security information (e.g. audit results) and training can also be helpful.



RECOMMENDATION: Before selecting an AI tool, it is necessary to verify what contract (including what version of the contract) will apply to using the AI tool in question, and to determine all the documents that make up the contract (including processing entrustment agreements, product use rights, etc.).

RECOMMENDATION 4: ASSESS WHETHER AND HOW THE CONFIDENTIALITY OF INPUT AND OUTPUT CONTENT, INCLUDING PROFESSIONAL SECRECY, IS ADDRESSED IN THE CONTRACT WITH THE AI TOOL PROVIDER

Why: Determining whether and how the confidentiality of input content and output content (including professional secrecy) is ensured is important because, in the absence of adequate contractual or technical safeguards against the disclosure of this information, generally applicable laws may be breached, including those relating to protecting professional secrecy, or provisions of a contract obligating the user to keep certain information confidential.

How: The attorney-at-law should review the contract for using a specific AI tool along with the related documentation provided by the AI tool provider in this regard and, in particular, verify:

- ownership of the input and output content (e.g. whether the user retains the right to such data or transfers it to the provider) → as a general rule, the attorney-at-law should not use tools that transfer rights to the data contained in the output or input content to third parties, this is especially true for tools used to process client data;
- confidentiality obligations for input and output content and other client data (e.g. whether, as part of filtering, such content is additionally stored by the provider for verification by a provider employee) → consider whether confidentiality obligations are sufficient and whether modifications are required (e.g. if data storage is used for verification by a provider employee, whether it makes sense to disable this feature);
- technical and organizational data protection measures (e.g. encrypting data in transmission and stored data, the provider's use of multi-component authentication, logging) → output and input content should be encrypted at least in transmission and when stored, the evaluation of other measures depends on the nature of the AI tool;

- results of security audits conducted, including by entities independent of the tool provider → independent audits confirming the security of the solution reduce the risk on the part of the user;
- rules for access to data by subcontractors or sub-processors → it should be determined whether such entities will have access to input or output content, to what extent, and on what terms; the provider should be held responsible for such entities;
- to ensure that input and output data are not used to train models, it is advisable to include a clause in the contract stating that the provider will not use the data for such purposes;
- provider liability rules for breach of confidentiality → provider liability rules for breach of confidentiality determine the feasibility of obtaining compensation in the event of a breach, if the provider's liability is limited, and whether the offered limit is adequate;
- evaluate potential enhancements to data protection for input and output content, and determine if such solutions should be implemented.



RECOMMENDATION: Before selecting an AI tool, review the contract and documentation provided by the AI tool provider for the provider's obligations to maintain the confidentiality of input and output content, and determine whether the solutions offered ensure the confidentiality of professional secrets, as well as whether additional safeguards are advisable.

RECOMMENDATION 5: REVIEW THE CONTRACT WITH THE AI TOOL PROVIDER TO UNDERSTAND COPYRIGHTS REGULATIONS AND THEIR IMPACT ON LEGAL PRACTICE

Why: The attorney-at-law decides on the content of the query (prompt) / input content, of which the work could potentially be a part. The attorney-at-law must have the right to use such work – whether as a property copyright owner, as a licensee, or under one of the forms of permitted use. The attorney-at-law is potentially liable for copyright infringement of the input content.

Given the doubts about the possibility of training models on copyrighted works, it should be verified whether the AI tool provider undertakes to protect users from third-party claims on this account.

Section V

It is also necessary to determine, if any, the AI tool provider's rights to the input and output content, and the restrictions on using such content, in particular, whether the tool provider obtains rights to such content, and possibly what kind of rights (e.g. a license).

How: The attorney-at-law should review the contract for using a specific AI tool in terms of regulating the rights to use the AI tool, input, and output content, and in particular:

- on what basis they will use the AI tool (e.g. license, see [Section II 3.1.](#));
- whether the provider undertakes to defend the user against third-party claims;
- how input and output (output) content rights are regulated, i.e. whether the client retains rights to such content and under what conditions → the right to input content should remain with the client while, in some cases, it may be permissible to grant a license to the provider (this requires individual assessment), the right to output content should not belong to the provider, and the attorney-at-law should assess whether and what rights it may have;
- input and output data should not be used to train models. It is recommended to include a clause in the contract to ensure this commitment;
- whether the client can use the output content for its own commercial purposes (e.g. in its documentation) and whether the contract contains any restrictions on the commercial use of the output content → assess whether any restrictions apply to the attorney-at-law (e.g. restrictions on using synthetic data the provided AI tool generates to train their own AI models will not be a restriction for most attorneys-at-law who want to use AI to support their daily work);
- whether the provider provides a defense for the client against third-party claims to the output content due to intellectual property rights violations (see further [Recommendation 6](#)).



RECOMMENDATION: Before selecting an AI tool, review the provider's contract to determine how copyrights to the AI tool, input, and output content are regulated, including limitations and the extent of the provider's obligations to defend against third-party claims related to copyright infringement. It is essential to assess whether such restrictions have practical implications for attorneys-at-law and if yes – what are they.

RECOMMENDATION 6: **DETERMINE – BASED ON THE PROVISIONS OF THE CONTRACT WITH THE AI TOOL PROVIDER – WHETHER THE PROVIDER WILL DEFEND AGAINST THIRD-PARTY CLAIMS FOR INFRINGING INTELLECTUAL PROPERTY RIGHTS TO THE AI TOOL AND TO THE OUTPUT CONTENT IN CONNECTION WITH USING MODELS APPLIED IN THE AI TOOL**

Why: Using AI tools, like any other intellectual property asset, may involve the risk of claims of infringing these rights. Additionally, due to unresolved concerns regarding the training of models on works or goods protected by intellectual property rights, it is also possible that infringement claims related to the use of output content could arise (see [Section II. 3.1](#) and [3.2](#)).

If a third party makes a claim, the attorney-at-law, as an entity using the AI tool, may have to litigate or stop using such a tool. The tool provider's obligation to defend against such claims, even limited by certain conditions of use, reduces the risk for the attorney-at-law.

How: The attorney-at-law should verify the contract for using a specific AI tool, whether it contains an obligation on the part of the provider to defend the client against third-party claims to the model and output content in connection with using models compacted in the AI tool for infringing intellectual property rights. It is also necessary to verify what additional conditions the use of this obligation is subject to and what claims the provider's obligation relates to. Such additional conditions are often quite obvious and do not create risks for attorney-at-law, e.g. the user must have a right to the input content (i.e. you cannot invoke protection if you yourself infringe on the rights of others), or you cannot disable, evade, interrupt or interfere with content filters or other security systems that are part of the AI tool (i.e. circumventing security features results in disabling protection). The attorney-at-law should put in place organizational and technical arrangements to ensure compliance with such additional conditions (e.g. in the form of internal instructions to staff).



RECOMMENDATION: Before selecting an AI tool, review the contract with the AI tool provider for the provider's obligations to defend the customer against third-party claims to the AI tool and the output content generated with its help, including the scope of additional conditions on which the use of such obligations depends. Steps should be taken to comply with additional conditions (e.g. provide personnel with appropriate instructions).

RECOMMENDATION 7: EVALUATE THE AI TOOL UNDER THE GDPR (INCLUDING THE NEED TO CONCLUDE OR ADAPT THE DATA PROCESSING AGREEMENT, MODIFY PRIVACY NOTICE, EVALUATE DATA TRANSFERS OUTSIDE THE EEA, CONDUCT THE DPIA)

Why: The GDPR's provisions apply to using AI systems to process personal data, but it is the responsibility of either the attorney-at-law or the company/ employer to comply with the GDPR's provisions and to determine the roles of the entities involved in personal data processing (controller/joint-controller/ processing entity).

How: The attorney-at-law or its organization will play the role of data controller, while the provider will play the role of controller (joint-controllers) or processing entity. To ascertain the provider's role, it is essential to examine the contract's stipulations pertaining to personal data, assess the extent of the data to be processed, and evaluate it in relation to the intended purpose of utilising the AI system. It is advisable that, in reference to attorneys-at-law' client data, the AI tool provider should function as the data processor. Regarding user data, it may be acceptable for the provider to process the data as a controller, subject to verification.

Fulfilling the GDPR's provisions will also involve, in particular:

- determining whether the AI system meets the GDPR's requirements, e.g. whether the provider ensures that it has implemented technical and organizational measures adequate to the risks associated with data processing, whether the system enables the realization of data subjects' rights;
- determining whether there is a legal basis to process personal data using the AI system (Article 6 of the GDPR) → this basis should exist both on the side of the provider (for the data used for training), but also the attorney-at-law (their organization) should legitimize the legal basis to process data in the AI system (e.g. in the input content);
- verifying the processing of data outside the EEA and put in place the appropriate safeguards required by Section V of the GDPR if such processing will take place → also remember to verify the provider's maintenance services in this regard, as potentially, in both cases, maintaining the AI system may involve processing data outside the EEA, e.g. regarding remote access to data by service technicians located outside the EEA. Some providers offer the option to restrict data processing to the EEA, in which case, you should verify the terms of such restriction and potential exceptions;

Section V

- analyzing the need for a data protection impact assessment (DPIA) (Article 35 of the GDPR) and carrying it out, if necessary;
- evaluating if it is required to update the information obligation applicable to individuals whose data is processed by the AI system (Articles 13 and 14 of the GDPR);
- assessing whether client contracts need to be updated in terms of personal data processing;
- assessing whether it is necessary to update the record of processing activities relating to the attorney-at-law's activities (Article 30 of the GDPR);
- entering into a data processing agreement (if the provider will process the data as a processing entity) or, if such a contract is already in place, verifying it against the AI tool under consideration, and fulfilling the controller's obligations related to its conclusion (Article 28 of the GDPR).



RECOMMENDATION: Before selecting an AI tool, it is necessary to verify both the contract with the provider, and in particular determine its role in the processing (as a general rule, it should be the processing entity when it comes to input/output content data) and assess whether the provider meets the requirements of the GDPR (e.g. whether a data processing agreement is in place, whether adequate technical measures are implemented). The attorney-at-law should review internal documentation on personal data processing for the AI tool, and determine if the client agreement needs updating.

RECOMMENDATION 8: DETERMINE WHAT SECURITY MEASURES TO IMPLEMENT/APPLY/CONFIGURE WHEN USING THE AI TOOL

Why: After determining how the AI tool works, the contractual terms and technical documentation, and performing an analysis on data processing, the attorney-at-law should determine what security measures to implement, apply or configure when using the AI tool. This is particularly important because the attorney-at-law has a duty of confidentiality and professional secrecy. The obligation to respect professional secrecy implies the need for the attorney-at-law to ensure that appropriate technical, organizational measures are in place to protect against disclosure (see further in [Section II.7](#)). The obligation to implement appropriate technical and organizational measures also stems from data protection regulations. If using high-risk AI systems as defined by the AI Act, attorneys-at-law may have an

Section V

obligation to implement technical and organizational measures to enable the use of the AI tool in accordance with the provider's user manual (see in more detail: [Section II.2](#)) – in practice, however, these will be rather exceptional situations.

How: Most AI tools are hosted on cloud computing. You should configure these tools, including the location of input and output data, as well as content filtering rules that range from less to more creative. Note that with cloud services, in practice, there is no option to modify such AI services/tools themselves.

The attorney-at-law should evaluate not only technical, but also organizational security measures, e.g. the method of communication and instructions to staff.

The attorney-at-law should consider whether it can perform the assessment on its own or within its own structures, or whether it should enlist the help of a developer or technology partner in this regard.



RECOMMENDATION: After understanding the functioning of the AI tool, reviewing the contractual terms and technical documentation, and conducting a data processing analysis, it is necessary for the attorney-at-law to evaluate the appropriate technical and organizational security measures required to ensure the AI tool protects professional secrecy. In particular, assess how to make or change the configuration of the AI tool, especially if it is provided in a cloud model, and determine how to communicate with users and determine the internal instructions.

RECOMMENDATION 9: EVALUATE THE USEFULNESS OF USING AI AGENTS TO AUTOMATE PROCESSES IN THE ORGANIZATION

Why: An AI agent is a computer program or AI-based system that is designed to perform specific tasks autonomously. With advanced machine-learning algorithms, the AI agent can analyze data, make decisions and learn from experience. AI agents are utilized in various fields, including customer service, business process management, virtual assistants, chatbots, recommendation systems, and autonomous robots.

AI agents can therefore provide support in automating routine (time-consuming) tasks, resulting in increased work efficiency and improved service quality. They can be used, for example, to monitor changes in the legislative process and prepare meeting scenarios based on designated documents.

AI agents can be developed using standard tools by attorneys-at-law, without requiring assistance from programmers.

How: The attorney-at-law should identify and evaluate whether AI agents would be useful in the organization, in particular, by answering the following questions:

- Can automation be applied to any aspects of an attorney-at-law's work?
- If so, can the AI agent relieve the attorney-at-law of the entire process or only a part of it (e.g. the AI agent performs preliminary document analysis or conducts preliminary due diligence)?
- What tools can help create AI agents and whether the AI tool offers such capabilities?

When creating AI agents, it is necessary to describe the creation process and evaluate the effects of the AI agent. It is essential to maintain current documentation for AI agents.



RECOMMENDATION: Before choosing an AI tool, determine whether it offers the ability to create your own AI agents and under what rules.

RECOMMENDATION 10: DETERMINE THE TECHNICAL FEASIBILITY (APIS, PLUG-INS) OF INTEGRATING THE AI TOOL WITH OTHER SYSTEMS AND PLATFORMS THE ATTORNEY-AT-LAW USES

Why: The ability to integrate an AI tool with the systems and platforms used by the attorney-at-law (e.g. document management systems, databases, CRM) allows the creation of a solution that is perfectly tailored to the attorney-at-law's needs and makes full use of the functionalities of a given AI tool.

How: The attorney-at-law should review the contract for using a particular AI tool, along with related documentation the AI tool provider provided, regarding the technical conditions for integrating a particular AI tool with other systems or platforms, in particular:

- whether the provider offers APIs, plug-ins, or extensions compatible with the advisor's systems, or if third parties provide such solutions and under what terms;

Section V

- whether the provider provides adequate technical support and documentation during the implementation process (dedicated technical support; knowledge base, etc.);
- whether the integration requires changes to owned systems and platforms, and whether it is possible to make such changes on one's own, with the help of the provider of such a system or a third party; assess whether the creation and use of such a plug-in or extension would require modifying the owned system or platform (including whether the attorney-at-law or their organization has the right to do so);
- whether the application of such integration requires a performance reassessment and security evaluation of existing systems and platforms on the one hand and the AI tool on the other.



RECOMMENDATION: Before selecting an AI tool, assess the technical and legal conditions for integrating the AI tool with the systems and platforms used by the attorney-at-law, in particular, taking into account data security, and the terms of existing contracts for the systems and platforms with which such AI tool would be integrated.

RECOMMENDATION 11: EVALUATE THE USEFULNESS OF MODEL TRAINING (FINE-TUNING) ON INTERNAL DATA

Why: Fine-tuning makes it possible to adapt the AI model to the specific tasks and needs of a given organization (see more in [Section I. 2.4.](#)) so the AI tool can better support specific business processes in the organization and deliver more precise results. Not all AI tools offer the possibility of customization (fine-tuning) and, therefore, it is also necessary to choose the right tool for this purpose.

How: The attorney-at-law should identify/assess whether it would be useful in the organization to train AI models on internal data by answering the following questions:

- In what areas can the use of fine-tuning benefit an organization?
- Is the internal data on which the model will be trained complete, accurate, and current? → low-quality data can lead to erroneous results;

- Does the organization have adequate technical resources and competence to conduct fine-tuning (infrastructure / specialists)?
- What will be the contractual terms of the model created as a result of fine-tuning; i.e. will such model be available only to the entity that creates it?
- What are the costs of fine-tuning and maintaining such a customized model?

Since fine-tuning may require special knowledge, the attorney-at-law should consider engaging a qualified person in this area. The attorney-at-law should develop a plan for adjusting and evaluating such model adjustment.



RECOMMENDATION: The attorney-at-law should assess whether they want to make model adjustments (fine-tuning) and select the appropriate tool for this purpose. It is also necessary to adequately prepare such a process, e.g. by selecting the right data and engaging a specialist to support the process.

B. Recommendations for implementing AI tools

RECOMMENDATION 12: REVIEW CONTRACTS WITH CLIENTS FOR RESTRICTIONS OR RULES ON USING AI TOOLS

Why: An attorney-at-law, when providing services to clients, should exercise due diligence and protect the client's interests and the information the client entrusts to them (professional secrecy).

How: The attorney-at-law should examine client contracts for AI tool usage provisions, specifically checking if the contract includes:

- Prohibitions on using AI tools to provide services;
- If the contract does not explicitly forbid the use of AI tools for providing services, whether it includes specific restrictions on their usage or does not require informing clients about the use of such solutions;
- If the contract includes restrictions on the usage of AI tools, it is essential to assess whether the AI tool and its application adhere to these restrictions. Furthermore, necessary adaptation measures should be identified and implemented accordingly;
- Liability rules in case of erroneous results generated by AI.



RECOMMENDATION: Before using an AI tool in your work for a particular client, verify that your contract with the client does not contain provisions restricting or prohibiting the use of the AI tool. If there are restrictions, determine the necessary adjustments to avoid contract violations.

RECOMMENDATION 13: IDENTIFY SITUATIONS WHERE IT IS NECESSARY TO INFORM THE CLIENT ABOUT THE USE OF THE AI TOOL

Why: A deployer may have limited disclosure obligations to third parties, as set forth in Article 50 of the AI Act, including the obligation to report on the generation or modification with the help of AI of text published to inform the public about matters of public interest (Article 50(4) of the AI Act) or interactions with AI, e.g. when providing AI-based chat bots to clients to obtain information about ongoing cases (Article 50(1) of the AI Act).

Regardless of the obligations indicated explicitly in the AI Act, the attorney-at-law should assess whether the obligation to perform legal services with due diligence also requires notifying the client of using AI tools, and whether such notification should be done in a formalized manner (e.g. in the form of a provision in the contract or a formal notice), or when providing ongoing services (e.g. before the start of the recording and transcription of the meeting to prepare its summary and task list using the AI tool). As in the AI Act, the evaluation can be based on assessing the risk of using such a solution for the client.

How: Determine if informing the client about using AI tools is necessary, taking into account following:

- whether the attorney-at-law intends to use standard solutions for streamlining daily work and increasing their efficiency which are not dedicated exclusively to lawyers, or specialized solutions for lawyers → using standard solutions for their intended purpose, as in the case of other standard IT solutions, should not generate an obligation to inform clients (analogous to how clients are not informed, for example, about standard document management systems used by law firms or attorneys-at-law), the evaluation of specialized solutions should be made on a case-by-case basis, taking into account the risk of using such tools for the client;

Section V

- whether it is a solution that is widely available in the market and offered by reputable providers, or whether it is a solution in the testing phase, or prepared for/by a particular attorney-at-law or their organization, without verification by an independent entity → in the case of solutions that are widely available and offered by reputable providers, their use as intended does not generally require notification to clients unless it is a solution that generates a higher than average risk for the client; in the case of solutions in the testing phase or in-house solutions, the risk should be assessed and notifying the client should be considered;
- what area of services/consulting will be covered by using the AI tool, i.e. whether the AI tool will be used for standard activities or for specific tasks assigned by the client that have or may have an impact on the client's business (e.g. using AI to recommend a settlement of a material matter and the terms of such a settlement, or to prepare a summary of a videoconference during which strategic issues are to be discussed regarding a planned transaction or other venture, the disclosure of which may have a significant impact on the client) → if it concerns issues that are material to the client's business, it is recommended to at least notify the client (see also [Recommendation 14](#) below), while it is not always required to regulate this issue in the contract, e.g. in the case of a videoconference on strategic issues, the information can be given verbally and recorded, or previously transmitted by email, allowing the client to object;
- the nature of the services the attorney-at-law provides, e.g. strategic consulting or involving a particular attorney-at-law due to their special qualifications, which would be taken over even in part by the AI tool used → in such case, it is recommended to notify of using specialized AI tools that would take over in part the functions entrusted to such lawyers.

If the attorney-at-law determines that notifying the client about the use of an AI tool is necessary, the attorney-at-law should specify which AI tool will be used, the reasons for its use, and the scope of its application. The attorney-at-law should make information about the security measures taken and the results of the analysis of the AI tool available to the client upon request.



RECOMMENDATION: Attorneys-at-law should review provided services and assess when accepting new assignments whether notification to the client is necessary due to the sensitive nature of the assignment or the type of AI tool

used and its planned use. The assessment should consider the risk to the client. Using standard AI tools as intended for routine matters does not, as a rule, require client notification. The attorney-at-law should notify of the use and scope of use of the tool concerning significant matters that, if disclosed, could adversely affect the client. The attorney-at-law should assess whether the notification should be formal (e.g. in a contract) or on an ad hoc basis for a specific case.

RECOMMENDATION 14: DETERMINE IN WHICH CASES THE CLIENT'S CONSENT IS NEEDED TO USE THE AI TOOL

Why: AI is a technology that has been available to the public for a relatively short time. It also carries risks like hallucinations. Regulations on AI, such as the AI Act, are in the early stages of implementation. These regulations, including codes of conduct and risk assessment measures, are expected to enhance the legal acceptance of using these tools.

For the above reasons, the attorney-at-law should assess in which cases, in addition to informing the client about using AI tools, it is advisable to obtain the client's consent to use the AI tool.

How: To assess whether client consent is necessary for the use of an AI tool, consider addressing the following inquiries:

- can customer data be used to train the AI tool? → The client's consent must be obtained, and the attorney-at-law should consider anonymizing the training data;
- whether the client engages a specific lawyer and expects their personal involvement in the case → using AI tools that would take over a significant part of the tasks of such a lawyer should be agreed with the client, as usually, the client agrees to incur higher fees to ensure a specific person is involved;
- whether the AI tool is used to predict the outcome of court or administrative cases → clients often ask for a percentage assessment of a particular settlement, which lawyers determine based on their experience and analysis of similar cases; if the assessment were to be made solely by the AI tool, the client's consent should be obtained;
- if a tool developed by a client's competitor or an entity with which the client is in significant dispute is to be used in work for the client → at least due to reputational risks for the client, the client's consent should then be obtained;



RECOMMENDATION: The client's consent to using an AI tool may be required, particularly if the client requires a specific lawyer to be personally involved and the AI tool is to take over a significant part of these functions, if client data is to be used to train an AI model, or if the AI tool is to be used to predict the outcome of proceedings without human verification. The attorney-at-law should assess on a case-by-case basis the necessity of obtaining such consent.

RECOMMENDATION 15: DETERMINE IN WHICH CASES USING THE AI TOOL MAY AFFECT CLIENT'S FEES

Why: If using an AI tool speeds up (automates) certain processes, the client can expect a reduction in fees if their attorney-at-law is charging them on a flat-rate basis (e.g. a lump sum per case). Using AI tools benefits clients billed hourly by reducing their chargeable hours. On the other hand, using an AI tool usually requires additional resources or licenses, which, especially for specialized programs, can be expensive. Hourly rates alone might not cover tool costs, justifying extra charges to the client, like fees for databases or technical infrastructure.

How: In assessing whether using an AI tool can affect a client's compensation and how, it may be helpful to answer the following questions:

- On what basis are settlements made with the client (hourly rate, lump sum)?
- How important is it to use the AI tool in a particular case (e.g. will the AI tool take over a significant part of the lawyer's work)?
- Does using AI tools incur additional costs, including licensing or implementation costs?
- Whether AI tools that streamline work and are intended for widespread use are employed, or specialized tools are chosen (e.g., for analyzing arbitration awards) → especially in the case of specialized tools, it may be reasonable for clients to compensate those costs.



RECOMMENDATION: In the case of hourly billing, using AI may justify introducing a fee to cover the cost of applying the AI tool, especially if these are specialized tools purchased by attorneys-at-law for that case. Using tools for common use in various cases may not justify additional fees (similarly to standard office software). Attorneys-at-law should carefully consider the impact of AI tools on their practice and discuss these implications with their clients.

RECOMMENDATION 16: DEVELOP INTERNAL RECOMMENDATIONS/INSTRUCTIONS ON USING AI TOOLS

Why: Developing internal recommendations/instructions on using AI tools is crucial for several reasons:

- it helps ensure compliance with applicable laws (e.g. the AI Act, the GDPR);
- it helps enhance data security and confidentiality (including professional secrecy); and
- it helps standardize how AI tools are used across the organization.

How: The attorney-at-law should develop internal recommendations/instructions on using AI tools which should specifically include:

- Clearly defining what tasks, the AI tool can be used for, and for which it is forbidden;
- Identifying the type of information or data that can be transferred to the AI tool;
- Rules for creating queries (input), including techniques for precisely formulating queries to the AI tool (prompt engineering) – to obtain the most accurate results and avoid the risk of claims;
- Rules for controlling input content (input);
- Rules for verifying and validating output content (output) generated by AI;
- Principles of staff training and qualification / availability of training materials for staff;
- Rules for monitoring the use of the AI tool (e.g. in terms of over-reliance on using these solutions, their correctness, effectiveness, the risks they generate, etc.).

These materials should be disseminated to staff and made accessible internally, ensuring users can readily familiarize themselves with them. Update materials as necessary. Persons responsible for updating them on an ongoing basis and answering users' questions should be identified.



RECOMMENDATION: Before using an AI tool, develop internal recommendations/instructions on using AI tools, including specifying how to use such tools. Update materials as necessary. It is advisable to designate an individual who will be responsible for updating these materials and addressing user inquiries.

RECOMMENDATION 17: CONDUCT INTERNAL TRAINING ON USING THE AI TOOL

Why: Pursuant to Article 4 of the AI Act, the deployer is obligated to ensure AI literacy for users of AI tools, considering their technical knowledge, experience, education, training, and the specific context in which they will utilize AI systems. Training those who are to use the AI tool will result in the more efficient use of AI tools, reduced errors, and increased data security. Trained personnel will be aware of their responsibilities, existing risks, and challenges in using AI tools, and consequently, more likely to use the AI tool (building trust in AI).

How: The attorney-at-law should perform the following steps:

- determine who will use the AI tool (own staff / service providers);
- make an analysis of the training needs of those who are to use the AI tool (determine the level of technical knowledge, experience, education, training, etc.);
- prepare relevant instructions / training materials in this regard;
- conduct training – before using the AI tool.

The attorney-at-law may entrust the implementation of training to external entities or other attorneys-at-law who are competent.



RECOMMENDATION: Users should receive training on how to use the AI tool before they begin using it.

C. Recommendations for using AI tools

RECOMMENDATION 18: CONDUCT REGULAR EVALUATIONS OF AI TOOLS IN USE (INCLUDING FINE-TUNED MODELS) AND MARKET OFFERINGS OF AI TOOLS DEDICATED TO LAWYERS

Why: The regular evaluation of AI tools in use allows one to verify if the AI tool in use meets the organization’s current needs, as well as the identification of threats (risks) and new challenges that have emerged in connection with using a given AI tool. Keeping track of the market offerings of AI tools dedicated

to lawyers, which are just emerging in the Polish market, allows you to keep up to date with the latest AI technologies and best practices in connection with using AI tools which can give attorney-at-law a competitive advantage in the legal services market.

How: The attorney-at-law should implement a process within the organization to regularly evaluate the AI tools used (including fine-tuned models) and the market offerings for AI tools dedicated to lawyers to:

- Ensure that the AI tool used is regularly monitored, maintained and updated, in particular, in the context of changes made by the AI tool provider, including verifying changes to the documentation the AI tool provider provides (regulations or price lists) and updating assessments and internal documentation on using the AI tool accordingly (see also [Recommendation 19](#));
- Obtain regular feedback on users' use of the AI tool and their comments;
- Perform regular analysis of whether the AI tool meets the organization's current needs; monitor market offerings for AI tools dedicated to lawyers;
- In larger organizations, individuals should be designated to perform these tasks, involving both attorneys-at-law and technical experts in the process;

Guidelines and rules for this process can be part of an overall policy for using AI tools in an organization.



RECOMMENDATION: There should be a regular evaluation of the AI tools used (fine-tuned models) and the market offerings of AI tools dedicated to lawyers. In larger organizations, individuals should be designated for this task, including for collecting feedback.

RECOMMENDATION 19: REGULARLY REVIEW INTERNAL RECOMMENDATIONS/GUIDELINES ON USING THE AI TOOL AND UPDATE THEM AS AI TECHNOLOGY DEVELOPS (AI COMPLIANCE)

Why: The legal regulations on using AI, the guidelines of authorities in this area, and the functionalities or rules of using a given AI tool may change, so regular reviews and updates of internal guidelines/recommendations on using AI tools will make it easier to ensure compliance with applicable laws and market

practice. AI technology is evolving rapidly, resulting in new challenges and options. Keeping guidelines / recommendations up to date allows for optimal and safe use of the AI tool.

How: The attorney-at-law should implement a process within the organization to regularly review internal recommendations / guidelines for using the AI tool and update them, specifically identifying:

- the frequency of such reviews;
- the terms and conditions of their conduct;
- the person(s) responsible in the organization for the process.

Guidelines and rules for this process can be part of an overall policy for using AI tools in an organization.



RECOMMENDATION: Internal recommendations and guidelines for using AI tools should be reviewed regularly and adjusted to ensure compliance. In larger organizations, individuals should be designated for this task.

RECOMMENDATION 20: HOLD REGULAR INTERNAL TRAINING SESSIONS ON USING THE AI TOOL

Why: Regardless of regulatory obligations (see more on [Recommendation 17](#)), organizing regular internal training on using the AI tool is also important for the following reasons:

- It allows the consolidation of good practices and the sharing of experiences in using the AI tool;
- It enables the introduction of new features and modifications to AI models (e.g. due to the provider's updates);
- It enables education and competence development among junior colleagues and trainees attorney-at-law.

How: The attorney-at-law should implement a process for regular training in using AI tools within organization, specifying in particular:

- the frequency of such training.
- the person(s) responsible for this process in the organization;
- recipients of such training.

The terms and conditions for conducting regular internal training can be part of the overall policy for using AI tools in the organization.



RECOMMENDATION: AI users should participate in regular training on using the AI tools they use.

RECOMMENDATION 21: CREATE AND MANAGE AN INTERNAL KNOWLEDGE BASE (KNOWLEDGE MANAGEMENT)

Why: Establishing and maintaining an internal AI knowledge base—comprising contractual and technical documentation, analysis, or experience with AI tools, including a repository of validated AI prompts or agents—is essential for numerous reasons:

- It accelerates decision-making and operational processes;
- It helps retain knowledge that may be lost due to employee turnover;
- It facilitates collaboration and internal communication within the organization;
- It expedites the onboarding process and decreases the time required to integrate new employees;
- The regular updates of the knowledge base help ensure compliance with applicable laws and regulations.

How: The attorney-at-law should implement procedures and policies in the organization that define the rules for creating, managing and updating the knowledge base which, in particular, will specify:

- What kind of documents (sample contracts, opinions, etc.) must be collected in the internal knowledge base, and identify the person responsible for this process;
- Indication of the secure “location” of the knowledge base in the organization’s infrastructure;
- The structure of the knowledge base / the key by which documents should be saved;
- The rules for updating the collected documents and the people responsible for this process.

A comprehensive knowledge base should encompass both AI tools that have been successfully implemented for use, as well as tools that have undergone

evaluation and were subsequently deemed unsuitable. In this case, the knowledge base should also include information on the reasons for non-implementation.



RECOMMENDATION: It is recommended that the organization implement procedures and policies for creating, managing, and updating the internal knowledge base of AI tools in use and those evaluated but not implemented.

RECOMMENDATION 22: MANAGE AI INCIDENTS AND TAKE PREVENTIVE ACTIONS FOR THE FUTURE

Why: Regulations such as the AI Act, the GDPR, national laws implementing the NIS2 or DORA Directive (if applicable) require organizations in certain cases to report incidents³⁶ and take corrective actions³⁷ and preventive actions. AI incidents may result in data protection breaches, which may require notifying the relevant data protection authority and data subjects. The obligation to notify the client may also arise from the contract concluded with the client.

Effective incident management helps to quickly detect and minimize the impact of such violations and helps to minimize the risk of future incidents. Implementing appropriate solutions to identify threats is crucial from the perspective of the security of the organization and its customers (maintaining confidentiality and professional secrecy).

How: Attorneys-at-law should establish a system to manage AI incidents and take corrective and preventive actions within the organization. Specifically, they should:

- Implement an incident management procedure that will specify, among other things: (i) the types of the most common incidents that may affect AI; (ii) the terms and conditions for reporting incidents to authorities and

³⁶ If an attorney-at-law (deployer) repurposes an “ordinary” AI system in such a way that it becomes a high-risk AI system, it will also become a provider of that system under the AI Act, with the result that the obligations of a provider of a high-risk AI system apply to it, e.g. obligations related to reporting “serious incidents” (Article 73 of the AI Act). Under DORA (which is relevant to the digital resilience of the financial sector), there is the concept of an “AI incident”. Article 9 of the AI Act requires an AI risk management system for high-risk systems. Article 12 of the AI Act mandates automatic logging solutions throughout the lifecycle of an AI system.

³⁷ See, for example, Article 20 of the AI Act.

Section V

clients and the handling them; (iii) the principles of responsibility for the areas described in the procedure and the principles of internal and external communication; (iv) the principles of recording incidents; and (v) the follow-up mechanisms (corrective and preventive actions);

- Introduce a “continuous learning” process within the organization to address incidents and risks, as well as AI challenges that the organization may encounter.

Guidelines and rules for this process can be part of an overall policy for using AI tools in an organization.



RECOMMENDATION: Implement policies for managing AI incidents, including protocols following their detection, procedures for reporting to relevant authorities and customers, and strategies for corrective and preventive actions to address future occurrences.

TIPS FOR BEST PROMPTING



- **Provide context:** Inform Copilot of the user’s context, e.g. “I’m a lawyer” or “I’m a legal advisor talking to a client,” so that Copilot can tailor responses to specific needs.
- **Structure of prompts:** Use a prompt structure that includes purpose, context, sources of information, and expected results. For example, the objective should be at the beginning so that Copilot can focus on it.
- **Precision of language:** Use clear and precise language to avoid misunderstandings. Avoid ambiguous words and phrases.
- **Length of prompts:** Prompts should be the right length – too short can be less effective, and too long can cause Copilot to get confused.
- **Using saved prompts:** Take advantage of the ability to save prompts so you can easily reuse them in the future.
- **Experimentation:** Experiment with different prompts and approaches to find the most effective ways to work with Copilot.

TECHNIQUES TO HELP WITH MORE COMPLEX SCENARIOS

- **Divide tasks into steps:** Divide tasks into smaller steps for better process control and better results.
- **Giving guidelines:** Indicate to Copilot not to invent content and if it does not know the answer to a question, to inform you about this.
- **Working with large documents:** For large documents, divide them into smaller parts and work on them in stages so that Copilot can better process the information.
- **Using examples:** Provide examples so that Copilot can better understand your expectations. Examples can be especially helpful for more complex tasks.
- **Use the document attachment feature** to enhance the prompt:
 - » for example, when creating a draft memo that uses a standard template, you can specify the necessary headings in the body of the prompt, or simply include, as an attachment, a template or example of a previous report and indicate that Copilot should follow the structure and style of the attachment.

EXAMPLES OF AI APPLICATIONS (USING MICROSOFT 365 COPILOT AS AN EXAMPLE)



Below is a general description of the capabilities and more detailed examples with print-screen listings.

WORD

- Summary of documents
- Inserting proposals for contractual clauses
- Simplifying texts
- Spell check

OFFICE

- Prepare a proposal for an email response
- Summary of correspondence history from a given person

COPILOT OPTION IN TEAMS

- Ability to prepare a summary of documents located online
- Ability to prepare a synthetic note from multiple documents stored in Onedrive
- Preparation of comparing documents
- Prepare a summary of correspondence from a given person or within a given time period

TEAMS

- Transcription of live meetings
- Prepare a summary of the meeting and to do list
- Access to a transcript and a recording that indicates at what point the given person spoke

POWERPOINT

- Preparation of a presentation based on a Word document.

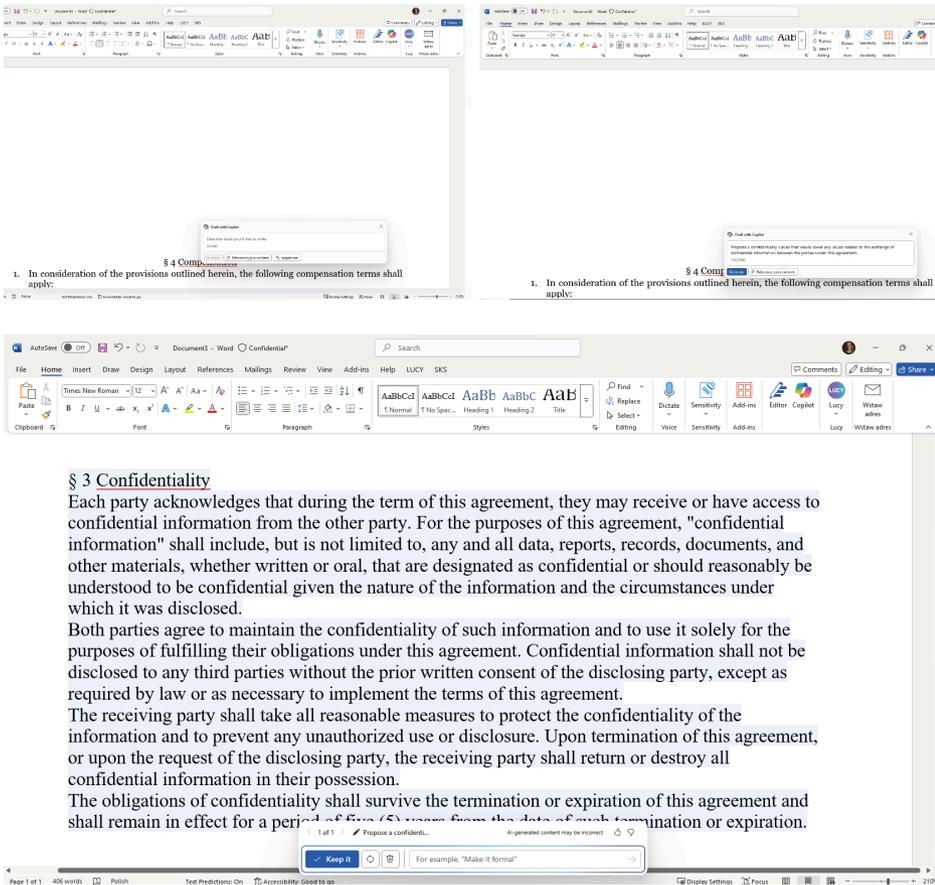
Appendix no. 2

EXAMPLE 2 – THE ABILITY TO WORK WITH COPILOT IN WORD

- Click on the Copilot icon and enter a prompt, e.g. ask to propose a provision, language verification of the highlighted passage, etc.
- You can accept the proposed text by clicking “Keep it” or ask to re-generate another proposal.

M365 Copilot functionality

Not just chat - a range of functionality adapted to individual Microsoft 365 programs, including the ability to edit text directly.



§ 3 Confidentiality

Each party acknowledges that during the term of this agreement, they may receive or have access to confidential information from the other party. For the purposes of this agreement, "confidential information" shall include, but is not limited to, any and all data, reports, records, documents, and other materials, whether written or oral, that are designated as confidential or should reasonably be understood to be confidential given the nature of the information and the circumstances under which it was disclosed.

Both parties agree to maintain the confidentiality of such information and to use it solely for the purposes of fulfilling their obligations under this agreement. Confidential information shall not be disclosed to any third parties without the prior written consent of the disclosing party, except as required by law or as necessary to implement the terms of this agreement.

The receiving party shall take all reasonable measures to protect the confidentiality of the information and to prevent any unauthorized use or disclosure. Upon termination of this agreement, or upon the request of the disclosing party, the receiving party shall return or destroy all confidential information in their possession.

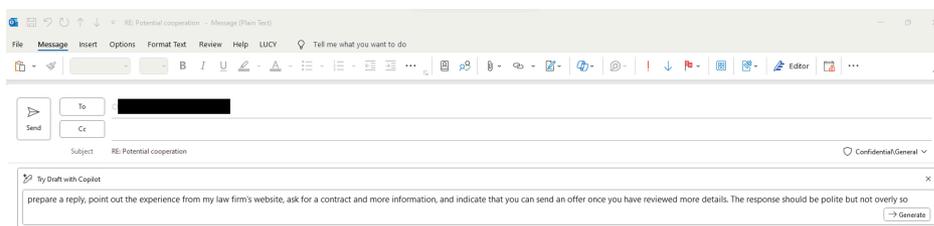
The obligations of confidentiality shall survive the termination or expiration of this agreement and shall remain in effect for a period of five (5) years from the date of such termination or expiration.

EXAMPLE 3 – PREPARING A RESPONSE TO AN EMAIL

- Click the reply button, and then the Copilot icon “Copilot draft version”.

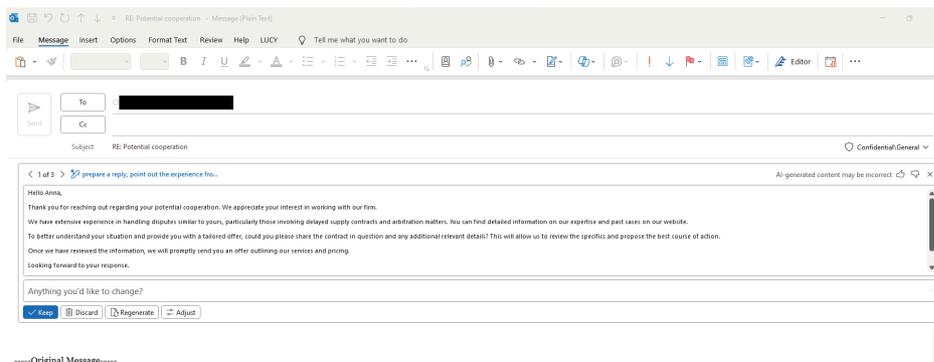
Appendix no. 2

- In the “Copilot” box, type a prompt, such as “prepare a reply, point out the experience from my law firm’s website, ask for a contract and more information, and indicate that you can send an offer once you have reviewed more details. The response should be polite but not overly so”. Then press the “Generate” icon.



-----Original Message-----

- In the “Copilot” box you will receive a draft of your answer, which you can keep, request another version or further change/adjust. Remember to read the draft carefully before sending.

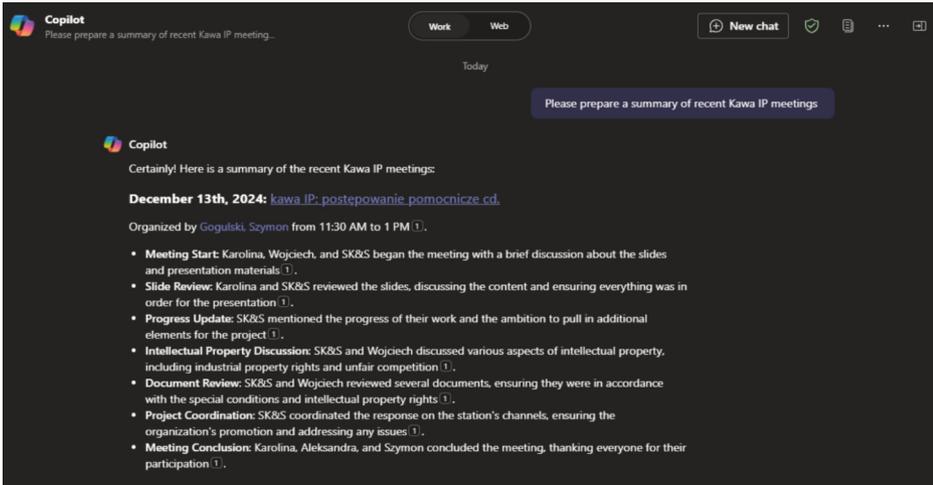


-----Original Message-----

EXAMPLE 4 – SUMMARY OF CORRESPONDENCE HISTORY FROM A PERSON

- In the “Copilot” box of MS Teams, type a prompt with a request for a summary of correspondence on a given topic. You can indicate from whom it should come, what the subject was or ask for a summary of the history of correspondence, for example, within one string of emails.

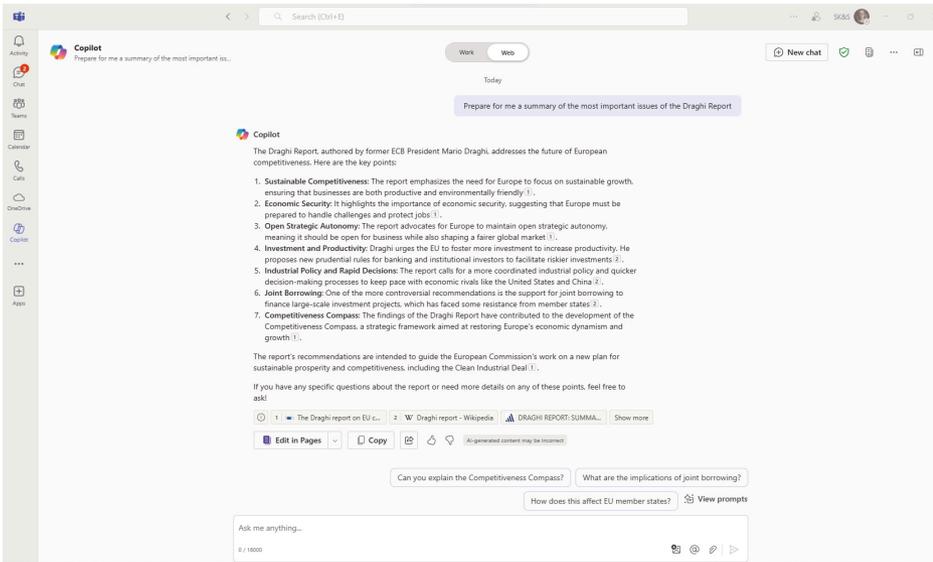
Managing your e-mail inbox



EXAMPLE 5 – SUMMARY OF DOCUMENTS AVAILABLE ONLINE IN TEAMS

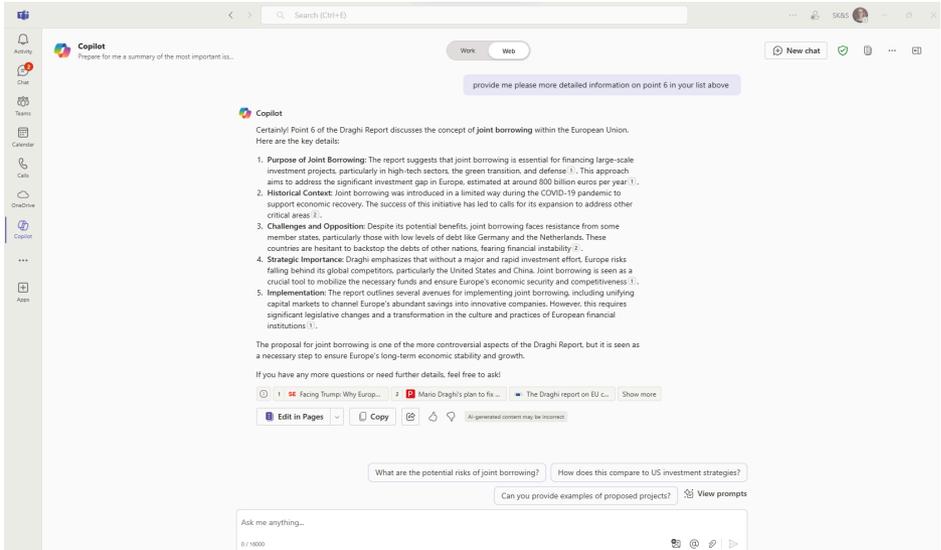
- Click the “Internet” button and ask a question about the content of the document.

Summaries of documents



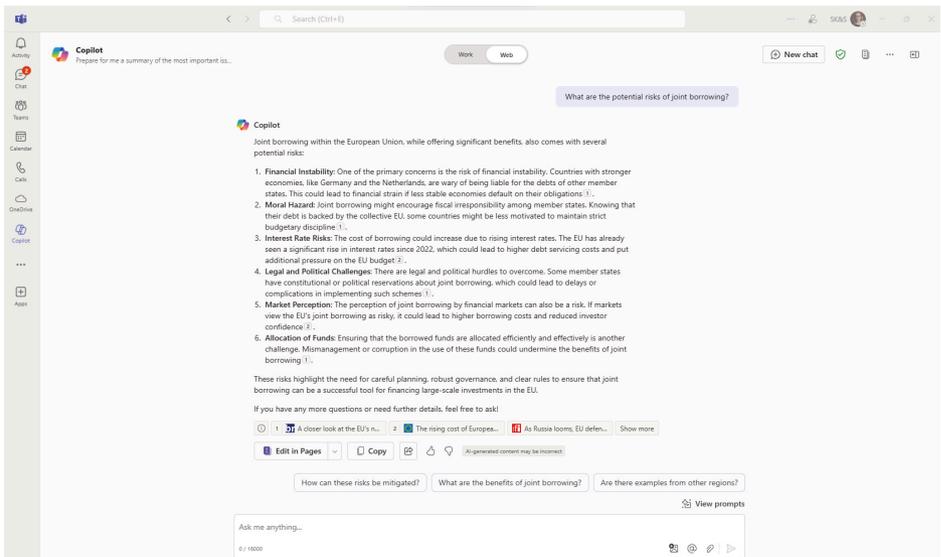
- Ask for very detailed information.

Summaries of documents



- Repeat the request for further, very detailed information.

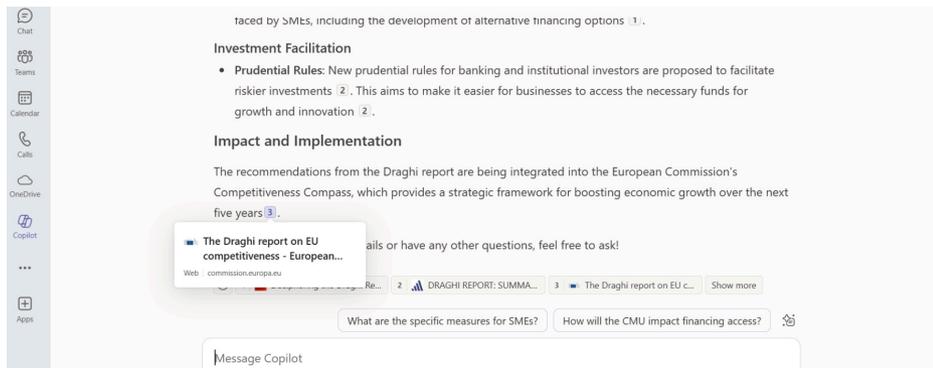
Summaries of documents



Appendix no. 2

- If necessary, check the source of the information Copilot provided (text underlined with a footnote number).

Summaries of documents

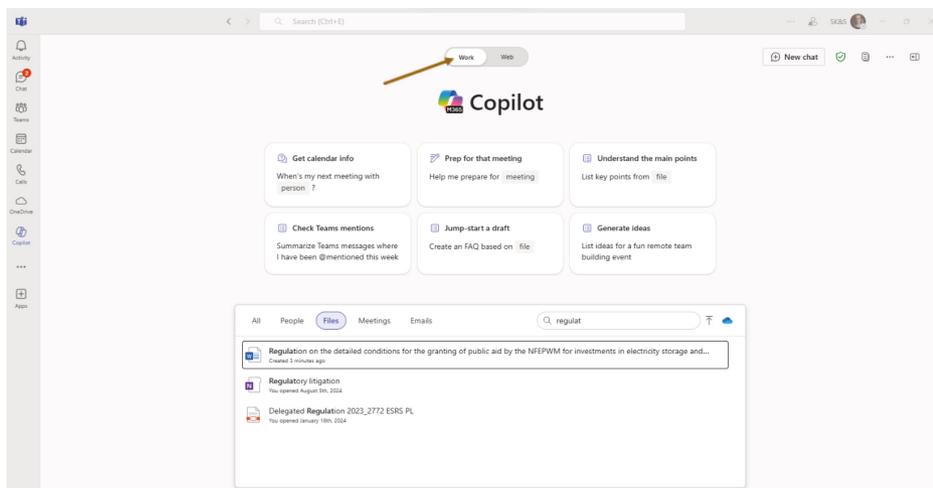


EXAMPLE 6 – CREATING SUMMARIES FROM MULTIPLE DOCUMENTS LOCATED ON ONEDRIVE USING COPILOT WITHIN TEAMS (example:

a note on the draft regulation on detailed conditions for granting public aid for investment in electricity storage)

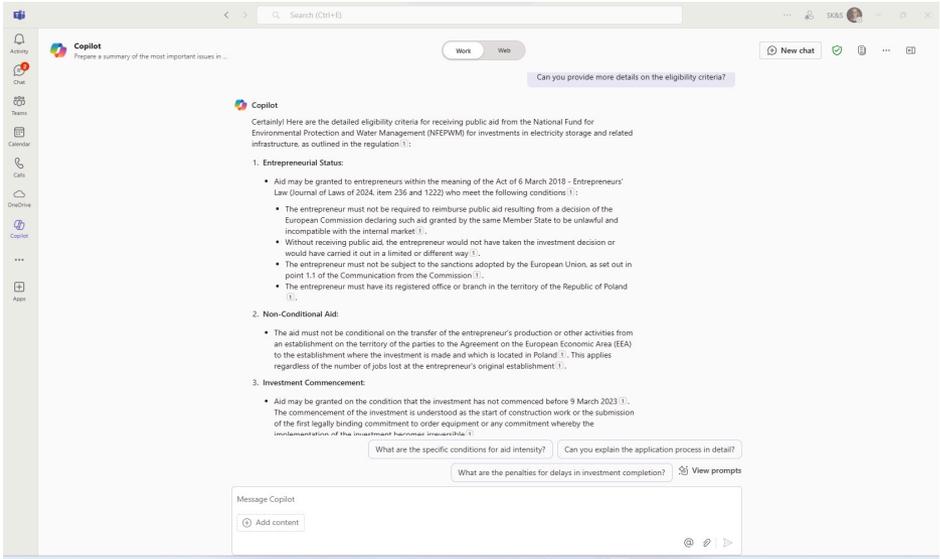
- Click the “Work” button, which will provide Copilot with work from within the law firm’s Onedrive structure. Use the “Submit” button to select the document from which you want to create a summary.

Summaries of documents



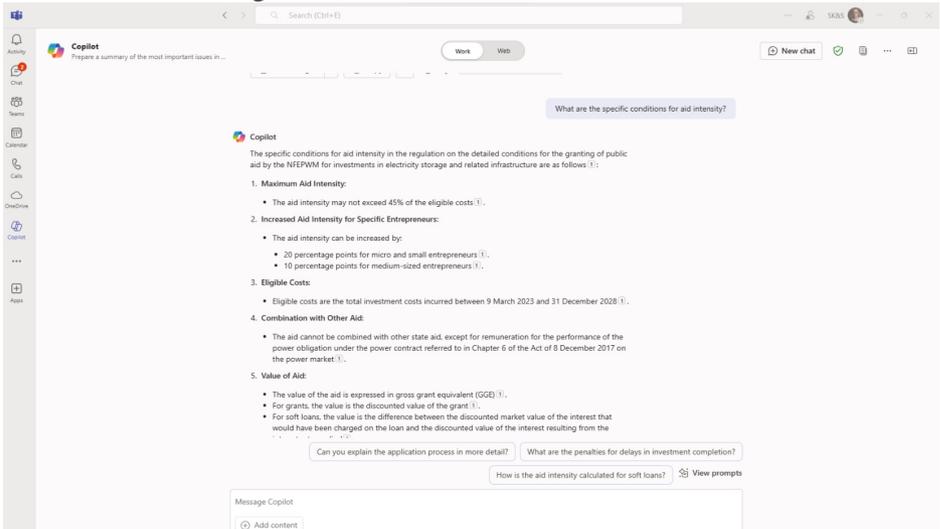
- Ask further, more detailed questions or use the question suggested by Copilot.

Summaries of documents



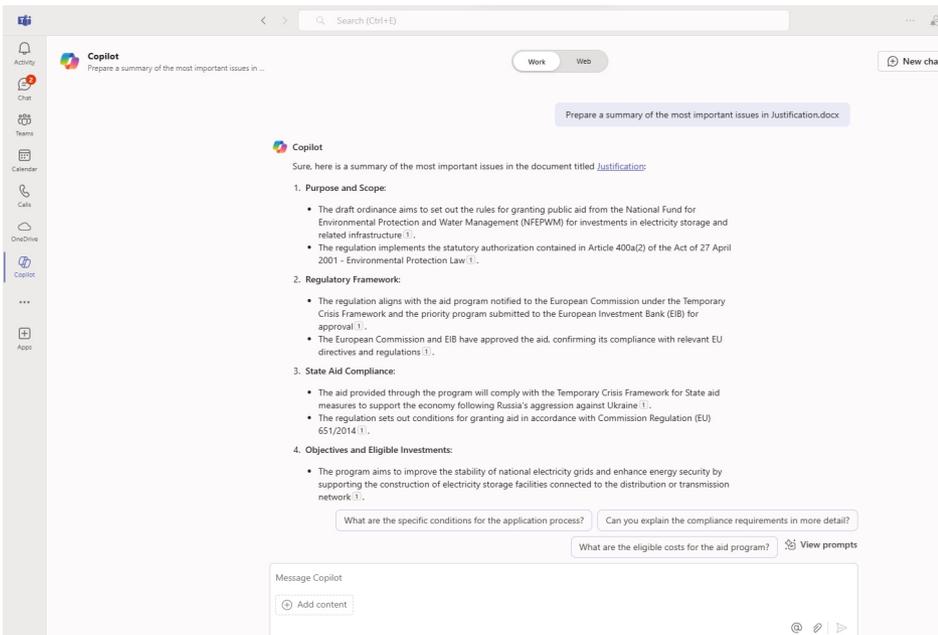
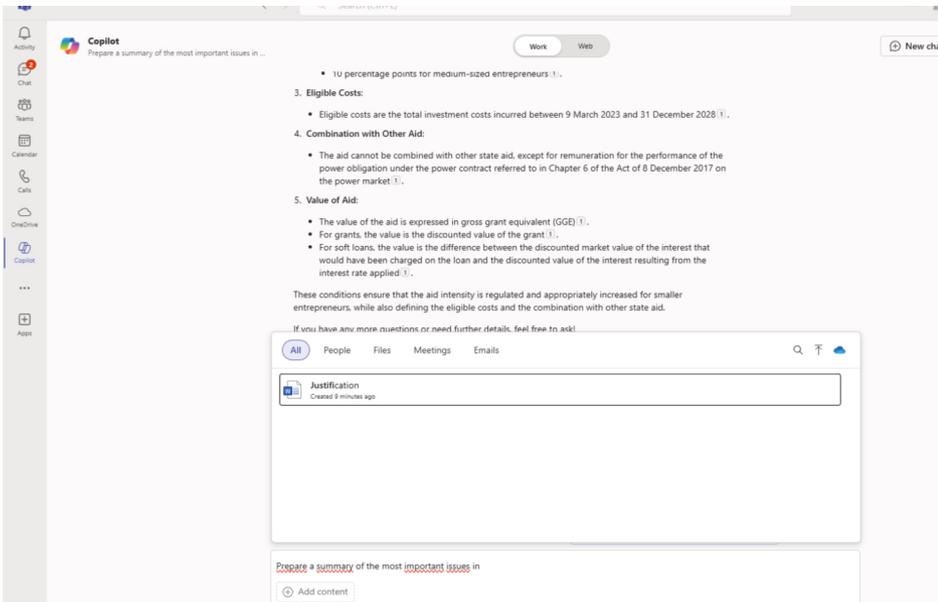
- Ask further, more detailed questions or use the question suggested by Copilot. In this way you build a database that will be used in the summary.

Summaries of documents



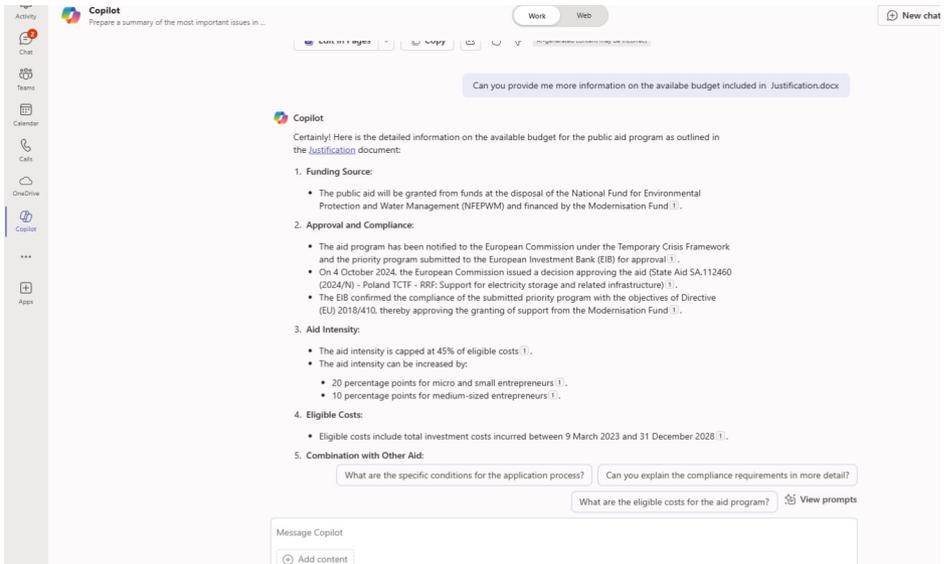
Appendix no. 2

- Add another document (here: Regulatory Impact Assessment) and ask for its summary. This is the next step in building the database that will be used in the summary.

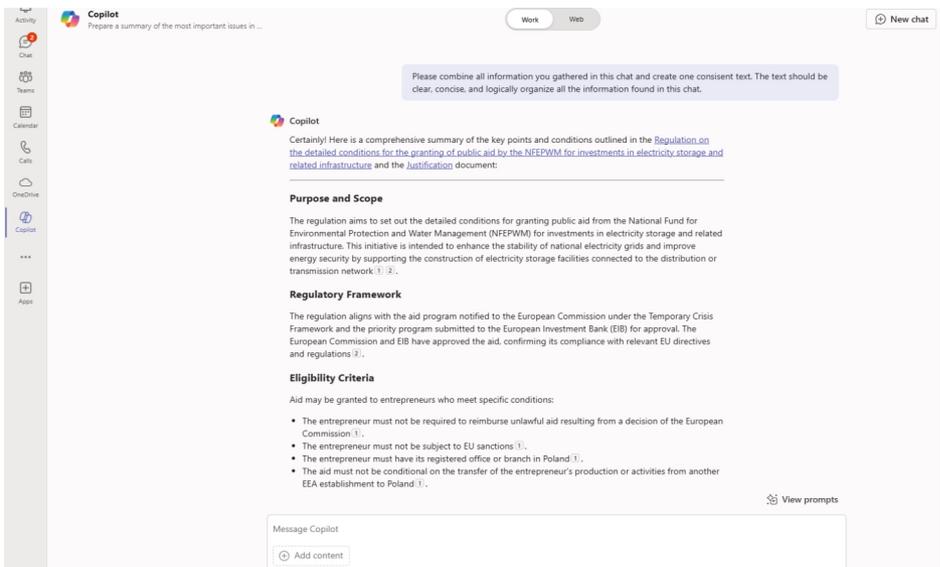


Appendix no. 2

- Ask further, more detailed questions or use the question suggested by Copilot.

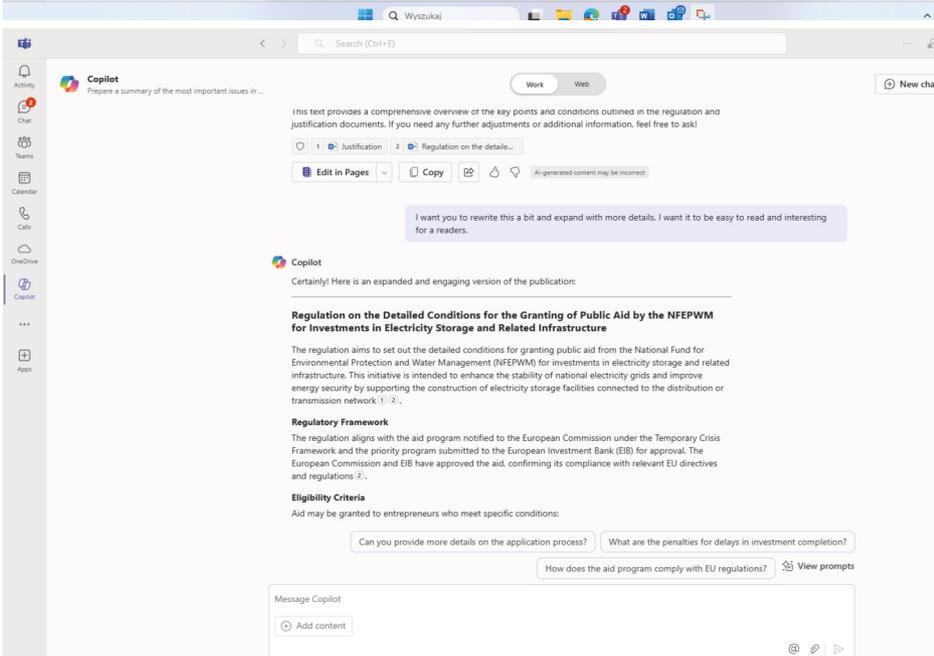
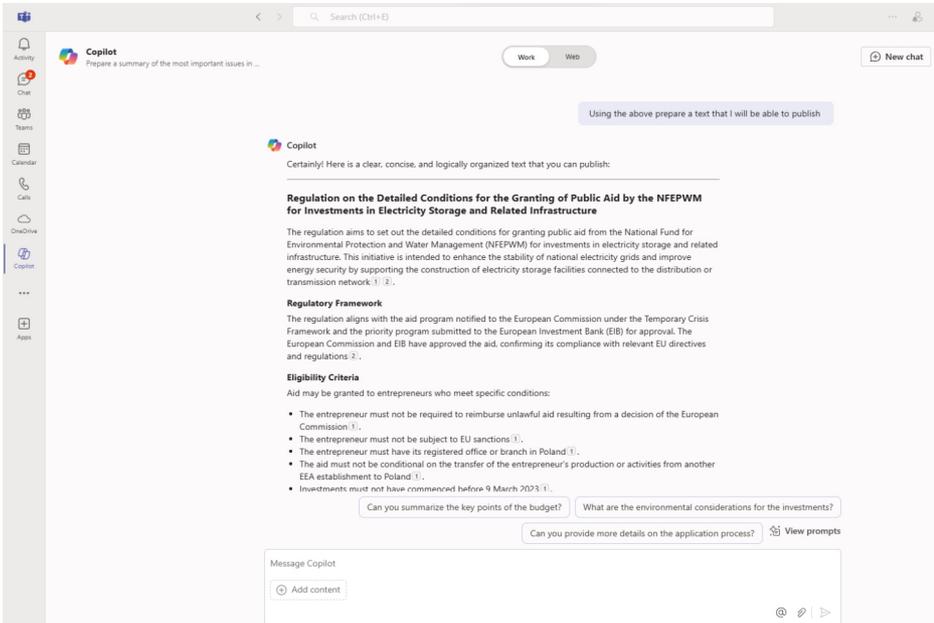


- Ask to compile all the information that is in the chat into a single, coherent text. Indicate what the tone of the text should be and other guidelines for its structure.



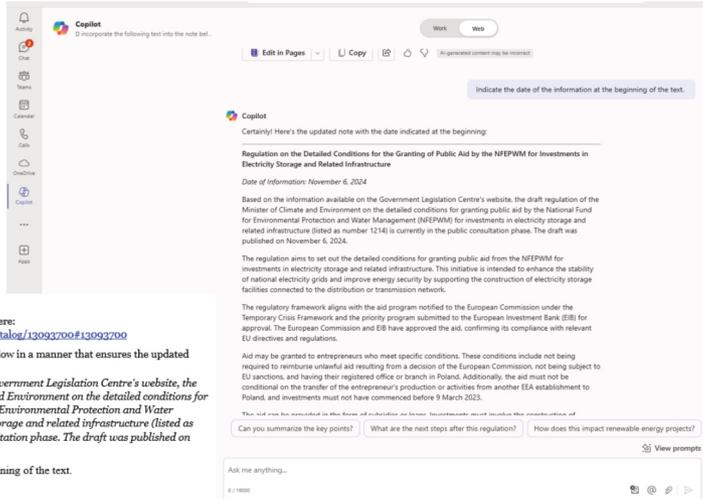
Appendix no. 2

- Ask to prepare the text of the publication and make further requests as to what the final product should look like.



Appendix no. 2

- You can expand the document with information found on the Internet.

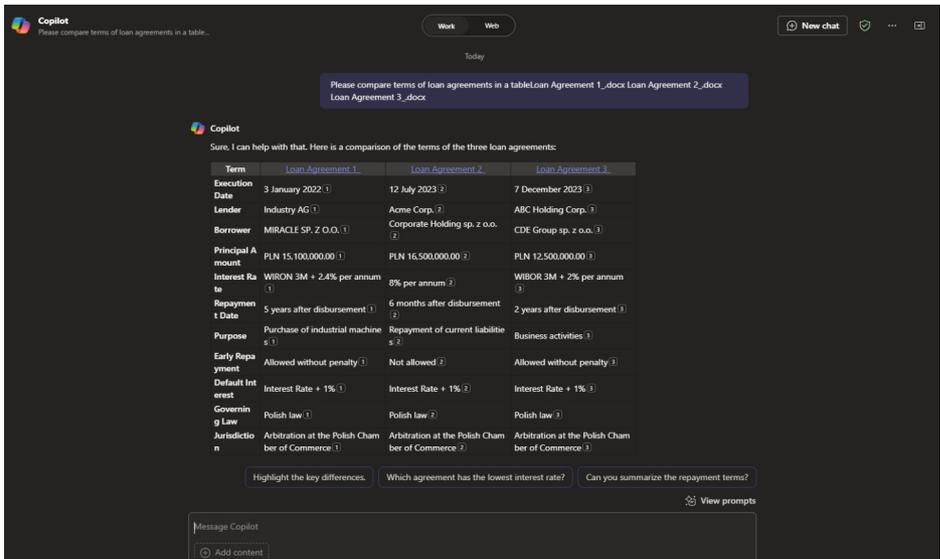


- ✓ prepare a summary of information available here: <https://legislacja.gov.pl/projekt/12301402/katalog/13093700#13093700>
- ✓ incorporate the following text into the note below in a manner that ensures the updated content is consistent and logical.
- Based on the information available on the Government Legislation Centre's website, the draft regulation of the Minister of Climate and Environment on the detailed conditions for granting public aid by the National Fund for Environmental Protection and Water Management for investments in electricity storage and related infrastructure (listed as number 1214) is currently in the public consultation phase. The draft was published on November 6, 2024.
- ✓ indicate the date of the information at the beginning of the text.

EXAMPLE 7 – COMPARING THE CONTENT OF DOCUMENTS (COPILOT OPTION IN TEAMS)

- Enter the prompt “Compare contract terms in a table form” and save the relevant documents, which you download from Onedrive.

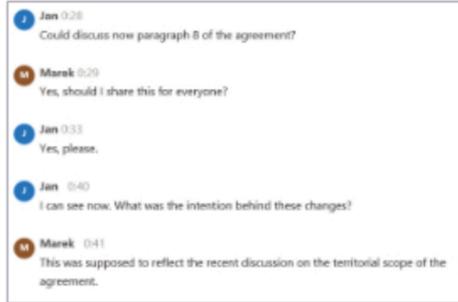
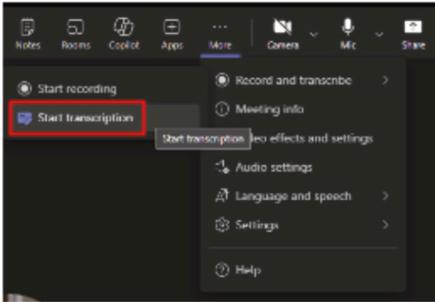
Comparison of the content of documents



EXAMPLE 8 – SUMMARY OF MEETINGS IN MS TEAMS

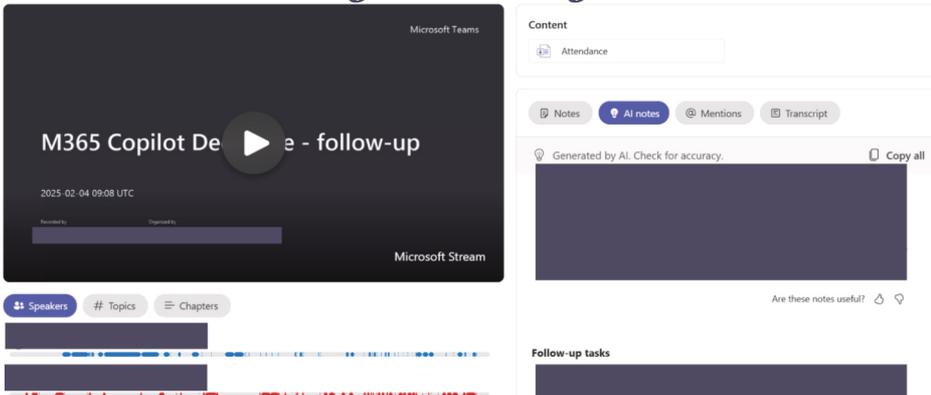
- After enabling the “Start transcript” option, the transcript of the conversation will appear in the right sidebar of the screen.

Transcriptions in MS Teams



- When the meeting is over, a window will appear with the recording and a list of participants and a line indicating when that person spoke. By selecting a place on a particular participant’s line, we can listen to the recording at the moment that participant spoke.
- To the right, there will be a summary from the meeting with a list of follow-up tasks and the persons who were assigned to perform the task at the meeting.
- The entire transcript of the meeting is also available.
- Due to the peculiarities of the Polish language, sometimes transcription errors may appear, especially when the interlocutor uses proper names or terms in a foreign language. Be sure to read the summary and the list of supplementary tasks.

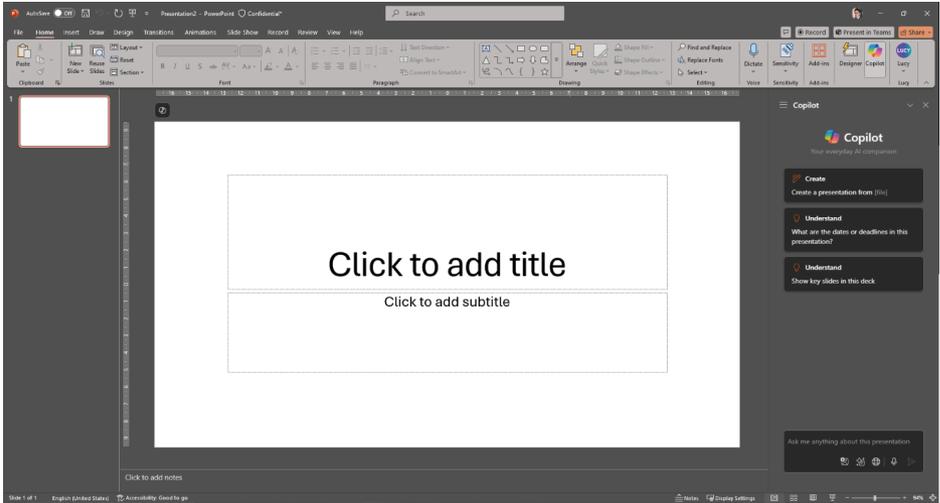
MS Teams meetings summary



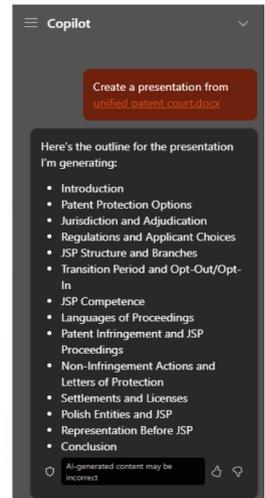
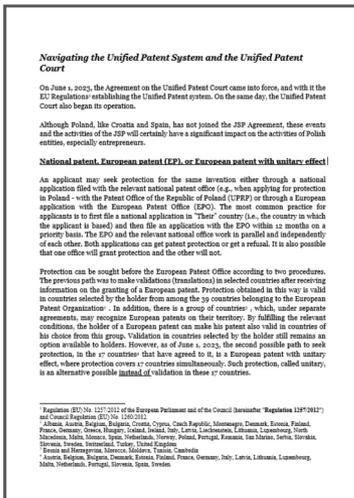
EXAMPLE 9 – CREATING A POWERPOINT PRESENTATION BASED ON A DOCUMENT (example: a note on the unitary patent and the Unified Patent Court)

- In PowerPoint, click the Copilot icon and ask to prepare a presentation based on a specific document (it must be saved on Onedrive).

Create presentations based on documents



Create presentations based on documents



Appendix no. 2

- You will receive a preliminary draft of the presentation with suggested notes.



EXAMPLE 10 – CREATING A DECLARATIVE M365 COPILOT AGENT

The example below offers steps for creating a sample Declarative Agent from within the M365 Copilot Chat application. Similar functionality is available from the SharePoint application. The Agent can be further extended with automation or standalone functionality through the Copilot Studio application.

- Provide information that identifies the Agent and add a prompt that acts as Instructions that define the Agent's behavior in interactions with the user.

Details

Name

Description

This is an agent curated on selected DORA (the Digital Operational Resilience Act) materials published by Microsoft.

Instructions

- Offer responses on DORA regulatory compliance and information based only on the source documents
- Ensure responses are accurate, concise and helpful. Avoid providing any unofficial or speculative information.
- Maintain a professional and supportive tone in all interactions
- Advise the requestor to seek proper legal and regulatory guidance as appropriate.

Appendix no. 2

- Add the sources to be used by the Agent (e.g. files / folders / pages in the SharePoint database, external sites, other databases).

The screenshot shows the 'Knowledge' configuration page. At the top, there is a 'Knowledge' header with a refresh icon and an information icon. Below it, a text box explains that users can select folders and files or add a website, with a limit of 20 knowledge sources and a 'Learn more' link. There are two input fields: one labeled 'Browse' and another for entering a URL for a public website or SharePoint location. The 'Web' section has a 'Web search' toggle switch that is turned on. The 'SharePoint' section shows a 'root' folder with a SharePoint icon and a three-dot menu. The 'From your organization' section lists three connectors: 'Azure DevOps Wiki' (0/13 active), 'Azure DevOps Work Items' (0/11 active), and 'Custom Connector' (0/2 active). A 'See more (+5)' link is at the bottom.

- Give examples of the questions that users can use.

The screenshot shows the 'Starter prompts' configuration page. It has a header with 'Starter prompts' and an information icon. Below the header is a table with two columns: 'Title' and 'Message'. There are three rows of prompts, each with a trash icon and a three-dot menu icon to its right. At the bottom, there is an 'Add new' button with a plus icon.

Title	Message		
Obligations	What are the obligations imposed on financial services providers ur	🗑️	⋮
ICT Risk	Can you explain the ICT risk governance and management requirer	🗑️	⋮
Customer Questions	What are customers in the banking sector most likely to ask a techn	🗑️	⋮

Appendix no. 2

- Now you can enroll and test the Agent.

New chat



Dora - Microsoft Ext Resources

This is an agent curated on selected DORA (the Digital Operational Resilience Act) materials published by Microsoft.

Obligations
What are the obligations imposed on financial services providers under DORA?

ICT Risk
Can you explain the ICT risk governance and management requirements under DORA?

Customer Questions
What are customers in the banking sector most likely to ask a technology service provider like Microsoft regarding compliance with the EU DORA regulation?

Type your message
0/2000

➤

Appendix no. 2

The screenshot shows a Microsoft Copilot chat window titled "Dora - Microsoft Ext Resources" with the subtitle "EU DORA Compliance Queries for Banking Sector". A "New chat" button is in the top right. A blue box contains the question: "What are customers in the banking sector most likely to ask a technology service provider like Microsoft regarding compliance with the EU DORA regulation?".

The chat response is titled "Dora - Microsoft Ext Resources" and contains the following text:

Customers in the banking sector are likely to ask a technology service provider like Microsoft several questions regarding compliance with the EU Digital Operational Resilience Act (DORA). Here are some common queries:

- 1. ICT Risk Management:** How does Microsoft help financial entities establish a governance framework for ICT risk management and monitor these risks continuously? Customers may inquire about specific tools and services, such as Microsoft Defender for Cloud, Microsoft 365 Service Health Dashboard, Microsoft Secure Score, Azure Service Health, and Microsoft Purview [1].
- 2. Incident Management and Reporting:** How does Microsoft support financial entities in managing, classifying, and reporting ICT-related incidents? Customers might be interested in tools like Microsoft Defender, Microsoft 365 Compliance Center, and Azure Sentinel for efficient incident detection, investigation, and reporting [1].
- 3. Digital Operational Resilience Testing:** What solutions does Microsoft offer for conducting digital operational resilience tests, including threat-led penetration testing (TLPT)? Customers may want to know about Microsoft's penetration testing program and other related services [1].
- 4. Contractual Requirements:** What specific contractual commitments does Microsoft offer to align with DORA and ESA guidance? Customers might ask about Microsoft's Data Protection Addendum, Product and Service Terms, and Financial Services Amendment [1].
- 5. Oversight of Critical ICT Providers:** How is Microsoft preparing to meet the requirements under DORA as a critical ICT service provider? Customers may inquire about Microsoft's compliance with DORA provisions and its engagement with industry stakeholders [2].
- 6. Business Continuity and Recovery:** How does Microsoft support financial entities in developing resilient setups and meeting DORA's business continuity requirements? Customers might be interested in solutions like Azure Site Recovery and Microsoft 365 Syntex Backup [1].

These questions reflect the key areas of concern for financial entities as they work to comply with DORA and ensure their digital operational resilience.

If you have any specific questions or need further details, feel free to ask!

At the bottom, there is a chat history bar with three items: "Microsoft General - Financ...", "Microsoft General - Micro...", and "Guide_Microsoft Product...". A "Show more" button is to the right. Below this is a follow-up question: "Can you provide more details on Microsoft's penetration testing program?". At the very bottom is a "Message Copilot" input field with a microphone icon on the left and a send icon on the right.

