Notaries of Europe

Providing legal certainty

AI HANDBOOK FOR EUROPEAN NOTARIES

This document has been prepared with the aim of encouraging reflection on artificial intelligence within the European notariat. It is intended solely for internal use within the CNUE network and is not intended for public dissemination.

Table of Contents

I. Introduction and purpose of the Handbook

Even if known in various forms for a long time, artificial intelligence (AI) became a visibly disruptive technology in the previous decade. The large amount of digital data produced every day and the previously unimaginable computational power jointly contributed to the growth of AI from simple software to an extremely powerful tool, capable of transforming processes, professions and also the way people live their lives. New AI solutions enter into our lives with lightning speed (e.g. the generative AI models), creating new phenomena, opportunities but also presenting new risks. Therefore, it is not surprising that the European Union legislator aimed at comprehensively regulating this technology, with the adoption of the Artificial Intelligence Act (AI Act) which is the first set of legal provisions applicable to this field worldwide.

Nowadays, AI deployment is widespread in everyday life and also in a high number of professions. The legal sphere is not an exception to that: attorneys-at-law, judges, company legal counsels and the State-administration legal professionals have already been using general and special AI solutions. Just like lay people, legal professionals can enjoy the benefits of using AI. At the same time—as mentioned above—AI is not without risks and dangers, which must be thoroughly taken into consideration. Often—not without any reason—legal professionals adopt the attitude of fear of these risks and dangers, and hence are reluctant to make use of AI.

The present Handbook aims at getting the notaries of Europe closer to AI technology, by presenting the potential ways of use of the multitude of AI solutions that presently exist. At the same time, this Handbook highlights the most important, already identified risks of such uses, in order to guarantee the legal security and the high level of professional services that notaries are accustomed to provide even when this technology is not deployed.

The application of the information and statements in the Handbook is entirely voluntary. Notarial organisations and individual notaries are free to take different steps and approaches, depending on their own decisions and the laws applicable to them.

Although the aim of the Handbook is not to make notaries experts of AI technology, the present document contains a comprehensive and thematic glossary clearly explaining the most important technological terms which are related to AI and with which notaries can be confronted in different circumstances. This enables the notarial profession to adopt a multidisciplinary approach by combining technology and law at an even more complex and sophisticated level than in the past.

It must be emphasised already in this Introduction, that in its current form, AI is not able to replace the notaries. AI is a technology which can be used to assist the notaries in their everyday work and if it is done appropriately, it may result in higher quality services and an enhanced efficiency, allowing notaries to concentrate more on difficult legal matters than routine tasks.

The Handbook also aims at leading the readers through the potential benefits of AI for notaries and notarial organisations. Although the basics of the notariat are similar or the same in the 22 countries of the EU having the Latin-type notarial system (also members of the Council of the Notariats of the European Union – CNUE), there can be also significant differences, depending on the legal, economic and social circumstances as well as the historical developments of the given countries. This may also significantly affect the use of AI applications. Therefore, the Handbook aims at being 'notariat-neutral', meaning that the information in this document is appropriate for and beneficial in the 22 States. Country-specific information (e.g. on specific AI solutions already in use by the notaries of a given State) and proposals do not form part of the present Handbook. References to them are only made when it is necessary to elaborate on the given topic.

Although the Handbook does not aim at establishing any European notarial AI system(s) to be applied across the 22 notariats of Europe, its statements can be used for such AI systems in case all members of the CNUE decide to set up such a system.

In the present document the risks and dangers linked to the use of AI are presented in details and potential solutions are proposed to mitigate or—if possible—to avoid them. As the AI Act mentioned above is applicable independently from the profession of the developer or deployer, the provisions that must or may be applied to the notariat as AI developer/deployer are also identified and analysed within the Handbook. This gives the opportunity for the notariat to prepare well in advance to the compliance with the provisions of the AI Act which will be fully applicable from August 2026.

Finally, the current version of the Handbook reflects the state-of-the-art technology the related information on which became public until 17 February 2025 and the legal provisions in force at the time of its adoption by the CNUE. However, due to the extremely fast development of the AI, the Handbook requires regular updating.

II. Glossary

This thematic Glossary aims at explaining the most commonly used terms related to artificial intelligence (AI), providing an easy understanding of the often technical vocabulary which is necessary to understand AI. The glossary does not follow the alphabetical order of the words, its content is grouped around the terms which come up in a similar context and/or follow a logical order from the general to the more special. The terms in the Glossary appear in the text of the Handbook under the different chapters, therefore they are not separately defined later on, however hyperlinks help the reader to get back to the relevant part of the Glossary.

It is important to note that—with some indicated exceptions—the definitions below are not official ones. Different specialists have different visions and understanding of the AI-related terms. Moreover, the actual meaning of the terms changes and evolves over time, depending on the new technological developments, legislation and use cases. Therefore, the aim of the Glossary is not to formulate definitions to be made official but to give a proper understanding of the terms with which notaries can be confronted in the more and more AI-driven world.

The examples under the present Glossary aim at explaining the definitions in practical context, focusing on the notariat. They do not necessarily represent real use cases. However, subject to regulatory permission or in the absence of prohibition, they reflect cases which might have already occurred or which might occur in future within the notarial profession. Furthermore, the examples explain a specific term without specifically highlighting all potential risks surrounding them. The latter can be found in various chapters of the present Handbook.

1. General terms

a) Artificial intelligence (AI):

Artificial intelligence is a branch of computer science with algorithms that can—independently from human intervention—make decisions, predictions, content and recommendations in the form of outputs. AI is able to carry out simple and even complex tasks that previously could only be performed by humans.

Despite its denomination, AI is not considered as intelligence in the human sense of the word. AI cannot think and understand the tasks it performs the way humans do. Moreover, it currently cannot put situations properly into context and neither can it make abstractions. AI systems can excel in specific tasks, but are not able to transfer this ability to the ones they are not programmed for.

Even if the term 'AI' is imprecise, the scientific literature, lay people and also this Handbook refer to software that fits the above description as 'artificial intelligence' (AI). As it is indicated below, AI comprises various technologies. Therefore, AI is used as an umbrella term for further discussions.

b) AI system:

'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' (AI Act definition, Article 3 (1)).

AI systems integrate one or more AI model(s) to perform specific tasks. The AI system is the operational framework. In addition to AI models, AI systems include the following main components: data collection and processing (for gathering and preparing training data for the model), user interface (by which users interact with the system, e.g. applications), and infrastructure (hardware and software necessary to operate the system).

For further (non-binding) guidance on the definition of 'AI system' see the *'Approval of the content of the draft Communication from the Commission – Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)'*.

c) AI model:

An AI model is the most important component of an AI system incorporating an algorithm. It is a mathematical or statistical representation of a specific problem, developed from data. AI models are trained to recognize patterns, make predictions or decisions based on data and to carry out a precise task.

2. Terms related to data and machine learning

a) AI data governance:

AI data governance focuses on managing the data used by AI systems and deals with the questions of data quality, integrity, legality, privacy, security and the usability of the data by the respective provider/deployer. Within the data governance framework, the provider/deployer sets up policies, standards and procedures for the collection, cleansing, annotation, storage, analysis and use of data with the aim of ensuring their compliance with legal as well as ethical rules.

In addition to supporting the needs of the provider/deployer, an appropriate data governance framework helps the mitigation of risks (e.g. personal data breaches, bias and discrimination) and contributes to the transparency of the AI development and use, enhancing trust in the framework. Within the data governance framework, organisational roles and responsibilities, as well as technical steps are established, and the framework has to be regularly audited and updated to keep up with the changes of legal rules and technological developments.

Example for the notariat: A notary uses an AI solution for the automatisation of processing large legal documents. A proper AI data governance framework ensures that the data used by him/her, such as personal (e.g. the name of the client) and non-personal confidential data (e.g. client's trade secrets) are kept secure and their handling is compliant with the relevant legal provisions. This includes, among others, rules about the persons with right of access to the data, the permitted duration of storing them, and the ways of protection.

b) Text and data mining (TDM):

TDM is an automated process of digitally selecting and analysing large amount of content (text and/or data), using various computational and statistical techniques (most often natural language processing) with the purpose of discovering hidden patterns, trends, relations and other useful information.

TDM can be divided into the following two sub-categories:

- Data mining is the computational process of discovering and extracting patterns and knowledge from structured data.

- Text mining does the same, but with unstructured raw (text) data. Text mining can be considered a specific form or the pre-processing phase of data mining, in which the unstructured textual data is first transformed into structured data which can subsequently be analysed more efficiently. Therefore, the term text and data mining are both commonly used.

TDM can help service providers to—among others—make predictions and better decisions.

Example for the notariat: A notarial chamber intends to analyse documents on real estate in order to discover current trends and to predict possible future issues in the sector. The organisation can make use of TDM to analyse a huge amount of relevant documents to identify patterns and trends and to get predictions. This helps the profession to streamline its actions and to prepare for future situations.

c) Training data—validation data—testing data:

'Training data means data used for training an AI system through fitting its learnable parameters' [AI Act definition, Article 3 (29)]. Training data is used to train the AI model by learning to carry out pre-determined tasks (e.g. make suggestions for decisions). Training data usually comes from human input, specific training datasets or from machines (e.g. sensors). Depending on the purpose of the AI system, the training data can be diverse: text (e.g. legal acts, contracts), image or video (e.g. for facial recognition), human speech (e.g. for dictating) and sensor data (e.g. for biometric verification). Training data can be labelled or unlabelled. The former uses labels helping the identification of similar objects, patterns, emotions, etc., the latter is without tags or labels.

'Validation data means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process in order, inter alia, to prevent underfitting or overfitting.' [AI Act definition,

Article 3 (30)]. Based on the validation data, the training of the AI system is assessed and the best model is chosen for the given task. The validation phase also gives an opportunity to fine-tune and further develop the model.

'Testing data means data used for providing an independent evaluation of the AI system in order to confirm the expected performance of that system before its placing on the market or putting into service.' [AI Act definition, Article 3 (31)]. Testing data determines how good the model really is. If a given benchmark is not reached, better training data should be given, and the training should be restarted. When the model reaches the benchmark, the model can be approved.

In order to guarantee the objective testing results, the merging of the validation and testing data is not allowed. The testing data should be close to the real world and the testing should be carried out always with previously unseen data.

Example for the notariat: A notarial chamber develops an AI solution to assist notaries in detecting missing clauses in their acts. The AI model is trained on a large amount of adequately prepared (e.g. anonymised) contracts from the past (training data). After training the system, the model gets a dataset (validation data) to carry out its first evaluation. During this phase, small imprecisions of the model are detected, which are solved before the model is carried into the testing phase. During testing, the model receives completely different contracts from those used in the validation phase (testing data) to confirm the model's accuracy before its deployment by the profession. Upon 'passing the test', the AI solution is ready to be used by notaries.

d) Synthetic data:

Synthetic data is artificial data generated from original data reproducing its characteristics and structure. Synthetic data mimics real-world data. In practice, it helps training machine learning algorithms when real-world data is of limited quantity or sensitive. The use of synthetic data is especially useful to avoid personal data protection issues while training the AI model.

Example for the notariat: The dataset available for a notarial chamber to train its AI model for assistance in drawing up contracts (under development) contains personal data which should be anonymised. However, thinking of the dangers of de-anonymisation (re-identification), the chamber decides to generate synthetic data (e.g. fake contracts with correct legal information but without personal data) based on real-world data to train the AI model without risking the privacy and personal data of clients.

e) Personal data, non-personal data:

'Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' [GDPR definition, Article 4 (1)]

Non-personal data is all data not falling under the previous category.

Example for the notariat: Personal data can be, among others, the name, date and place of birth, address and personal identification numbers of clients. Notarial acts also include a wide variety of non-personal data such as the purchase price, the capital of the company under establishment, the interest rates, etc.

f) Pseudonymisation and pseudonymised data:

'Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.' [GDPR definition, Article 4 (5)]. The original data is replaced with a pseudonym. Pseudonymisation is reversible, and allows re-identification later on. It is a data protection method recommended in the GDPR. Since the process of pseudonymisation is reversible using the given key, pseudonymised data are still considered personal data according to the GDPR.

Example for the notariat: In order to protect the privacy and personal data of clients in automated systems, the notary/notarial organisation replaces personal data with pseudonyms. For instance, the name of the client is replaced by a unique identifier, enabling the retrieval of the real data behind only to those having the necessary entitlement (key).

g) Anonymisation and anonymised (de-identified) data:

If the data is anonymised, it is—in principle—irreversibly altered, meaning that the individuals behind them can no longer be (directly or indirectly) identified, which results in that the GDPR does not apply anymore. The de-identification process involves encrypting, masking, generalizing, perturbing or deleting both the direct and indirect identifiers.

Example for the notariat: A notarial chamber intends to develop an AI system for its member notaries. Before training the system, the chamber anonymises the personal data of the clients in the relevant training material. This means the removal of names, birthplaces and birthdates, addresses, personal identifiers and any other data on the basis of which the given natural person can be identified.

h) De-anonymisation (re-identification):

Personal data de-anonymisation is the method of matching anonymised data with publicly available information, or auxiliary data, by using technology in order to identify the person the data belong to. De-anonymisation reverses the process of anonymisation. Information can be retrieved from the available dataset to put together a person's identity.

Example for the notariat: In case one is able to cross-reference the anonymised data in a notarial act with publicly available information (like for instance from the electronic land registry), the given person might also be able to identify the individual behind the specific transaction. Therefore, this risk requires extremely circumspect proceeding from the notariat also in case of AI development and use.

i) Data collection/acquisition:

Data collection/acquisition is the process of collecting raw data for AI training. The collected data has to be of a large amount, high-quality and representative enough for the purpose of the AI model. The collection of real-world data is the most ideal solution, but in case of insufficient amount of such data, synthetic data can help to fill in data gaps.

Example for the notariat: For the training of a notarial AI system, the developer chamber gathers the necessary data from various sources which can be—among others—databases, public registries, legal literature and, subject to legal permission and in the absence of the objection of the notary drawing them up, contracts, and other notarial deeds.

j) Data labelling / Data annotation:

The process of giving tags/labels to the training data or part thereof. This solution is mostly used for supervised learning.

Example for the notariat: A machine or a team of experts puts labels on training data within documents for the sake of identifying the key information, such as the purchase price, the interest rate or the jurisdiction and applicable law clauses. This helps the AI system to recognise the same or similar types of data in other documents.

k) Data cleansing:

The process of responding to issues regarding data which includes for instance the correction of errors, the removal of irrelevant, duplicated or inconsistent data, as well as solving the issue of incomplete datasets.

Example for the notariat: Before training its AI model, the developer chamber must clean the data collected. This can be, for instance, the removal from the dataset of deeds drawn up based on legislation not in force anymore, or data which occur several times unnecessarily in the given dataset.

l) Training of artificial intelligence:

The activity of feeding the training data into the AI algorithm.

Example for the notariat: The developer notarial chamber feeds data from various sources into the system, enabling the algorithm to carry out its pre-determined task.

m) Machine learning (ML):

Machine learning is a type training method of AI models. With the use of ML, algorithms learn from data without being explicitly programmed.

Example for the notariat: By using labels, patterns and correlations in the data fed into the AI system, the model can 'learn' itself and, by time, gets better and better in how to identify features in contracts and how to ameliorate, amend, etc. specific contracts, helping the deployer notary in the drawing up process.

Three main types of ML methods exist:

– **Supervised learning:** the AI model is fed with labelled data, the labels are the output the AI must learn to produce, just like in the physical world students learn from the examples provided by the teacher and give this knowledge back at the exam. The AI trained with supervised learning is capable of correctly recognising unlabelled data. Examples of use cases of supervised learning are—among others—classification, speech recognition and sentiment analysis.

Example for the notariat: The notary can use AI solutions trained by supervised learning to classify their acts based on previously labelled data. This solution facilitates—among others—the retrieval of documents at a later stage.

– **Unsupervised learning:** the AI model is given unlabelled data without any help in order to find itself patterns and correlations among them. The AI model trained this way can often find and identify unusual patterns helping to get more efficient solutions. Unsupervised learning is used for example for the extraction of features.

Example for the notariat: After finding patterns and correlations in the training data, the AI solution can help the notary to make a summary of information in large volume documents, accelerating the identification of the most important points of the specific documents.

– **Reinforcement learning:** in this case, upon performing a series of actions, the AI model regularly gets feedback which has the form of 'reward' (for correct actions) or 'punishment' (for incorrect actions). The AI model registers the consequences of its steps, and based on them, adjusts its future steps and starts making better decisions.

Example for the notariat: The AI solution which is being trained with the method of reinforcement learning, for instance, for the verification of the completeness of the notarial acts, receives a 'reward' (positive feedback) in case the output is correct (i.e. the AI suggests a correct clause to add or detects correctly that the contract is complete) and a 'punishment" (negative feedback) if the output is incorrect. Thanks to this method, the AI model becomes more and more accurate and reliable.

n) Neural network:

A neural network is a machine learning model using processes mimicking the way biological neurons in the human brain work together to identify phenomena, weigh options and arrive at conclusions. Neural networks consist of layers of nodes (which are artificial neurons): an input layer, one or more hidden layers, and an output layer. The nodes connect to each other, and have their associated weights and thresholds. If the output of any node is above the specified threshold value, that node is activated, sending data to the next layer of the network. One of the most famous examples of a neural network is Google's search algorithm.

o) Deep learning:

A neural network that consists of more than three layers is considered a deep learning algorithm. Deep learning is thus a type of machine learning using artificial neural networks with multiple layers in order to learn complex patterns in large amounts of data. Deep learning is used in applications like speech recognition and natural language processing.

p) Data poisoning:

A type of cyberattack in which a training dataset used by an AI model is intentionally compromised to manipulate the operation of the model. It can be done in several ways like injecting false information in the training dataset, modifying or deleting (part of) the dataset. The possible consequence of the data poisoning is the unreliable and inaccurate output by the AI system. When a breach is detected, it must be traced back and the dataset restored. In some cases, the model needs to be completely retrained.

Example for the notariat: In the training dataset of an AI system used by notaries to detect the compliance with the law in force, somebody intentionally introduces data on outdated legal texts ('poisons' the training dataset). As a result, the AI gives incorrect suggestions based on legal provisions not in force any more.

3. Types and main uses of artificial intelligence

a) Rule-based systems:

In the earliest versions of natural language processing applications 'if-then' statements were formulated which relied on a predefined set of explicit rules. Rule-based systems are only able to provide answers to specific user inputs in specific domains, limiting their capabilities compared to machine learning systems by not being able to handle complex situations and adapt to them.

However, the advantage of rule-based systems is the transparency and subsequently the ease of interpretation of the decision-making process by the system. Rule-based systems are efficient in dealing with well-defined issues. Moreover, updating of the system and solving its errors is easier than in case of sophisticated machine learning systems.

Example for the notariat: A notarial chamber develops a chatbot for helping clients in getting basic information about the law. For instance, in case of question if a certain type of contract can be drawn up validly without notarial intervention, the rule-based chatbot can provide a clear 'yes' or 'no' answer.

b) General purpose AI (GPAI) models / Foundation models

'AI models that display significant generality, are capable to competently perform a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications.' [AI Act definition, Article 3 (63)].

A foundation model is a deep learning model that serves as the basis for several different types of generative AI applications. As these models are capable of performing a wide range of general tasks, they are different from the so-called narrow AI systems which focus solely on a specific task like, for instance text generation. For the training of foundation models, enormous amount of raw and unlabelled data is needed (mostly scrapped from the internet), and they can be used for different tasks with minimal fine-tuning (adding additional datasets and not starting the development from scratch).

These models are made available to downstream developers through application programming interfaces (API), often open-source. Examples of GPAI models are GPT-4, DALL-E, Google BERT.

GPAI models have been for long in the focus of the EU legislator while working on the AI Act because they are bases for a range of applications (e.g. OpenAI's foundation model GPT-4 of Microsoft's Copilot), and any error at the GPAI level may negatively impact any applications built on top of them. Moreover, GPAI models use also 'transfer learning' meaning that they apply learned patterns from one task to another.

c) Generative artificial intelligence (gen AI):

Generative AI can create content—such as coherent and relevant text, images, video, audio, speech or software code—on demand, upon the deployer's input. One of the most widespread gen AI is the ChatGPT. Gen AI is most often based on foundation (GPAI) models tuned to a specific content generation task. The most developed generative AI model architecture is the so-called transformer (GPT means: Generative Pre-trained Transformer) which is able to generate articles, artistic works and not only simple answers to questions. Transformer models can also be trained to use additional tools to create output in a specific format.

From the negative characteristics typical to generative AI can be mentioned the hallucinations, the different outputs given to the same inputs, the generation of biased outputs and the lack of explainability.

GPAI and gen AI example for the notariat: A notarial chamber as a downstream developer decides to integrate from a trusted foundation model developer a GPAI based on individually agreed contractual terms (guaranteeing the compliance with notaries' legal obligations). The model is trained on a large amount of legal data from the country of the chamber. After fine-tuning the model for specific notarial purposes and creating a proper generative AI system within the specific notarial chamber, notaries are able to make use of it, for instance, by automatically generating the first drafts of their acts.

d) Unimodal and multimodal AI:

Modality refers the type of data which can be processed by AI systems. These are for instance text, image, audio, video or multimedia data.

Unimodal AI systems can only process one type of modality (most often text) and provide only the same type of output.

Multimodal AI is capable of processing multiple modalities of data input and generate the same or different modalities of output. An example of a multimodal AI system is OpenAi's GPT-4V(ision), which can process text and image (both on the side of input and output). A multimodal AI system consists of numerous unimodal neural networks.

Multimodal AI systems require larger amount of different data but in exchange are able to recognise patterns and connections between different types of data inputs, and produce more accurate output.

Example for the notariat: A unimodal AI processes large amounts of texts which the notary must revise and makes the first (written) summary of those texts as an output. A multimodal AI is capable of combining for instance, the draft text of the act (written format) and the orally presented needs of the client (audio format) into a second draft of the specific notarial act.

e) Large language models (LLMs):

Large language models use deep learning technology, possessing sometimes hundreds of billions of parameters and are trained on immense amounts of textual data (billions of pages). They recognise and generate in a human-like manner natural language and other types of content in order to deal with a multitude of tasks. They are able to generate coherent and relevant responses to questions (e.g. chatbots and virtual assistants), autocomplete sentences, translate documents, summarise text (e.g. for research) or generate content (like articles) or even computer codes.

Tokens are the basic units of input and output in an LLM. Tokens typically represent words, or characters. During training, the LLMs process input text as a sequence of tokens.

LLMs learn to autonomously predict the next character or word (token) in a sentence based on the preceding words and context, by attributing a probability score to the recurrence of words. The output is a coherent and contextually relevant text. This technology is widely used in e-mails making suggestions for the next word(s) while writing. During use, the performance of LLMs can be enhanced by prompts given by deployers.

LLMs are among others used in natural language processing and are well-known for instance in Open AI's ChatGPT or Meta's Llama.

f) Natural language processing (NLP):

Natural language processing is a branch of AI that applies machine learning, deep learning and linguistics to enable computers and various other devices to detect, recognise and capture human text and speech and communicate with it. NLP requires huge amounts of labelled training data. NLP technology is widely used in search engines, chatbots, virtual assistants, grammar correction applications, machine translation and voice-operated systems. Moreover, NLP models help filter personal data in large volumes of text, identify spam e-mails (e.g. by identifying bad grammar), summarise long text files and generate human-made-like texts.

Some factors influence the proper functioning of the NLP technology. These are among others the biased training data, the low quality or confusing input (e.g. use of incorrect grammar, idioms and newly created words, excessive background noise, accents). Even in human-to-human communication, language is full of ambiguities which either cannot be programmed into AI or can but not without huge difficulty. Therefore, a big challenge of AI programmers is to tackle these issues.

The most common types of NLP in practice are as follows:

- **Speech recognition (speech-to-text):** Speech recognition is the process of transformation of human voice into written text data (the speech is the input and the written words are the output of the system). This technology involves linguistics, mathematics and statistics. Among others, the following factors can impact the error rate of the system: bad pronunciation, accent, volume, and background noise.

  Speech recognition is not to be confused with voice recognition which aims to identify an individual's voice.

> **Example for the notariat:** The notary has the task of drawing up an act which contains the minutes of a meeting. He/she uses a speech recognition AI to transform the oral statements during the meeting into text data. This solution accelerates the notarial work by freeing the notary from the task of manually typing long pages.

- **Natural language generation (NLG):** NLG is the process of putting structured data into conversational (written or oral) human language. Amazon's Alexa and Apple's Siri are two everyday examples of this technology.

> **Example for the notariat:** The notary is confronted during his/her practice with documents which use a specific language with terms that are not easily understood by legal professionals (e.g. technical and architectural documents on real estate, financial statements, etc.). In order to facilitate the first understanding of such content (and before consulting an expert of the field, if necessary) NLG solution is applied to make an easy-to-understand summary of the given document.

g) Computer vision:

Computer vision is a field of AI using machine learning and neural networks to teach computers to gain meaningful information from digital images, videos and other visual inputs. This technology works similarly to human vision. For computer vision to work, we need sufficient computing power and a big amount of training data which it analyses until it recognises images with appropriate accuracy. Computer vision is especially used nowadays for image classification, object detection in an image or video and subsequent object tracking, as well as for automatic image annotation.

One of the best-known real-life applications of the computer vision technology is the function of Google Translate which makes it possible for people to point the camera of their smartphones/tablets to a text in one language and to get the translation in another one. Besides, self-driving vehicles make essentially use of the computer vision technology.

h) Facial recognition:

Facial recognition is an AI application that identifies a person or verifies a person's identity using the features of his/her face in an image or video. This can be done by determining if faces in two or several images belong to the same person or finding the face in a large visual dataset. One of the most widespread uses of this technology is the facial recognition by mobile devices but it is also used in other security solutions.

i) AI emotion recognition and sentiment analysis:

'Emotion recognition system' means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data' [AI Act definition, Article 3 (39)].

Based on Recital 18 of the AI Act, this *'notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It does not include physical states, such as pain or fatigue. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.'*

AI emotion recognition is a branch of AI enabling computers to analyse non-verbal signs such as facial expressions, body language, gestures, and voice tones to assess (analyse, interpret and classify) the emotional state of natural persons. AI emotion recognition uses computer vision technology and deep neural networks that involve facial emotion detection and sentiment assessment from visual data (images and videos) and also text analysis (even if the latter—due to the lack of biometric nature—is not included into the definition of the AI Act).

Most training databases for AI emotion recognition consist of 2D static images or 2D video sequences; sometimes 3D images. The emotions an AI model can detect depend on the trained classes (e.g. anger, fear, happiness).

Example for the notariat for computer vision, facial recognition and sentiment analysis: A notary has the task of drawing up a remote authentic act (i.e. an act without the physical presence of the client, via videoconferencing, in a country whose legal system permits such proceedings). Among other things, the notary has to make sure the client's identity, the appropriateness of his/her surroundings for the safety of the videoconferencing and the free will of the client are not compromised (e.g. he/she is not under threat). With the help of facial recognition technology, the notary may get technical assistance to verify the identity of a client. The AI compares the client's face with the photo on the ID-document in order to ensure that the person is truly the one he/she claims to be. Besides, in the same remote process, the emotion recognition and sentiment analysis technology may assist the notary in verifying that the client is not under pressure, since if the presence of pressure is detected, the notary has the obligation of not concluding the task at hand or of asking the client to show up personally at the notarial office. Besides, other computer vision solutions may be used during the procedure to assist the checking of the surroundings of the client by the notary to make sure that no element is present which can compromise the legality of the procedure.

4. Terms related to the types and uses of AI systems

a) Parameters and weights:

Parameters govern how the model learns and generates output. The LLM model size is the number of parameters: the more parameters a model has, the more complex it is and the more data it can process. The parameters for the LLM depend on the specific task for which they are used. For complex tasks, a model with a large number of parameters is required.

Weights are a subset of the parameters representing the strength of connections between variables. During the training process, the LLM adjusts the weights to optimise its performance, i.e. to minimise the error between the predicted output and the actual output.

b) Prompts:

Prompts are input queries provided by the deployers of generative artificial intelligence systems. These systems generate specific outputs based on the prompts.

Generative AI relies on the repetitive refinement of different prompts to effectively learn from input data and to produce more accurate responses (outputs). The role of the so-called prompt engineering is to craft and fine-tune queries that help generative AI models capturing nuances of the given query, enhancing the quality of the AI-generated content, with minimal post-generation review.

Example for the notariat: The notary wishes to use an AI solution to extract the clauses of a sale and purchase contract related to obligations of the seller. In order to get them, one of the possible formulations of the prompt the notary has to type or dictate into the system is: *'Extract the clauses related to the obligations of the seller.'* The more precisely the prompt is formulated, the better and more precise is the quality of the output.

5. Main participants of the AI ecosystem

a) Provider:

'Provider means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.' [AI Act definition. Article 3 (3)]

Example for the notariat: The provider of notarial AI systems can be, for instance, the notarial organisation (chamber) the individual notary is member of (internally developed AI system) or any other external entity (externally developed AI system) which develops such systems for use by notaries.

b) Deployer (user):

'Deployer (or user) means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.' [AI Act definition, Article 3 (4)]

Example for the notariat: The deployers or users of AI systems can be the notarial organisations (chambers) or the individual notaries themselves.

6. Issues and phaenomena related to the AI

a) AI hallucination:

AI hallucination is a phenomenon related to LLMs—most generally to generative AI models—perceiving non-existent patterns or objects and creating inaccurate outputs, which often seem entirely realistic and which are capable of misleading the deployer.

It is important, that AI hallucination is not equivalent to human hallucination, the term is only used to describe this phenomenon.

Several ways are known to tackle AI hallucination, such as the use of high-quality training data, setting the exact purpose of the AI system, limiting the output responses, continuously testing the model and—most importantly—exercising human oversight and validation of the AI output.

Example for the notariat: A notary wants to access the case law related to transactions of crypto-assets. The system lists and describes cases which have never existed and have no basis. By giving these fake output results, it gives the impression that such cases are real cases. By checking the AI suggestions, the notary identifies the cases made up by the AI system.

b) Black box AI:

Black box AI means the difficulty or the impossibility of understanding the AI decision-making process. Very often, even the engineers or data scientists developing the applied algorithm are unable to understand or explain what is happening inside it and how it arrives at a specific output. This has a negative impact on the transparency of the functioning of the AI model and on the explainability of its outputs. The black box phenomenon is the most typical in case of—but not limited to—generative AI models.

Example for the notariat: The notary uses an AI solution that provides recommendations for a complex legal issue. The notary himself/herself would like to understand why the system provided the given output, but can understand neither the reasons behind the AI's decision-making, nor the process itself. When contacting the AI developer for explanations, the latter has the same issues of understanding and is unable to provide valuable assistance to the notary. Due to their lack of explainability, the notary decides to discard the AI recommendations.

c) AI bias:

AI bias means the occurrence of biased outputs by AI systems due to the characteristics of the human brain (humans are by nature biased and AI systems are developed by humans) appearing in the AI mostly through the biased AI training data and the biases embedded into the algorithm—often unconsciously—by its programmers. The AI system is likely to replicate biases in the outputs, leading to inaccurate functioning. Early and continuous bias monitoring, detection and mitigation is crucial for the reliability of the AI systems.

Example for the notariat: The AI system used by the notary was mainly trained on transactions with high-risk of money laundering of clients from a certain country. The AI system may on the basis of this develop bias for other individuals from that same country even if their intended transactions do not carry any risk of money laundering, resulting in that their transactions are flagged by the system as suspicious.

d) Overfitting and underfitting:

Overfitting happens when the AI model learns the training data 'too well' resulting in struggles to generalise to new data. Underfitting occurs when the AI model fails to identify the underlying patterns in the data which results in weak performance on the testing datasets. Both have the risk of unreliable and inaccurate output data, therefore, they need to be mitigated when evaluating the performance of the AI model.

Example for the notariat: If the notary's AI system is trained too much on specific contracts (e.g. sale and purchase), it might learn to detect patterns that only apply to those contracts and may be unable to proceed correctly on different ones (e.g. donations), resulting in incorrect outputs (overfitting). On the other hand, if the AI system is not sufficiently trained for one type of contracts, it may fail to identify patterns which should be used in contracts of that type (underfitting).

e) AI feedback loop:

An AI feedback loop is a process by which an AI system receives feedback from various sources (humans, other systems, etc.) on its functioning and uses that feedback to improve its algorithm and performance. This process is repeated later on in several stages, allowing the AI system to continuously learn. The feedback loop can be an issue when the input data is not of appropriate quantity or quantity, the feedback is biased or the applied technology is not sufficient.

Incorporating human feedback into the feedback loop can optimise an AI system's performance by identifying areas where improvement is needed. For example, if a chatbot is not responding appropriately to certain types of queries, human feedback can help identify these issues.

Example for the notariat: The notary uses an AI system the outputs of which in certain respect (e.g. recommendation of unfitting clauses in the given contract) are constantly overridden by him/her. Based on these human expert feedbacks, the system might adjust its functioning by reducing the number of the same or similar outputs.

f) Human-in-the-loop (HITL):

Human-in-the-loop is a collaborative approach integrating human input into machine learning and AI systems by humans actively participating in the training, evaluation, and operation of ML models. HITL aims to enhance the accuracy, reliability, and adaptability of ML models and helps mitigating biases.

Moreover, the insights provided by humans help explain model decisions. The human input ranges from labelling training data, through the evaluation of the performance of the AI model, to providing feedback on its actions. The human involvement enhances AI adaptability and allows AI models to evolve with user preferences and real-world scenarios.

Example for the notariat: The notary deploys an AI solution for automated document drafting. When checking the outputs of the system, he/she discovers several imprecisions and anomalies, therefore, discards (parts of) the output and inserts his/her self-written clauses. In order to raise the awareness of the developer to these deficiencies, the notary informs the developer about them and makes proposals to ameliorate the system.

g) Automation bias:

Automation bias is the inclination for humans to over-rely on suggestions from automated decision-making systems and to ignore contradictory information made without automation, even if it is correct.

Example for the notariat: An employee of the notary starts over-relying on the AI system's outputs for document review and accepts every modification suggested by the system without checking their accuracy. This carries the high risk that the unverified notarial acts include incorrect clauses and imprecisions, resulting in negative legal consequences.

h) Deepfake:

'Deepfake means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful'. [AI Act definition, Article 3 (60)]

Deepfakes are very often generated with malicious intent, and used to spread misinformation or to commit cybercrime.

Example for the notariat: In a remote notarial procedure, the notary suspects that the facial image of the client he/she sees on the screen is not a real one but a deepfake. With the help of facial recognition AI, the notary can make sure that this is the case and refuses to proceed further.

7. Main legal sources related to the AI

a) Artificial Intelligence Act (AI Act):

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised 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

The AI Act is the first comprehensive regulatory legal act worldwide on AI, applicable in the EU with an extraterritorial effect, and with a progressive entry into force. The AI Act follows a risk-based approach according to which AI can be divided into 4 risk categories (prohibited AI practices, high-risk AI systems, certain AI systems with transparency obligations and minimal-risk) which trigger various obligations for the participants of the AI ecosystem (mostly providers and deployers). When developing and/or using AI systems, notarial organisations (chambers) and notaries shall strictly observe the provisions of the AI Act. The present Handbook seeks to identify the potential cases in which the rules of the AI Act must or may be applied in the notarial context.

b) Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law:

This is the first international legally binding convention aimed at ensuring the respect of human rights, the rule of law and democracy during the use of AI systems. The Convention applies to the entire lifecycle of AI systems and addresses their main risks (adopts a risk-based approach). It covers the use of AI systems in the public and also in the private sector. The document establishes transparency and oversight requirements and requires the parties to adopt solutions to identify, prevent and/or mitigate possible risks. Moreover, the respect of equality, the prohibition of discrimination, and privacy rights are also in the focus of the Convention.

c) DSM Copyright Directive:

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

The DSM Copyright Directive introduced the so-called text and data mining exceptions and limitations which are crucial for the efficient training of the AI models. The relevant rules contribute to the legality of the training process by avoiding the copyright, related rights and database rights infringements when the AI model is trained with protected works.

d) General Data Protection Regulation (GDPR):

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

AI—especially generative AI models—may result in serious concerns in respect of the protection of privacy and personal data. Therefore, the GDPR and the relevant rules of the AI Act need to be seriously taken into consideration. In the present Handbook a separate chapter is given to efficiently prevent the potential breaches of personal data during the development and use of AI systems.

III. Potential ways of AI use by notaries

1. General insights

Despite the risks associated with the use of AI solutions—if used appropriately—this technology offers opportunities and benefits for the notarial profession. In the first place, it has to be emphasised, that technology in general—including AI—cannot be an aim itself, but a tool in the hands of the profession to provide higher quality services and to facilitate the work of notaries.

When determining the potential ways of use of AI by notaries, it is important to take into account the fact that, although all CNUE member notariats belong to the group of Latin-type notaries, there can be significant differences among the 22 CNUE members, mostly regarding their status (e.g. some notariats are more closely connected to the judicial system—i.e. the status of courts and judges—than others) and their competences. These features may result in the fact that some notariats could be able to make use of certain AI solutions differently than others. Within the present Handbook, we try to identify and present the most common potential ways of AI use across the 22 CNUE member notariats.

Below, the most plausible AI uses by notaries are—not exhaustively—presented, without dealing with their risks. The latter—including the prohibited AI practices and the high-risk AI systems—are discussed separately under the subsequent chapters. It is important to emphasize, that any notarial use of AI, can only be carried out in case of regulatory permission or in the absence of prohibition.

2. General benefits of AI use

As it is mentioned in numerous scientific sources dealing with the topic, AI solutions contribute to the automation of certain tasks also in the field of law. These concern mostly the routine tasks which can be related to the legal work (e.g. drawing up minutes with the use of the speech-to-text applications) or to the notarial office administration (e.g. handling the requests for appointment from clients, billing). These solutions contribute to the streamlining of professional workflows and to the increase of the work efficiency and productivity whose ultimate beneficiaries are the clients of the notaries.

The human resources (notaries and notarial employees) spared this way can be used for deeper and complex legal tasks requiring the level of creativity that AI systems are currently lacking. Besides, on the medium and long run, the applied AI solutions may result in significant cost savings for the notarial offices. Moreover, the use of AI systems might enhance the ability to research and process more data not only by notaries but also by notarial organisations.

As will be dealt with later on, the core notarial work which requires extensive legal knowledge and experience cannot and—because of the inherent deficiencies of the current AI systems—should not be replaced by the AI.

3. Specific ways of AI use by the notariat

a) Document automation

Document automation, i.e. the creation of notarial deeds with the use of AI, using technologies like NLP and LLMs, may have important benefits for the profession. It can be the case for the generation of simple routine documents (e.g. attestations, certificates) or the creation of deeds based on templates (e.g. the European certificates of successions). Besides, the automation of some 'post-contractual' formal tasks (e.g. for the execution of deeds) is also possible with the help of AI solutions. It must be emphasized that document automation shall not in any case mean the removal of notaries from the process of drawing up the relevant deeds. Even in case of an automatically generated deed, the notary has the obligation to accurately revise it and to correct the possible errors made by the system. Therefore, AI applications for document automation should only serve as assistance tools for notaries, mostly to save time from drawing up documents from scratch.

b) Review of documents

At the end of drawing up notarial deeds, document reviewer LLM solutions might be efficiently used for complementing (but not replacing) the human review for checking the completeness of the given act, to check missing clauses relevant for the context and to identify potentially conflicting clauses and terms. This can also include the check of the consistency of the given notarial act with previous ones related to the same/similar goods and/or persons. Moreover, AI could be used for checking the conformity of the act with the latest legislative changes. These enhance the precision of notarial services and assist in reducing human errors.

c) Speech-to-text transcriptions

In cases when notaries have to draw up minutes and similar documents, NLP tools can accelerate and streamline the procedure by applying the speech-to-text transcription technology, naturally with the subsequent correctness check of the text by the notary.

d) Document summarizing and assistance for analysis

Very often, notaries need to identify and analyse numerous documents with high number of pages which range from official legal acts to documents necessary for their notarial deeds and proceedings. NLP and LLM solutions might also provide assistance in finding and summarising such documents, extracting the relevant clauses, articles and paragraphs and highlighting the main changes compared to previous versions of such texts. This does not, however, relieve the notary from his / her duty to review the documents personally, as it cannot be assured that the AI will not leave out important information.

e) Facial recognition, emotion recognition and sentiment analysis

In the recent years, remote notarial acts became a reality and widespread in the practice of several notariats of the CNUE. This is especially the case with the notariats having extensive competences in the field of company establishment, where the relevant EU rules made it mandatory to introduce remote notarial services (i.e. the drawing up of the relevant notarial acts without the physical presence of the client in front of the notary, by using videoconferencing solutions).

In these processes, the secure and efficient verification of the client's identity is a crucial step, for which biometric facial recognition AI tools may provide assistance. These tools can potentially complement the human identification of the client by the notary, contribute to the legal security and to the spread of the remote notarial services. Besides, in order to enhance the security of such proceedings, emotion recognition and sentiment analysis AI solutions may also be deployed in order to detect if the given client is under pressure or force affecting the validity of the given act. These solutions are able to detect nuances in the movements, gestures and other physical, as well as psychological characteristics of natural persons, which cannot be detected or may be more difficult to be detected by the human eye. When applying such solutions, the notary must take into consideration that AI solely provides assistance and that he/she is obliged not to automatically accept the machine outputs (in order to avoid among others the automation bias).

Furthermore, it needs to be emphasised that emotion recognition systems—when they do not fall under the prohibited practices of the AI Act—are considered as 'high-risk systems' in accordance with point (1) c) of Annex III of the AI Act with special transparency obligations under the same Act [Article 50 (3)].

f) Document storage, classification and retrieval

Already simpler ML tools can provide assistance for the post-drawing up management of notarial deeds, assisting the notaries in the storage, classification and quick retrieval of documents. This can contribute to the effective management of the clients' files.

g) Automatic monitoring of legislative changes and new jurisprudence

In the day-to-day work, but also in the training of notaries, AI systems can be extremely useful by permanently monitoring the legislative changes and the new jurisprudence affecting the notarial activities, giving fast access to relevant judicial information. Moreover, in case of use of templates for certain notarial activities, the relevant changes can be automatically incorporated into such templates.

h) Machine translation

AI-based machine translation tools are widespread in the professional activities and the notaries are not an exception to this. Tools available also freely or for a low cost (e.g. DeepL translate) can be effectively used to accelerate the communication with foreign language clients and also—with strict restrictions—for the preparation of notarial acts. However, machine translation cannot replace the sufficient level of knowledge of the given language by the notary. Therefore, in case the notary (or one of his/her employees) does not possess sufficient knowledge of the language of communication/of the act, the use of machine translation must be avoided, as the human control of the translated output cannot be securely carried out.

i) Notarial chatbots

In respect of communication activities of the notarial profession, chatbots can be useful tools. These can range from simpler rule-based chatbots to more sophisticated AI chatbots. Since AI is not able to give personalised legal services to the clients, the role of these chatbots should be limited to the provision of very general information to the most frequently asked legal questions from the notarial field. This limitation should be in every case indicated to the clients. Personalised legal services should be only provided by notaries (possibly with AI assistance), as chatbots and AI systems are unable to recognise the circumstances and the context in which the legal solutions are required.

Moreover, in case of more complex AI chatbots, the data input by the users could be used by the profession to further develop the system, and also to get information on the most commonly asked questions, allowing the competent notarial organisations to get statistics on the mostly consulted fields and to streamline the notarial services in them.

j) AI for the security of data and notarial systems

AI solutions can be effectively used contribute to the security of notarial data and systems as well as to prevent the occurrence of cyberattacks ('cybersecurity with AI').

4. Implementation of AI solutions by the notariat

Depending on the decision of the competent notarial organisation (chamber) or notary, the above solutions could be introduced as modules or integral parts of multifunctional management software or used as standalone solutions for the different tasks. The former has the advantage of interlinking various solutions under one umbrella, and providing a more consistent and integrated system, the latter's advantage is the easier independent enhancement by focusing only on the purpose.

Key takeaways

- AI technology is a tool in the hands of the notarial profession to provide higher quality services and to facilitate the work of notaries.
- AI systems contribute mostly to the automation of notarial routine tasks.
- The core notarial work (requiring extensive legal knowledge and experience) cannot and should not be replaced by AI.
- Document automation (i.e. the creation of notarial deeds with the use of AI) is one of the fields of application of the technology in the notariat, especially for creating simple routine documents and deeds based on templates.
- Facial recognition, emotion recognition and sentiment analysis technologies may assist the notary proceeding remotely (i.e. by videoconferencing) in verifying the identity of the client and the free and voluntary expression of his/her will.
- Certain AI tools may be used for revising the completeness and correctness of notarial acts and to help in the storage, classification and easy retrieval of such acts.
- Machine translation tools are only recommended if the notary speaks at sufficient level the given languages.
- Before accepting the outputs provided by AI systems, the notary has to check their accuracy and carry out the necessary modifications, if necessary.
- The various AI solutions can be introduced as parts of the notarial management software or used as standalone applications for the different tasks.

IV. Applicability of the EU Artificial Intelligence Act

1. General insights and timeline

On 12 July, 2024, the Artificial Intelligence Act (AI Act) of the European Union was published in the Official Journal of the European Union and entered into force 20 days later, on 1 August. The AI Act is a directly applicable EU regulation and is the first comprehensive set of legal rules on AI worldwide, adopting a so-called risk-based approach. The obligations set out in the AI Act shall become applicable progressively. The AI Act aims to enhance AI innovation within the EU and to protect the fundamental rights of citizens and the rule of law.

For the sake of clarity, this chapter will cover and analyse only those rules of the AI Act which may be applicable to the notarial profession. However, one should be aware that the AI Act includes numerous provisions which regulate various AI systems, which provisions will not be analysed since they cannot be used for the scope of notarial activities.

The progressive applicability means that as a main rule, the AI Act will be fully applicable within 24 months after its entry into force, i.e. from 2 August 2026. However, its provisions on the ban of prohibited practices apply from 6 months after its entering into force, i.e. they are applicable since 2 February, 2025. Moreover, the legislator set a 12 month-long deadline for the application of governance rules and obligations for General Purpose AI (GPAI) models (2 August, 2025).

2. Personal and territorial scope

The AI Act has a broad personal scope which encompasses the following categories:

- Providers;
- Deployers;
- Importers; and
- Distributors of AI systems.

From the perspective of the notariat, only the categories of 'provider' and 'deployer' are relevant. According to the definition of the AI Act, the provider means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge [Article 3 (3)]. The AI Act does not include any limitation regarding the profession and status of the provider. Therefore, if any notarial organisation (chamber) develops an AI system, it is classified as a provider of the given system.

The role of the deployer is attributed by the AI Act to natural or legal persons, public authorities, agencies or other bodies using an AI system under their authority except where the AI system is used in the course of a personal non-professional activity [Article 3 (4)]. This means that when notaries use AI systems for notarial activities, they fall under the category of 'deployer'. However, this provision does not mean that notaries are always subject to the AI Act, because in case of using any kind of AI system outside their professional activities (e.g. ChatGPT for writing private e-mails), they are not under the scope of the EU Regulation.

It must be emphasised that the definitions of 'provider' and of 'deployer' expressly cover public authorities, and in respect of certain articles (e.g. on the obligation to make fundamental rights impact assessment), this status has special relevance. Hence, if in an EU Member State, an individual notary or a notarial organisation (chamber) representing the notariat of that Member State is considered by national law as being a public authority, the relevant specific rules may apply.

Difficulties to determine whether a natural or legal person qualifies as a provider or a deployer can occur in particular when he/she/it not only uses an existing AI system, but makes a substantial modification to a given system that has already been placed on the market or has already been put into service. In this case, the given natural or legal person will be considered provider of the system on the condition that the system was qualified as high-risk and remains in that category also after the modification. The same can occur if the deployer modifies the intended purpose of a non-high-risk AI system, in such a way that it becomes a high-risk AI system [Article 25 (1) b) and c)].

It is necessary to emphasize that the qualification of a notarial organisation and/or a notary as a 'provider' or 'deployer' does not automatically mean that further provisions of the AI Act also apply to them. At the same time—subject to the fulfilment of certain criteria—their classification into one of these categories determines the obligations they are required to comply with, and this is due to the fact that different obligations apply to 'providers' and 'deployers'.

Just like the General Data Protection Regulation (GDPR), the AI Act also has a wide extraterritorial scope (i.e. applies also to providers and deployers established outside the EU territory in certain predetermined cases). However, in the case of the notariat, both the notarial bodies (chambers) and individual notaries are always established within the EU territory, and therefore, the territorial scope of the AI Act always covers them (if qualified as 'providers' or 'deployers' and if further criteria are fulfilled for the application of the AI Act).

3. The risk categorisation system

Based on the rules of the AI Act, we can classify the AI systems into 4 risk categories. The first category covers AI systems whose use is prohibited by the AI Act due to the fact that they carry an unacceptable risk to the fundamental rights of citizens. Within EU territory, such AI systems cannot be provided (that is, placed on the market or put into service) and used. As previously mentioned, the prohibition of these systems is so crucial to the legislator, that such systems are the first to be prohibited under the AI Act. In fact, their prohibition applies 6 months after the entry into force of the AI Act (from 2 February 2025).

The second category, the high-risk AI systems, is the main focus of AI Act. The providers as well as the deployers of such systems must fulfil stringent and extensive obligations prescribed by the AI Act (see below).

The third category is defined by the AI Act as 'certain AI systems with transparency obligations', indicating that the providers and deployers of such systems are mostly (but not exclusively) subjected to transparency obligations.

Finally, even if such category is not expressly named in the AI Act, minimal-risk AI systems are recognised in practice as the fourth category. These systems do not fall under the material scope of the AI Act. Several authors and practitioners also acknowledge the existence of the category of 'no-risk' AI systems, however, in case of AI, there is always a kind of risk present, even if very minimal, independently from the rules of the AI Act.

4. Categorisation of (potential) notarial AI solutions under the AI Act

Under this point, it will be determined under which categories AI systems (potentially) developed/deployed by the notariat may fall. The identification of the categories reflects the current interpretation of the AI Act. It is based on the main notarial activities across Europe and is not exhaustive. This means that in different countries there can be notarial AI use cases which are not presented in this Handbook, but which may fall under one of the categories established in the AI Act. Therefore, analysis on the AI uses for the individual notarial activities must be always thoroughly carried out. Finally, subject to further interpretation and clarification—including by the Court of Justice of the European Union—the categorization might change.

a) Prohibited practices

The prohibited AI practices are exhaustively listed in the AI Act. The inherent characteristics of the notarial activities is the respect and protection of the fundamental rights of citizens. As the prohibited practices cover, among others, systems that manipulate individuals, exploit their vulnerabilities, collect their sensitive personal data without consent or make social scoring by assigning scores based on human behaviour, affecting access to services or other opportunities, and so on, it is clear that no notarial activity requires the use of any AI system which may fall under this category.

However, for their security, when developing or using any AI system, notaries and notarial organisations always need to verify whether the given AI system falls under this category. For instance, the AI Act [Article 5 (1) f)] prohibits the placing on the market, the putting into service or the use of AI systems to infer emotions of a natural person in the areas of workplace, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons. This provision prohibits the emotion recognition systems which identify or infer emotions of natural persons on the basis of biometric data.

For this prohibition to apply, the place of application has to be the area of 'workplace', which—based on the Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (*'Guidelines on prohibited AI practices'*)—should be interpreted broadly, including also virtual spaces (e.g. in case of home office work). The text of the AI Act does not expressly mention 'employees' as the targets of such AI systems. However, the related Recital 44 of the AI Act explains that the limitation to 'workplace' is meant to address the imbalance of power in the context of work which may suggest that the prohibition applies to the deployment of such AI solutions on 'employees'.

Furthermore, the Guidelines on prohibited AI practices clarify that the status as an employee, contractor, trainee, volunteer, etc. is irrelevant in respect of this prohibition and that the notion of 'workplace' should also be understood to apply to candidates during the selection and hiring process. This clearly indicates that the use of emotion recognition systems is strictly prohibited already in the recruitment process, also in case of online recruitment of new 'employees', and the list of examples suggests that the use of such systems is only prohibited on 'employees' (interpreted broadly). Besides, the Guidelines on prohibited AI practices include some guiding examples about possible prohibited uses of emotion recognition systems. For instance, the use of such systems to track the emotions of employees during phone calls with clients is prohibited.

The interpretation above is important, since the pure grammatical interpretation of this provision of the AI Act might lead to a broad applicability of the provision encompassing within it any person who happens to be present in the areas of workplace (for instance clients who enter into notarial offices). However, in accordance with a practical example of the Guidelines on prohibited AI practices, using cameras in a supermarket or bank to detect suspicious customers (for instance those who are about to commit a robbery) is not prohibited under the relevant article of the AI Act, when it is ensured that no employees are being tracked. By analogy, the prohibition can be interpreted as not applying to cases when emotion recognition technologies are applied to clients in notarial offices.

However, the non-prohibited use of emotion recognition systems falls under the high-risk category, with special transparency obligations. Besides, in order to prevent breaches of personal data protection, the relevant provisions of the GDPR have to be strictly observed.

This example shows in any case that the applicability of all the rules of the AI Act—even if the related situations are improbable to occur in practice—always have to be verified.

b) High-risk AI systems

According to the AI Act, systems which fall under this classification are those which could have an adverse impact on the health, safety and fundamental rights of persons.

The AI Act introduces two main categories based on which a certain AI system can be classified as high-risk. The first one—which does not concern the notarial profession—encompasses those AI systems which are intended to be used as safety components of a product or are themselves products, are covered by the EU harmonisation legislation in Annex I of the AI Act, and the product or the AI system must undergo a third-party conformity assessment. These are for instance autonomous robots, self-driving cars or medical diagnosis tools.

Annex III of the AI Act includes the other group of areas and criteria, according to which a given AI system may fall under the category of high-risk. The provision of legal services is not present in Annex III, however based on notarial competences and activities in the EU, two points of that Annex can be identified on the basis of which we must examine whether the AI systems (potentially) used by the notariat in those areas and under those circumstances fall under the high-risk category.

The first one is point 1. c): the biometric AI systems intended to be used for emotion recognition. According to Recital 44 of the AI Act, emotion recognition systems are AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. As previously mentioned under Chapter III about the possible use cases of AI systems by notaries, especially in remote notarial proceedings, the emotion recognition and sentiment analysis AI solutions might complement the relevant human (notarial) skills and might give assistance to the notaries in order to make a well-founded decision—for instance—on whether the client at the other end of the video call is under threat or pressure. Even if it is not recommended that the notary makes his/her decision based exclusively on the recommendations of such systems, their mere use can result in their classification under the high-risk category.

It is important to remark, that under the same point—in sub-point a)—only the remote biometric identification systems are classified as high-risk. AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he/she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, fall outside the high-risk category. Therefore, the biometric verification by the notary with the assistance of AI in case of remote proceedings is not considered as high-risk.

The second point which may concern the notarial profession is point 8 a) which classifies under the high-risk category *'AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution'*. This provision may concern only a part of the members of the CNUE which are considered 'judicial authorities' or entities proceeding on behalf of a judicial authority. For instance, this provision can affect the notaries of Hungary, who act as judicial authorities (as first instance courts) in succession proceedings, or the notaries of Austria, proceeding on behalf of courts as commissioners of justice (*'Gerichtskommissär'*). If notaries whose status falls under one of the previous two categories use any AI system for researching and interpreting facts and the law and in applying the law to a concrete set of facts, their uses may fall under the high-risk category. For instance, if such a notary uses AI solutions to find the bank accounts of the deceased (researching a fact), to discover the case law related to certain provisions of the law in order to correctly interpret them (research and interpretation of the law), or to draft a probate decision based on the facts of the case (applying the law to a concrete set of facts), his/her use of the AI may fall under the high-risk category. The same can apply if any notary having the status of judicial authority or acting on behalf of it acts as a mediator (a form of alternative dispute resolution), and uses certain AI systems for that purpose. However, the AI Act includes a wide range of situations in which the use is exempted from being high-risk, therefore, it is not certain whether the examples above will finally be considered as high-risk cases.

When interpreting these provisions, one has to take into account, that they are not applicable until 2 August 2026 and consequently, no jurisprudence will clearly highlight their content until then. Some relevant practical guidance is expected from the side of the European Commission, but at the time of writing this Handbook, it is not yet published. Therefore, the profession can only interpret the relevant provisions on their grammatical meaning and on the related recitals highlighting the intent of the legislator. For instance, Recital 61 mentions *'judges'* and *'judicial independence'* but the classification of notaries as judicial authorities or acting on their behalf in certain legal systems suggests that AI use by those notaries in the relevant cases can also fall under the high-risk category. Similarly, the expression *'intended to be used'* is subject to interpretation, since it is not clear as to what is the applicable classification if a given AI system is not intended to be used for the purposes listed under Annex III, but is in fact so used.

c) Exemption from the high-risk category

In accordance with the AI Act [Article 6 (3)], exceptions or derogations are in place, rendering what would otherwise be considered under the AI Act as a high-risk system not to be considered as such. These are as follows: *'an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. The first subparagraph shall apply where any of the following conditions is fulfilled:*

(a) the AI system is intended to perform a narrow procedural task;

(b) the AI system is intended to improve the result of a previously completed human activity;

(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or

(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.'

Therefore, in case an AI system developed or deployed by the notariat falls under the high-risk category, it has to be examined whether one of the above exceptions applies. In these cases, the legislator deemed the risk of harm to the fundamental rights of natural persons so low that it did not deem necessary the application of obligations prescribed for high-risk AI systems. Very importantly, it is the case when the AI system does not materially influence the decision of the deployer.

There are several cases from the notariat that would presumably fall under these exemptions. For instance, the extraction of the heirs' data from the electronic documents related to succession cases in order to transfer them directly into the draft of the notarial probate decision is a narrow procedural task. In the eventuality that it is automatised by AI, the first exception might apply and the system might be considered as non-high-risk. Furthermore, if the notary uses an AI tool which has the functionality to improve the quality of his/her decision by removing typos and grammatical errors when quoting the relevant legal provisions, the second exception can certainly apply. Moreover, under the third category can fall the use of an AI system which helps the notary to detect the deviations from his/her similar previous decisions and warns the notary about this deviation. Finally, when applying AI solutions to search the bank accounts of the deceased, the notary might be considered to be using an AI system to carry out a preparatory task to an assessment relevant for drawing up a probate decision, in which case the given system would seem to fall out of the high-risk category. However, if the notary makes an input of the facts in a generative AI solution in order to have an automated first draft of his/her decision, the above exception most probably does not apply and the given use of the system is considered high-risk.

In case of assessment of the exceptions, the notary has to proceed with utmost care and has to determine on a case-by-case basis whether one of the exceptions can apply.

It is important to mention already here that when a notarial organisation (chamber) is a provider of a high-risk AI system which it considers as not being high-risk, it shall document the relevant assessment before putting that system into service [Article 6 (4)]. Moreover, before putting such a system into service, the notarial provider must in any case register the given system in the EU database to be set up based on the AI Act [also Article 6 (4)]. The registration obligation also applies to deployers of high-risk systems when they are public authorities (e.g. notaries if they are considered as such under their respective legislation) or persons acting on their behalf. This registration (deployer, entity, use) should be carried out before using the given system [Article 71 (3)].

d) Certain AI systems with transparency obligations

The AI Act includes a list of AI systems which can fall under this category (Article 50). As it is wider than the possible use cases within the notarial profession, the present sub-point is only focused on two relevant provisions, which are the development and use of chatbots and the deployment of emotion recognition systems.

Chatbots can be provided by the notarial organisations (chambers) and individual notaries with (potential) clients for various purposes (e.g. to answer simple questions about the law, to find a notary, to make an appointment with a notary office). Based on the relevant provisions of the AI Act [Article 50 (1)], the providers of such systems which are intended to interact directly with natural persons must be designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system. Such information obligation does not apply if it is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect that such person is interacting with an AI system. However, for the security of the provider and the deployer, it is strongly recommended to always indicate the fact that the (potential) client is interacting with an AI system.

The AI Act deals with the emotion recognition systems under various articles. As mentioned above, the emotion recognition systems at workplace (e.g. in notarial offices) are in principle prohibited. Besides—when the prohibition does not apply—these systems also fall under the high-risk category. Finally, the relevant article [Article 50 (3)] about the specific transparency obligations of certain AI systems prescribes that deployers of an emotion recognition system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with the GDPR. In the notarial practice—as previously mentioned—the potential use of emotion recognition systems within the procedure of drawing up remote notarial acts (through videoconferencing) may trigger this transparency and personal data protection obligation.

The AI Act determines the way this information shall be provided to the affected natural persons: this must be in a clear and distinguishable manner and should be carried out at the time of the first interaction and exposure with the given natural person.

e) Minimal-risk AI systems

Even if this category is neither defined nor mentioned in the AI Act, in theory and in practice, the *'minimal-risk AI'* arguably exists. The AI Act itself does not prescribe any obligations applicable to systems which do not fall under the category of high-risk or under the category for which transparency obligations have to be fulfilled. Therefore, AI solutions—even when used in the field of administration of justice—if they do not fall under one of the two previous categories, are not under the material scope of the AI Act. This however, does not mean that they are completely free of any risk. As mentioned in the different chapters of this Handbook, several risks can occur in relation to the use of such systems. For instance, when not used appropriately, such solutions can cause infringement of privacy and personal data, of professional secrecy, etc.

In the notarial practice, one may classify a wide range of AI solutions under the minimal-risk category, for which the AI Act is not applicable. For instance, the AI solutions for the anonymisation of notarial acts and decisions, the appointment reservation AI systems, the speech-to-text tools, the document summarising tools, etc. might fall under this category. In principle, when a high-risk AI system falls under the exception, unless specific transparency provisions under the AI Act apply to it, it has to be observed what kind of risks out of the AI Act have to be addressed.

5. What to do if a notarial AI system is in the high-risk category?

The AI Act prescribes extensive compliance obligations both for the providers and the deployers of high-risk AI systems. These obligations often require additional workforce and significant financial resources. Therefore, when the possibility of introducing AI solutions which can fall under the high-risk category occurs, the notarial organisation (chamber) and the notaries need to assess whether the fulfilment of the obligations in the AI Act results in a higher overall burden and whether it would be better and less burdensome if they were to solve the given issue by other means which do not fall under the category of AI or do not fall under the high-risk category. This decision is particularly important because the AI Act prescribes monetary sanctions with high maximal amounts in case of non-compliance with the respective obligations (e.g. EUR 15 million in case of non-compliance with the obligations of providers and deployers).

As the aim of this Handbook is not to analyse the AI Act in depth, only the main obligations with the identification of the relevant articles which a (notarial) provider and deployer must fulfil when putting into service/using a high-risk AI system are listed under this point.

i) The obligations of the providers of AI systems are as follows:

- Establishment, implementation, documentation and maintenance of a risk management system for the continuous monitoring and mitigation of potential risks (Article 9);
- Ensuring the data quality and relevance in respect of training, validation and testing data (Article 10);
- Drawing up and regular updating of technical documentation (with the elements under Annex IV) for compliance check (Article 11);
- Establishment of an automatic record-keeping function, registering the events (logs) over the lifetime of the system, keeping the automatically generated logs at least for six months (Articles 12 and 19);
- Ensuring the transparency of the AI operation to enable deployers to interpret a system's outputs and provision of instructions for use to deploy the AI system appropriately (Article 13);
- Efficiently allowing human oversight to ensure the monitoring of the AI system and to intervene into its operation (Article 14);
- Ensuring the accuracy, robustness and cybersecurity of the system in order to be secure, precise and resilient to attacks (Article 15);
- Establishment of a quality management system (written policies, procedures, instructions) to ensure compliance with the AI Act (Article 17);
- Keeping the relevant documents (e.g. technical documentation, quality management documents) at the disposal of the national competent authorities for 10 years after the AI system is put into service (Article 18);
- Immediately taking the necessary corrective actions to bring the AI system into conformity, to withdraw it, to disable it, or to recall it in case of suspicion of its non-conformity with the AI Act; subsequent pro-

vision of information to the deployers (Article 20);
- The provision of information to the competent authority (including the automatically generated logs) and documentation demonstrating the conformity of the AI system with the AI Act, upon reasoned request (Article 21);
- Carrying out a conformity assessment procedure to demonstrate that the AI system complies with the mandatory requirements for trustworthy AI. The conformity assessment must be repeated if the system or its purpose are substantially modified (Article 43); drawing up an AI declaration of conformity with the content in Annex V of the AI Act (Article 47);
- Registration of the AI system in the EU Database (Article 49);
- Ensuring a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf (Article 4).

ii) The obligations of the deployers of high-risk AI systems are as follows:

- Taking appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems and they assign competent personnel with human oversight and support (Article 26, points 1 and 2);
- To the extent the deployer exercises control over the input data, implementing data control, to ensure that input data is relevant and sufficiently representative in view of the intended purpose of the AI system (Article 26, point 4);
- Monitoring the operation of the AI system on the basis of the instructions for use, providing feedback and information to the providers and the competent authorities in predetermined cases (e.g. serious incident) (Article 26, point 5);
- To the extent the deployer exercises control over them, keeping the automatically generated logs for least six months (Article 26, point 6);
- In case the deployer is an employer (e.g. a notary), he/she shall inform the affected employees (e.g. notary candidates, administrative staff) that they will be subject to the use of the high-risk AI system (Article 26, point 7);
- In case the deployer is a public authority (as the case may be for notaries under their respective national legislation), he/she/it must register him/her/itself in the EU Database mentioned above and verify if the system they intend to use has been registered (if not, they cannot use the system and shall inform the provider) (Article 26, point 8);
- In case the AI system makes decisions or assists in making decisions related to natural persons, the deployer shall inform the natural persons that they are subject to the use of a high-risk AI system (Article 26, point 11);
- Cooperation with the relevant competent authorities (Article 26, point 12);
- Ensuring a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf (Article 4).

Also, prior to deploying a high-risk AI system, deployers that are bodies governed by public law, or are private entities providing public services, shall perform an assessment of the impact on fundamental rights that the use of such system may produce (fundamental rights impact assessment – FRIA, Article 27). The FRIA should be updated when the deployer considers that any of the relevant factors have changed. The AI Office (established within the European Commission) will develop a template for a questionnaire to facilitate deployers in complying with their obligations related to the FRIA in a simplified manner. Once the FRIA has been performed, the deployer shall notify the competent market surveillance authority of its results.

Based on the wording of this article, it is uncertain whether notarial organisations (chambers) and notaries fall under this obligation when they deploy high-risk AI systems. There is a risk of falling under this clause for notarial organisations (chambers) because in numerous countries they are governed by public law. Furthermore, in certain Member States, notaries may be considered private entities that provide public services. According to Recital 96, '*private entities providing such public services are linked to tasks in the public interest such as in the areas of education, healthcare, social services, housing, administration of justice*', which may imply that notaries of such status providing public services related to the administration of justice are subject to FRIA obligations.

Key takeaways

- The AI Act is a directly applicable EU regulation, the first comprehensive set of legal rules on AI worldwide and the primary legal act to apply to AI within the EU.
- The AI Act will be in principle fully applicable 24 months after its entry into force, i.e. from 2 August 2026, but part of its provisions will be applicable at a prior date.
- The AI Act adopts a risk-based approach based on which the AI systems can be classified under 4 categories: prohibited AI practices, high-risk AI systems, certain AI systems with transparency obligations and minimal-risk AI systems.
- The personal scope of the AI Act covers the providers, the deployers, the importers and the distributors of AI systems.
- Notarial organisations (chambers) can be considered providers solely by developing an AI system and notaries can be considered deployers when using AI systems within their professional activities.
- The qualification of a notarial organisation (chamber) and/or a notary as 'provider' or 'deployer' does not automatically mean that further provisions of the AI Act also apply to them.
- Prohibited AI practices are unlikely to be present in the notariat, however, the rules applicable to these practices always have to observed (e.g. emotion recognition at workplace).
- Annex III of the AI Act includes areas and criteria also relevant for the notarial profession, according to which a given AI system may fall under the category of high-risk.
- The two cases in which a notarial AI solution might fall under the high-risk category are the biometric emotion recognition AI systems (e.g. for remote notarial proceedings) and the AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution.
- Exceptions are in place in the AI Act which result in the fact that not all high-risk systems are finally considered as such. The exception applies in listed cases encompassing situations in which the given system does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including when the AI system does not materially influence the decision of the deployer (notary).
- In case of assessment of the exceptions, the notary has to proceed with utmost caution and has to determine on a case-by-case basis whether one of the exceptions may apply, taking into consideration that other obligations in the AI Act may still apply.
- The two AI systems which may fall under specific transparency obligations from the notarial field are the chatbots and the emotion recognition systems. In these two cases, the notary shall inform the affected person (client) that he/she interacts with/is exposed to an AI system.
- In the notarial practice, we can classify a wide range of AI solutions under the minimal-risk category, for which the AI Act is not applicable (e.g. appointment reservation AI systems, speech-to-text tools).
- The AI Act prescribes extensive compliance obligations both for the providers and the deployers of high-risk AI systems and high-amount monetary sanctions in case of lack of fulfilment of those.

V. Data and artificial intelligence

1. The importance of data for AI

Data science is a discipline separate but, at the same time, closely linked to the science of artificial intelligence and absolutely essential for it.

Data can be simply compared to the fuel of motor vehicles, meaning that in the same manner as the fact that not even the highest quality vehicles are able to operate without fuel, likewise AI is unable to function without data. In addition to this—still taking the example of motor vehicles—the type of the fuel (diesel or petrol) plays a fundamental role to the functioning of the vehicle. Based on this analogy, AI systems for use by legal professionals can only work with appropriate legal and auxiliary data. Finally, as low-quality fuel results in broken engines, the low quality of data (*'impaired data'*)—due to various factors presented below—causes wrongful functioning and outputs of the given AI system. Just like the effects of the low-quality fuel, the effects of impaired data are likely to get visible only after a certain period, during which the damage is already present.

2. Data governance frameworks

Before being ready for use, the fuel is subject to processing in order to fine-tune it for the modern vehicles, and this process is carried out in accordance with serious protocols. Data used for AI systems is also processed based on established data governance frameworks, according to which it is cleaned to be good enough for use in AI systems. The cleansing of data based on these frameworks enables us to get a data corpus which is freed from duplicated (*'de-duplication'*) or irrelevant data, structural errors (e.g. typos), and where the issues of missing data are tackled.

More precisely, the data governance frameworks should include policies on data management from the data collection phase through the processing until the storage of data. They should contain among others data validation rules and measures for the protection of privacy and personal data (due to its specific characteristics and importance, this topic is presented in a separate chapter of the Handbook). In addition, the matter of bias of AI systems is an issue which has one of its sources in the training data, mostly because of the imbalance of data used (the question of bias is also presented in a separate chapter), and which should also be part of the data governance frameworks.

The frameworks should deal with data security by introducing measures to protect data from unauthorized access, alteration or destruction. Besides, processes should be established for continuously and proactively improve and fine-tune the data quality. However, it should be emphasised that the extensive legal knowledge and professional experience cannot be incorporated into AI systems.

Even if the data processing is more and more automatised, the human role still remains crucial, therefore the *'data literacy'* of the competent staff of notarial organisations (chambers) and notaries must be developed on an ongoing basis.

3. AI training process with various data

The training process of the given AI model is not only based on the training data but also on the so-called validation data and testing data. The training phase can be compared from the physical world with students of a class (here: the AI model) receiving the same material, instructions and method of learning. The training material can be learnt by all the students but it is not sure that all of them understand the material at the same level and are able to apply the learnt information in the same manner. There comes the role of the validation data which is used to choose the best AI model (*'the best student'*) for a given task. Finally, the testing data gives the opportunity for the developers to check how accurate the given AI model really is, which can be compared to the performance of the students at the final exam. For the sake of the objective evaluation of the model, the validation and testing data cannot be merged.

During the training process, the issues of overfitting and underfitting should be efficiently handled, both partially caused by issues with data. In the former case, it must be avoided that the AI model becomes 'too well' trained for a specific output and missing other outputs within its purpose due to the too homogenous nature of the training data. In the latter case, the model delivers accurate outputs only in limited circumstances, for instance in case of using real-world data.

4. The risks of impaired data and characteristics of appropriate data

For guaranteeing the legal security and the reliability of the data and—through this—the AI system, the following characteristics of the training data must be observed and the following data processing activities must be carried out. The risks related to impaired data are serious as the slightest error can have significant impact on the output data of the AI system and on the activity of the deployer.

The impaired dataset can have multiple grounds and forms. The most obvious is the outdated data which reflects data which was correct earlier but is no longer valid for its set purpose (e.g. revoked legal acts, jurisprudence based on them). An incomplete dataset is characterised by missing elements which influences the ability of the AI system to give accurate and trustworthy output. In the case of misleading data, the data is correct in isolation but because of the context, it results in incorrect conclusions. The use of different data formats can lead to inconsistent data which confuse the AI algorithm. The training dataset including contradictory data can also cause negative outcomes. These impairments are generally caused by human errors, contrary to data poisoning which is in principle made maliciously with the intention of compromising the training process to make the system provide an unreliable output.

For the efficient training and reliable functioning of AI systems, the training data has to be accurate, complete (of sufficient quantity), relevant and consistent. Early detection and correction of data impairments is crucial for the reliable functioning of the AI system. Therefore, the regular audit, monitoring and update of the training data is necessary. In case of need, data professionals (e.g. data scientists) and other professionals (e.g. linguists) shall be deployed to make the training data as fit as possible for the purpose of the given AI system.

5. Notarial internal data and external data sources

Within the framework of their activities, notaries and notarial organisations (chambers) produce and process significant amounts of data on a daily basis. This *'notarial data corpus'* can be a perfect but raw basis for the training of AI systems developed and/or used by the profession. In addition to this internal data, it is unavoidable to have recourse to external data which should be collected from reliable data sources and with the strict observation of the relevant legal restrictions.

Especially in the field of law, the recourse to external databases containing the latest versions of EU, national, regional and local legal acts, as well as the jurisprudence is a necessity to get the reliable output. The management of external datasets is crucial as in this case we are often faced with already processed, cleaned and categorised data reflecting the needs of the persons and entities having rights on that data, with limited control or lack of control over them by external users. However, the same quality standards have to be maintained as in the case of internally collected data, independently from the rules and standards the persons and entities having rights on that data are subject to. In case these quality standards are not fulfilled, steps should be taken to make the data comply with the requirements above or to simply ignore the use of such external datasets when this is not possible.

Besides, the different intellectual property—especially copyright—rules (presented in detail under a separate chapter) and conditions determining the use of data on which others have rights, have to be thoroughly observed in order to avoid legal disputes for unauthorised use of data and copyright-protected works.

When collecting the various training data from external sources, in order to guarantee the relevance of the data, the issue of the language should be seriously taken into consideration. Even if in bigger languages (like French, German or Spanish), the size of the available dataset is naturally larger than in smaller ones (like Hungarian), building up notarial training datasets of sufficient size in those languages is also possible. At the same time, when building datasets in bigger languages, from the point of view of the language, one must be extremely careful to use appropriate sources for different training purposes, as the same language can be the official one in two or more countries with different legal systems. Mixing the datasets relevant to different countries, legal systems and concepts can easily result in false outputs (e.g. Austrian AI tools trained on German language data coming from Germany or Switzerland).

The internal and external data fulfilling the requirements above need to be efficiently integrated and interlinked in order to guarantee their consistency and interoperability. This process helps the developers of the AI systems to eliminate gaps in the data, to find possible errors and contradictions and eliminate them before the system uses them for giving false or erroneous outputs.

6. Data in prompts and feedback loops – the human role in the enhancement of data

It must be also emphasized that besides the quality of the initial training data—and the algorithm applied—the quality of the prompts (formulation of questions and instructions) that deployers enter into the system have an impact on the quality and accuracy of the output produced. Therefore, it is important to make the deployers of the AI systems aware of the appropriate formulation of their prompts. In case specific steps are required by a given system in respect of prompts, the deployers of such systems have to be informed about them before they start using such systems.

Moreover, certain AI systems using ML algorithm constantly learn by using also the input data from their deployers. That is why the correct data in prompts has an impact on not just the quality of the specific output but the reliability and efficacy of the whole system.

The role of humans is therefore without doubt necessary for the improvement of various AI systems also during their use. The phaenomenon of feedback loop results in the refinement of the AI learning through feedback. For instance, if the output of an AI system is marked as incorrect by its deployer—through prompts or separate notification—the system can use this feedback and adjust its dataset. At the same time, the errors in the feedback loop are able to cause negative consequences when the input data has deficiencies in quantity or quantity.

Key takeaways

- AI is unable to correctly function without appropriate data.
- The low quality of data (*'impaired data'*) causes wrongful functioning and outputs of the given AI system.
- In case of impaired data used, the slightest error can have significant impact on the activity of the deployer. Therefore, early detection and correction of data impairments is crucial.
- Data used for AI systems should be processed based on data governance frameworks which include policies on data management.
- The training process of the AI model is based on the training data, validation data and testing data, all of them having different roles.
- Training data has to be accurate, complete (of sufficient quantity), relevant and consistent.
- Internal (e.g. notarial documents) and external (e.g. legal databases) data sources have to be applied for the efficient functioning of notarial AI systems. In both cases, the data quality requirements have to be strictly observed.
- The quality of prompts (the formulation of questions and instructions) by deployers has an impact on the quality and accuracy of the output.
- Certain AI systems learn by also using the input data from their deployers which also stresses the importance of the quality of the data present in prompts of deployers.
- In case the output of an AI system is marked as incorrect by its deployer, the system can use this feedback and adjust its dataset (*'feedback loop'*).

VI. Personal data protection and artificial intelligence

1. General insights

Notaries produce and process huge amounts of data every day while carrying out their professional activity. A huge part of these are personal data, mostly of their clients, but also of third natural persons (e.g. individuals having rights on the real estate subject of notarial sale and purchase contract). Without any exception, all the notaries of the EU have to apply the rules of the General Data Protection Regulation (GDPR), in their quality of data controller or data processor. The same applies to the notarial organisations (chambers) processing personal data (e.g. when operating notarial registers including such data of notarial clients).

The aim of this Chapter is not to analyse in details the application of the GDPR by notaries, but to highlight the most important matters related to the personal data protection within the context of notarial AI use and development. Therefore, under the following points, only those provisions of the GDPR will be analysed which (may) have relevance to this specific topic.

2. GDPR and the AI Act

The AI Act aims at regulating various aspects of AI systems and general-purpose AI models in accordance with a risk-based approach. The purpose of the GDPR is different: the protection of the personal data of natural persons (and through this, the persons themselves) within (in certain cases also beyond) the territory of the EU. In other words, the AI Act regulates a specific technology, the GDPR regulates the processing of a data category. However, the issue of the protection of personal data is significantly present at the development stage and use of AI systems. Just to mention the most obvious examples: the training dataset of an AI system may include personal data, the input (prompts) as well as the output of the system might also contain such data.

On the one hand, the AI Act barely includes specific provisions related to the protection of personal data. Under Article 3 (50), the AI Act makes reference to the definition of personal data in the GDPR, which results in the fact that there is no difference regarding the concept of this term within the two regulations. Furthermore, Article 2(7) of the AI Act explicitly states that the AI Act is without prejudice to the application of the GDPR, hence it does not replace or restrict its provisions. Therefore, despite the fact that their aims and focuses are different, the two regulations apply simultaneously in a complementary way, and when the given AI system involves the processing of personal data, the providers and deployers shall comply with their obligations under the GDPR as well.

On the other hand, the GDPR does not include any explicit reference to AI technology. The reason for this is twofold: at the time of its adoption, the technological landscape was different, the extent of development and deployment of AI systems was less significant (e.g. ChatGPT was still an idea). Moreover, the GDPR is technology-neutral, meaning that it applies to the processing of personal data through the use of a simple typewriter up to the same activities carried out with the help of the most cutting-edge technologies, as AI. This means that the GDPR is fully applicable to the processing of personal data by using AI solutions as well as to the processing of such data during the development of such systems.

However, the relationship of the GDPR with the emerging technologies has never been devoid of tensions. One example of this is the exercise of the right to erasure ('right to be forgotten') within the context of the blockchain technology, which—in its purest form—has one of the main characteristics of being unalterable and indelible.

Issues do already come up and will continue to do so also in relation to AI technologies. For instance, personal data within the context of AI shall be processed in a way compatible with the principles of GDPR such as data minimisation and purpose limitation. This can be quite difficult in some cases, as the essence of several AI solutions (e.g. LLMs) is exactly the use of large datasets for various purposes (predictions, generation of content, etc.). Besides, the existence of the appropriate legal ground for processing is crucial in relation to the training of AI systems, which activity undoubtedly falls under the broad definition of 'processing' (*'any operation or set of operations which is* *performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'* – Article 4 (2) of the GDPR).

The matters in the relation between AI and data protection may require a change of approach, deep reflection as well as the exercise of a high level of caution from the notarial profession.

In 2024, an intensive period of legislation (including the AI Act) at EU level was closed and despite requests to amend the GDPR to make it more compatible with and streamlined to the age of AI, the EU institutions do not have such plans. They rather intend to focus on the implementation of the provisions currently in force within the context of AI. Explanatory documents and guidelines are expected to be issued, but they may provide only limited specific guidance to the notarial profession. Under the following points, one will find a summary of the main data protection matters to which notarial organisations (chambers) and notaries should pay attention when developing and/or deploying AI systems. When it comes to the relation between AI and data protection, there is no unanimous opinion between professionals (practitioners, scholars, etc.), and hence in case of doubt, consultation with the competent data protection authorities is recommended before the beginning of the given activity.

3. Different legislation – different roles

As mentioned under the previous point, the GDPR and the AI Act complement each other and have to be applied hand in hand. However, the two regulations operate with distinct categories of actors falling under their scope.

In respect of the notarial profession, the categories of 'provider' and 'deployer' established by the AI Act are relevant. Chapter IV of this Handbook includes an extensive analysis of these different roles, therefore, the relevant statements will not be repeated under this point.

In the GDPR, the categories of data controller and data processor have relevance for the notariat. In accordance with Article 4 (7) of this regulation *'controller'* means *'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'*. Point (8) of the same article provides the definition of the *'processor'*, which means *'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'*.

Just like the obligations of the providers and deployers under the AI Act are different, the duties of the controllers and processors also vary. Moreover, the respective roles always have to be determined on a case-by-case basis and in accordance with the applicable legislative text (AI Act and GDPR). In other words, the fact that a notary may fall under the category of *'deployer'* according to the AI Act, does not directly imply that he/she is a *'data processor'* under the GDPR. Similarly, if a notarial organisation (chamber) is the *'provider'* of the given AI system under the AI Act, it cannot be directly concluded that it is the *'data controller'* under the GDPR.

For instance, if a chamber processes personal data in order to train a specific AI system, it will be considered a 'provider' under the AI Act and a 'data controller' under the GDPR because the chamber develops the system ('provider') and—within the framework of this activity—takes decisions about how to process personal data for the purpose of training the system ('controller'). If subsequently, the chamber provides the specific system with notaries for their use, and notaries use it by including the personal data of their clients, the notaries would be acting as 'deployers' under the AI Act and as separate 'controllers' under the GDPR in respect of the processing their clients' personal data (i.e. personal data that is distinct from that which was used for the training of the system). However, as will be illustrated under the subsequent points, this example is mostly fictional and merely illustrates a possible separation of roles, since such activities (especially AI system training with personal data) involve additional activities that have to be carried out in order to avoid breach of personal data.

4. GDPR principles in case of AI use by notaries

a) Principles of GDPR

One of the main messages of this chapter is that the GDPR applies in its entirety also when AI systems are used in notarial proceedings. This has the direct consequence that the principles of the GDPR remain in application also when AI solutions are deployed. These principles are lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, as well as accountability (Article 5 of the GDPR). Under the following sub-points, only those principles which require special consideration are discussed.

b) Lawfulness and legal grounds of processing

The principle of lawfulness presupposes the existence of one of the exhaustively listed grounds for processing under Article 6 (1) of the GDPR. The applicable ground depends on numerous factors, for instance on the status and role of the notary in the given procedure and on the characteristics and the purpose of the specific proceedings. Since the GDPR cannot be considered as a new legislative act (it entered into force almost 10 years ago, in 2016), currently the legal grounds of the notarial processing of personal data are clear-cut and crystallised within all the Member States (e.g. consent of the data subject client, compliance with a legal obligation, exercise of official authority). In order to verify which legal ground applies, the respective national rules related to the given procedure need to be analysed.

The main question is therefore whether the use of AI systems within these proceedings changes anything in respect of these grounds (i.e. are new processing grounds needed when the notary uses AI systems?). As mentioned in various chapters of this Handbook, AI systems cannot replace but merely assist notaries in their professional activities. Therefore, the role of AI in these proceedings is a helping tool which does not change the essence and the aim of the proceedings. Therefore, the deployment of AI solutions in this context—in principle (see the next subpoint on sensitive data)—does not require any change in the legal ground for processing the personal data (e.g. if the consent of the client was the legal ground before the application of the AI, it remains so).

Moreover, the activities of notaries are based on their competences prescribed by the relevant national rules. This implies that the use of AI by notaries does not extend their proceedings by making predictions on or profiling of natural persons, i.e. to activities which often prove to be problematic in respect of the processing of personal data in other sectors.

c) Processing of special categories of personal data

The legal grounds for processing special categories of personal data (*'sensitive data'*) have to be analysed separately. The processing of such data may come up for instance in case of deployment of facial recognition or emotion recognition and sentiment analysis AI systems which might be helpful to complement the human assessment in case of remote notarial proceedings with the use of video-connection. These technologies use the biometric characteristics (data) of natural persons and in accordance with Article 9 (1) of the GDPR, *'the processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited'*.

Even if the AI Act makes a clear distinction between the identification and the verification of natural persons, this is not the case with the GDPR. Despite the lack of definition of the two terms in the latter regulation, according to (non-binding) guidelines of the European Data Protection Board from 2022, in respect of data protection, the same prohibition applies to the processing of biometric data for the verification of the identity of a natural person. The prohibition is not without exceptions, however, the grounds for processing are different than in the case of 'ordinary' personal data. In accordance with the currently applicable text of the GDPR, only the express consent of the data subject [Article 9 (2) b)] may give a clear way to the notary to be assisted by AI systems for the remote verification of the identity of his/her client.

However, the same is not necessarily true for the use of emotion recognition and sentiment analysis AI systems which may be helpful in assisting the notary in ascertaining that the will of the client at the other side of the screen is freely given and the client is not under threat or any other pressure. The prohibition of processing based on Article 9 only concerns biometric data for the identification (and verification) of natural persons and does not cover the recognition and analysis of emotions and sentiments. The determination of the free will of the client is an integral part of notarial procedures and in this case the AI system could only assist the notary in making a judgment about the client's will. Therefore, even if such AI systems use mostly biometric data, they may not be prohibited based on the rules of data protection. The grounds for processing regarding the procedure in which such systems are deployed may remain the same as without their deployment. However, it needs to be emphasised also under this Chapter, that such systems fall under the high-risk category and transparency obligations under the AI Act. Moreover, in order to have absolute clarity, before the deployment of such systems, consultation with the competent data protection authority is recommended.

d) Transparency, integrity and confidentiality

In respect of transparency, the notary may need to provide additional information to the data subject whose data are processed with the use of AI (transparency obligations can also be found in the AI Act). For this reason, the notary should be able to give information about data processing with the use of AI and at least basic and understandable (non-technical) information on how this processing of data takes place. Related to this principle, the data subjects have an extensive right to be informed (Article 12).

However, the provision of information and its depth should always depend on the circumstances of the case, as well as the significance of the role of the AI system in the procedure. For instance, it may not be necessary to inform the client about the use of machine translation assistance, in which situation the notary uses it just to accelerate the procedure and thoroughly checks and corrects the final version of the translated text him/herself. Conversely, it could be necessary to provide this information in case of use of speech-to-text solutions, where the client is directly connected to the given AI tool (the AI directly detects the speech of the client and transforms it into text).

Finally, the respect of the principle of transparency may be problematic in case of use of *'off-the-shelf' AI solutions* (e.g. ChatGPT). As described under Chapter IX—due to their complexity—these solutions do not always enable the deployers to understand and explain their functioning (*'black box issue'*).

Moreover, in case of deploying *'off-the-shelf'* solutions, the principles of integrity and confidentiality cannot be guaranteed either. These AI solutions often learn from the prompts of the deployers (who may be also notaries). This implies, that in case of giving client data as input (prompt) to such systems, there is a high risk that personal data will be further processed by the specific system in an unauthorised and unlawful manner (such AI systems generally constantly learn from the user prompts), even without the knowledge of the given data subject (and the deployer of the system).

Moreover, such personal data not only can enlarge the training dataset of such systems, but the output of them can be also the personal data of the client accessed by unauthorised persons which creates further issues of data protection. Therefore, based on the principles of integrity and confidentiality, it is suggested to discard the use of *'off-the-shelf'* solutions in notarial proceedings. In any case, if the notary needs to use such AI systems, it is strongly recommended to anonymise the personal data (see the details below) of data subjects in the prompt provided with the AI system so that the identification of the given data subject would be impossible later on.

5. Data subject rights in case of AI use by notaries

a) Rights of data subjects

Next to the principles under the previous point, the GDPR also includes specific rights of data subjects. These are as follows: the right to be informed, the right of access, the right to rectification, the right to erasure (*'right to be forgotten'*), the right to restrict processing, the right to data portability, the right to object and the rights (or rather prohibition) relating to automated decision-making and profiling.

In respect of AI use in notarial proceedings, the right to erasure and the rights related to automated decision-making (ADM) will be further analysed under this chapter.

b) Right to erasure

The issues of the right to erasure can mostly occur in case of the use of *'off-the-shelf'* AI solutions. In addition to what was presented under the previous point related to the matters of transparency, integrity and confidentiality, it has to be emphasised that once personal data get into the training dataset of such systems, the data subject can face extreme difficulties to exercise his/her right to erasure. These AI systems are very often LLMs, which operate with extensive datasets and complex algorithms. Based on the current technology, it is impossible to remove even one piece of personal data without re-training the given system. As the aim of the current AI regulatory environment is not only the safeguard of the rights of affected persons but also to create an innovation-friendly environment, it is unlikely that companies processing personal data this way would be obliged to re-train their systems, as this would create an excessive additional burden and unforeseeable consequences to such entities. Based on the above, it is once again strongly recommended to avoid the use of personal data when deploying *'off-the-shelf'* solutions in notarial proceedings.

c) Automated decision-making

In respect of ADM, the GDPR prescribes a default prohibition with various exceptions. In accordance with Article 22 (1), *'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'*.

Within the context of notarial proceedings, the application of this Article is very unlikely. First of all, it has to be checked, whether the outcome of the specific notarial proceedings is a *'decision'*. For instance, in the case of drawing up a deed on real estate transaction, the result of the proceedings is not a decision. However, in some non-litigious cases (e.g. in successions proceedings in certain countries), the notary makes a decision (often equivalent or similar to judicial decisions).

Furthermore, one of the main messages of this Handbook is that notaries must be the final decision makers even when using the most reliable and cutting-edge AI solutions. This implies that the condition of the *'decision based solely on automated processing'* is not fulfilled, as the decision is not solely based on the output of the AI. The human role in these proceedings is and must remain guaranteed and meaningful, the notaries should check all the details of the output of the AI system before making their decision in order to avoid the trap of automation bias (over-reliance on the outputs of AI systems).

6. GDPR and development of notarial AI systems

a) Same principles and data subject rights – different approach

Under Chapter XII of this Handbook, the prioritisation of internally developed AI systems or systems developed externally based on individually negotiated contractual terms is strongly recommended. Based on the statements above, the GDPR principles and data subject rights are fully applicable also in case of such solutions, but because of the difference of the purposes (creating such systems and not the use of AI for individual proceedings), the principles and data subject rights may apply differently.

b) Purpose limitation and legal ground for processing

First of all, the purpose limitation and the legal ground for processing of personal data need to be analysed. As mentioned earlier, in the case of use of AI solutions by notaries, the purpose of AI is to assist the completion of the specific notarial task (for instance the drawing up of a sale and purchase contract). For special notarial AI systems, one of the main sources of data are the data produced during notarial proceedings (e.g. data in notarial acts).

However—due to the principle of purpose limitation—the purpose of the data processing in individual cases does not extend to the subsequent training of special AI systems with the personal data of the notaries' clients and other affected data subjects. The purpose of the data processing will be different from the initial one, and the risk of further processing in a manner that may be incompatible with the initial purpose is present. Moreover, in respect of such processing, the roles of data controller and processor most probably change, depending on the specific circumstances (see above).

In case of the training of special notarial AI systems with the use of personal data, the determination of the applicable legal ground for processing can be also problematic. The client may provide his/her consent for further processing for the purpose of AI training, but the consent can be withdrawn at any time. Such withdrawal may cause technical issues in the functioning of the specific AI system, as the relevant personal data should be removed from the training dataset, which can lead to costly re-training of the system.

Since notaries are not obliged by law to set up AI systems, the ground under Article 6 (1) point c) (*'the processing is necessary for compliance with a legal obligation to which the controller is subject'*) cannot be evoked either.

Point e) of the same article 6 (1) also seems to be problematic as it requires the processing of data to be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In this case, it is highly questionable whether the training of the AI system (processing) is necessary for the task carried out in the public interest or in the exercise of official authority. Most probably, the answer is negative.

The application of point f) of Article 6 (1) (*'legitimate interest'*) can also be excluded because—depending on the national legislation—the notarial profession is generally considered as a public authority and the application of the legitimate interest ground is excluded for such data controllers.

Moreover, notaries have the duty of confidentiality which extends also to the personal data of their clients. Upon using such data for developing notarial AI systems, there is a risk of breaching the confidentiality obligations of individual notaries (e.g. by providing access for the notary to the personal data of the clients of another notary in the developed AI system).

At the same time, it has to be emphasised that the statements above only concern the development of notarial AI solutions by using personal data. Taking into account the specificities of the notarial proceedings and possible uses of AI solutions by notaries (see Chapter III), it can be observed that the use of personal data for training such systems is not always a crucial factor for the efficiency of the AI system. This means that AI systems for notarial use can be developed by using training data in which the personal data are not present at all or are anonymised, as well as where the personal data of existing data subjects are replaced by synthetic data.

7. Notarial AI use and development out of the scope of the GDPR

a) Use of anonymised data

Based on the above, the obligations of the GDPR burden the notaries using and the notarial organisations (chambers) developing AI solutions unless they use data which fall out of the scope of this regulation. The GDPR makes a difference between the pseudonymisation and the anonymisation of personal data. Pseudonymised personal data may provide a certain level of security but the rules of the GDPR remain fully applicable to such data. However, this is not the case with anonymised data which fall out of the scope of the GDPR (Recital 26).

As mentioned above, the use of anonymised data is especially—but not exclusively—important where the notary intends to use *'off-the-shelf'* AI solutions. For instance, in case of machine translation AI systems, the notary may prompt a text in which all the personal data are anonymised (e.g. replacing the names of the parties to a sale and purchase contract by *'seller'* and *'purchaser'* next to the anonymisation and deletion of other personal data). The output of the system may subsequently be complemented by the relevant personal data manually or by using secure internal software solutions. This way, the risk of further using the personal data by the provider of the given AI service can be efficiently avoided.

The same applies to the development of notarial AI systems, but for different reasons. By using anonymised personal data for the training of AI systems, the provider does not need to find the appropriate ground for the processing of data, as this data category fully falls out of the scope of the GDPR and there is no risk of unintended unauthorised use of the given personal data by other notaries deploying the specific system.

b) De-anonymisation (re-identification)

The risk of using anonymised data with AI solutions is the possibility of de-anonymisation (re-identification) of such data. The de-anonymisation can most often occur when anonymised data is matched with publicly available information or auxiliary data, which leads to the identification of the person the data belong to. De-anonymised data are again considered personal data which trigger the application of the GDPR. In case where *'off-the-shelf'* solutions are used, and where there is a risk that de-anonymisation can occur (e.g. when drawing up deeds with specific details for well-known persons whose data and information can be found at numerous places online), it is recommended to discard the use of the given AI system even with the exclusive use of anonymised data.

In case of internally developed solutions, appropriate technical and organisational measures shall be taken in order to prevent the de-anonymisation. The same applies to externally developed notarial AI solutions based on individually negotiated contracts: the relevant provisions have to include the obligation of the provider to prevent the de-anonymisation, as well as the appropriate legal consequences of the breach of this obligation.

c) Synthetic data

Another way of avoiding the risks and issues of personal data protection is the use of synthetic data for the training of AI systems. The GDPR does not include the definition and provisions of/on the synthetic data and as this category assures an even higher level of security than anonymised data, it can be stated that such data also fall out of the scope of the data protection regulation. Synthetic data mimic real-world training data but since there is no specifically identifiable natural person behind, the risk of re-identification is not present. Furthermore, the use of synthetic data is beneficial also when not enough real-world data is available for the given AI training.

d) Personal data of deceased persons

Finally, it has to be remarked that notaries—especially when carrying out succession proceedings—have to process a huge amount of personal data of deceased persons. In accordance with Recital 27 of the GDPR, the regulation does not apply to the personal data of deceased persons. Although the GDPR excludes personal data of deceased persons from its scope, it leaves the Member States free to introduce national rules in this respect or to leave the personal data of deceased persons fully unprotected. Therefore, the relevant national rules need to be consulted in order to determine to what extent these data can be processed.

8. Data protection impact assessment and fundamental rights impact assessment

As mentioned in Chapter IV, in case of deployers that are bodies governed by public law, or private entities providing public services, the AI Act introduced the obligation of carrying out fundamental rights impact assessment (FRIA – Article 27 of AI Act) prior to deploying a high-risk AI system. The FRIA has to be updated when any of the relevant factors change. Despite their similarities, the FRIA should not be confused with the data protection impact assessment (DPIA) mandated by the GDPR.

The aim of the FRIA is to identify the impact on fundamental rights of individuals or groups of individuals and the measures to be taken in case such rights are impacted through the use of high-risk AI systems. As mentioned under Chapter IV, it is uncertain whether notarial organisations (chambers) and notaries fall under the obligation of carrying out FRIA when they deploy high-risk AI systems.

Article 35 of the GDPR includes the provisions on the DPIA. This article states that the data controller evaluates in the DPIA the impact of processing operations on the protection of personal data. The DPIA shall be carried out when the processing operations make use of new technologies and is likely to result in a high risk to the rights and freedoms of natural persons. In case of AI use/development, the main question is whether AI can be considered as a *'new technology'*.

It has to be emphasized that the technological solutions applied in the current AI products are not inventions of the last decade, many of them have their roots in the second half of the 20th century. According to the Guidelines on Data Protection Impact Assessment by the European Data Protection Board, the use of artificial intelligence systems is not systematically a matter of application of new technological solutions. Therefore, not all processing using an AI system meets this criterion and it is necessary to make the distinction among the different systems. For instance, systems using deep learning fall under the category of *'new technology'*.

In this respect, it also has to be taken into consideration that according to Paragraph 4 of the same Article, *'the supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA'*. The consultation of such lists is strongly suggested.

In case a notarial organisation (chamber) develops a specific notarial AI system by discarding the use of personal data/by using anonymised or synthetic data, the DPIA shall not be carried out, as the GDPR is not applicable to these data. The same applies in case of AI use by notaries in such a manner.

In the event of processing personal data for AI development, the above-mentioned Guidelines on Data Protection Impact Assessment shall be consulted. In this document, 9 criteria are listed, and the fulfilment of 2 criteria (e.g.

large-scale collection of personal data and innovative use or application of new technological solutions which are the most probable in this context) leads to the presumption that the DPIA shall be carried out. In case of use of AI by notaries as data controllers, with the processing of personal data, the risk of carrying out DPIA assessment may be present in case the given system is considered a new technological solution (see above) and large scale of personal data is processed. In both cases (development and use), the characteristics of the specific processing shall be taken into consideration to make a decision on the necessity of DPIA.

Finally, if a notarial organisation (chamber) or a notary becomes obliged to carry out both the FRIA and the DPIA, the two documents may be merged in accordance with Article 27 (4) of the AI Act to create a comprehensive analysis.

Key takeaways

- The AI Act makes reference to the definition of personal data in the GDPR, which results in that there is no difference regarding the concept of this term within the two regulations.
- Furthermore, the AI Act explicitly states that the AI Act is without prejudice to the application of the GDPR.
- The technologically-neutral GDPR is fully (including its principles and the data subjects' rights) applicable to the processing of personal data through the use of AI solutions, as well as to the processing during the development of such systems. The AI Act and the GDPR complement each other.
- The AI Act and the GDPR operate with different categories under their personal scope (provider-deployer and controller-processor, separately defined in their texts). Determining the category under which the notarial organisation/notary developing/using an AI system falls, requires case-by-case analysis.
- The legal grounds for processing personal data in various notarial proceedings are already determined. AI solutions in these proceedings only serve as assistance to the notary. Therefore, the deployment of AI systems—in principle—does not require any change in the applied legal ground for processing the personal data.
- The processing of special categories of personal data (*'sensitive data'*) can be present in the case of using remote facial recognition or emotion recognition and sentiment analysis systems to assist the notary. The GDPR qualifies the processing of biometric data for the purpose of uniquely identifying a natural person under the special category which implies a prohibition by default of such processing. Unlike the AI Act, the GDPR does not make a distinction between the identification and verification of natural persons, and the prohibition to process biometric data for the verification also applies with the consequence that it can be only lifted by getting the express consent of the client.
- The use of emotion recognition and sentiment analysis AI systems may not be prohibited in accordance with the previous point and the grounds for processing regarding the procedure in which such systems are deployed may remain the same.
- Based on the principles of transparency, integrity and confidentiality, it is suggested to discard the use of *'off-the-shelf'* solutions in notarial proceedings. When the notary absolutely intends to use such AI systems, it is strongly recommended to anonymise the personal data of data subjects in the prompts provided with the AI system, making impossible the identification of the data subject later on.
- In case of *'off-the-shelf'* AI solutions, the data subjects' right to erasure (*'right to be forgotten'*) is extremely difficult or impossible to exercise, as this would require the re-training of the very often complex system.
- The GDPR prohibition on automated decision-making is unlikely to apply to the notarial profession. The notary should always remain the final decision maker, therefore the criterion of the prohibition of *'the decision based solely on automated processing'* is not fulfilled.
- In case of the development of notarial AI systems, the developer has to take into consideration that the purpose of the data processing in individual notarial cases does not extend to the subsequent training of special AI systems. There is a high risk of further processing in a manner that is incompatible with the initial purpose. Furthermore, finding the appropriate legal ground for such processing (training of the AI system) can be problematic.
- AI systems for notarial use can be developed by using training data in which the personal data are not present at all or are anonymised, as well as where the personal data of existing data subjects are replaced by synthetic data.
- The rules of the GDPR do not apply in case of processing anonymised data. In case of use of *'off-the-shelf'* AI solutions, the use of anonymised data is strongly recommended. For the notarial AI training, having recourse to synthetic data is a secure option.

- The processing of personal data of deceased persons does not fall under the scope of the GDPR, but national rules may apply to the protection of such data which must be taken into consideration in case of AI development.
- In certain cases, carrying out fundamental rights impact assessment and/or data protection impact assessment is necessary.
- In case of doubt regarding any of the questions in relation to AI and data protection, the consultation with the competent data protection authorities is recommended before the commencement of the given activity.

VII. Protection of confidential data

1. Confidential data in notarial activities

Notaries in Europe are trusted third parties, which in principle implies that they are under the duty (legal and/or deontological obligation) of professional secrecy. Professional secrecy refers to the obligation to keep secret the data and information communicated by the clients and other relevant data which the notary comes to know in the course of his/her professional activity. However, the obligation of professional secrecy of notaries is exclusively regulated by the applicable national law, which can result in big differences among the European notariats in different countries. Moreover, even if in a given country, the notarial professional secrecy is regulated, there can be situations in which this obligation is lifted (e.g. in case of criminal prosecution). The present chapter provides guidance by taking as a basis the principle that the obligation of professional secrecy applies.

Notaries process daily a huge amount of data which goes far beyond just personal data (the subject of the previous chapter). Among these data, there can be publicly available data, confidential data which may include trade secrets of clients and it cannot be either excluded that State or other qualified (e.g. military) secrets appear in notarial proceedings (e.g. succession procedures) and various acts. The analysis of the nature and the handling of such data in general is not the aim of this chapter. This chapter focuses on the avoidance of risks arising from the breach of professional secrecy while using AI solutions. Differently from other phaenomena which can only be mitigated (e.g. AI bias)—by proceeding appropriately—it is possible to avoid such risks.

2. Issues of data input in AI systems

As mentioned in different chapters of this Handbook, AI solutions can efficiently assist notaries in their activities. However, notaries must proceed with utmost caution when choosing which solutions they intend to use for various purposes. As is mentioned in the chapter comparing the internally developed AI systems and externally developed ones, if the notariat develops an AI system, it has sufficient control to build into it functionalities which guarantee the preservation of notarial secrecy and confidentiality. In case of externally developed systems, the notariat, as purchaser, shall insert in the individually negotiated contractual terms provisions that guarantee the technical preservation of professional secrecy.

However, this is very much different and challenging in case of the so-called *'off-the-shelf'* systems which are generally AI systems available for free or upon payment of fees based on the general terms and conditions dictated by various service providers. Two examples from everyday life are ChatGPT to generate text and the DeepL application for machine translation. The providers of such services often promise strict confidentiality of the data introduced into the system (many of them only in case of paying, upgraded versions). However, the verification of this remains an issue.

First of all, as a general rule, the general terms and conditions of *'off-the-shelf'* AI systems remain fully unread, and the majority of the users only click on the given button to accept them. This is an entirely reasonable behaviour, because in case of some activities (e.g. generation of e-mails, simple translations), the thorough reading and interpretation of such terms would constitute an excessive burden and is time consuming.

Secondly, especially in the case of large language models and generative AI systems, the model generally 'learns' from the input data (prompts) of the users. Once the data gets into the system, it remains in because based on the current technology, removing a piece of the dataset from the system is only possible by fully re-training the AI model. Needless to say, in case of models like the GPT-4, this is an unrealistic expectation. Therefore, if confidential data is prompted into the given AI system, most probably it remains there and the AI algorithm uses it for generating outputs. In worst case scenario, the system's output includes the confidential data learnt from the prompt of the user and there is the possibility of getting in the hands of unauthorised persons.

3. Solutions for the avoidance of the breach of professional secrecy

In case of internally developed AI solutions, and systems ordered from external providers, already at the design and development phase of the given solution, the relevant issues have to be identified and tackled. This requires the cooperation of notaries and developers to identify and incorporate the needs and solutions which guarantee the protection of professional secrecy.

In case *'off-the-shelf'* solutions are used, notaries should proceed with utmost caution and simply avoid any input which may include confidential data (some providers offer options which—based on their advertisements—do not use further the input data, however, this cannot be verified/is extremely difficult to verify). For instance, it can be a safe option to manually mask or remove data from the prompts and to re-incorporate the original data when controlling the given output (which is always necessary in order to guarantee the correctness of the document – see the Chapter on 'Human-in-the-loop').

In case this cannot be carried out, it is strongly recommended that notaries do not use the given system, and if any other convenient solution is not available, perform the given task without the use of AI.

Key takeaways

- Notaries in Europe are trusted third parties, and are bound by the duty of professional secrecy whose precise rules are determined by national laws.
- Notaries process a huge amount of data, including among others, personal data, publicly available data and confidential data.
- By proceeding appropriately, it is perfectly possible to avoid the breach of the duty of professional secrecy.
- In case the notariat develops an AI system, it has the sufficient control to build into it functionalities which guarantee the preservation of notarial secrecy.
- In case of externally developed systems, the notariat, as purchaser, shall insert in the individually negotiated contractual terms provisions that guarantee the technical preservation of professional secrecy.
- In case of using *'off-the-shelf'* systems, despite the promises of their providers, the protection of professional secrecy can arguably not be guaranteed.
- *'Off-the-shelf'* large language models and generative AI systems 'learn' from the user prompts, including from the data which should be guarded by professional secrecy.
- If *'off-the-shelf'* solutions are used, the relevant data shall be masked or left out of the prompts. If this is not possible, the notary should not use the given system.

VIII. Artificial intelligence bias and hallucination

1. Causes and effects of the AI bias

Across the European Union (and also outside it), the principles and obligations of impartiality and neutrality commonly characterise the notarial profession. If not handled efficiently, these can be compromised by the use of AI solutions, which can have a negative impact on the trustworthiness of the entire profession.

Strictly speaking, AI bias is an anomaly in the output by the AI system which has two main sources:

- prejudices in the training data and/or
- prejudiced assumptions made during the development of the AI algorithm.

However, both sources can be traced back to the inherent characteristics of the human mind which is by nature characterised by bias. AI systems are created by humans which obviously reflect their—individual or group—biases (e.g. the bias of the AI programmers). Most biases are not intentional and cannot be detected until the use of the AI system begins.

Bias in the AI system possibly results in discrimination and leads to the violation of the principle of fairness by giving incorrect recommendations and suggesting unfair decisions.

Historical imbalances and societal prejudices are very likely to be reflected in the training data. Bias can originate from various stages of data collection and processing and may be of different types.

Sampling bias occurs when the data collected is not representative of the target to be analysed. This imbalanced data results in AI bias towards the category that contains the higher number of data records. Measurement bias arises from errors in data acquisition, when the data collected is not measured accurately. Exclusion bias occurs when data is improperly omitted from the training dataset and confirmation bias happens when the data cleaner's expectations influence the cleansing process.

A special type of bias is a selection bias known as *'survivorship bias'*, which might have serious implications on the development and also on the deployment of AI systems. Survivorship bias ignores the unsuccessful outcomes in a selection process. This means that when making the selection of a specific group or dataset, the focus falls only on examples of successful elements (*'survivors'*, e.g. profitable transactions, companies with high profits) and not the group or dataset as a whole (including the failed transactions and less well functioning companies). This leads to the incompleteness of data and very often to incorrect outputs.

Similarly, in the AI data collection process, survivorship bias leads to the selection of training data that mostly represent successful examples (e.g. transactions in which the debtor fulfilled his/her duties) and to the exclusion of failed or unsuccessful ones (e.g. transactions where judicial enforcement because of non-performance took place). This might lead to the limitation of the variety of outputs generated by the AI system and to missing out insights and opportunities for improvement.

Survivorship bias can significantly impact the development and evaluation of AI models as well. When selecting the AI model, the presence of survivorship bias might result in favouring well-known AI algorithms from big multinational companies, overlooking alternative solutions which may be more accurate and suitable for the given tasks. Besides, survivorship bias can influence the evaluation of AI algorithms and can lead to the overestimation of the performance of some solutions because of focusing exclusively on the successful outcomes, overlooking the negative ones.

2. Bias identification and mitigation (de-biasing)

As AI systems become more complex and are trained on more and more data, bias identification and mitigation get more difficult.

Based on the statements above, fully removing biases from the AI systems is not possible, but mitigating and reducing the biased outputs to the greatest extent can be a realistic aim. Despite this, it must be admitted and accepted that even a trustworthy AI model will still contain biases because bias is inherent of ML. It is also precisely for this reason that the intervention of the notary is required also when the notary uses AI systems.

In the first place, one should begin with clearly defining the purpose of the AI model which involves determining the objective rules for data inclusion and exclusion in order to have a balanced dataset already in the data cleansing stage. In the development phase, the documentation of the data collection and processing activities is extremely helpful to provide transparency for identifying the parts or items of the dataset which causes the bias of the AI system. This is useful to perform also in the case of changing the relevant dataset. This can also be effectively applied to the AI algorithm to spot potential bias issues and take corrective measures.

In order to tackle the issue of bias as efficiently as possible, the training data and the applied algorithm should be regularly and accurately monitored and comprehensively audited. Upon detection of biases, the training dataset must be augmented and/or modified and/or the algorithm must be adjusted.

Just as other biases, survivorship bias can also only be mitigated, and cannot be totally avoided. Most importantly, the incorporation of data in the training dataset which represents also negative outcomes is crucial. Moreover, the more objective and comprehensive evaluation of the AI algorithm to be deployed, and—in case use of externally provided algorithms—considering the adoption of the ones provided not only by well-known companies, can help mitigate survivorship bias. Through this feedback, the dataset and also the algorithm can be effectively fine-tuned.

In simple cases, de-biasing the system can be carried out internally, but already various academic and market-based solutions—several of them open-source—are available for this process. Such solution is for instance the AI Fairness 360 which helps to identify and mitigate biases.

The human role in de-biasing the notarial AI solutions is crucial, and this task should be carried out by not by IT experts on their own, but in cooperation with notaries who are the best placed—based on their knowledge and experience—to spot the most frequent situations in which bias may occur.

Upon receiving the outputs of the AI system, notaries should carefully check them also in respect of finding biases. Biased outputs should be disregarded for the notarial activity in the specific cases and the competent developer should be notified of the issue in order to mitigate it.

3. Causes and effects of AI hallucination

AI hallucination—which is closely related to the issue of bias—is often mentioned, and can have a significant impact on the use of AI systems by the notarial profession. The phenomenon of AI hallucination is present in case of LLMs, mostly during the use of generative AI solutions, and consists of providing outputs which are non-existent (therefore, incorrect). At the same time, when the AI provides hallucinating output, it shows 'a high-level of confidence' regarding its accuracy. This is very much in contrast with the standard expectations of the human users who require the most appropriate and precise outputs to their prompts typed or dictated to the AI system (just like in real life, we expect correct answers to our questions from our service providers).

The most infamous AI hallucination case from the legal world comes from the United States, where a lawyer, Steven A. Schwartz, sent documents to the court containing several non-existent case law. The lawyer used ChatGPT to assist him in drawing up the documents, and the system made up cases which seemed fully and convincingly real. The lawyer proceeded uncarefully by not verifying the cases provided by the system. However, they were identified as non-existent by the competent judge, which led to the lawyer's liability and loss of reputation.

Behind the hallucination of the AI systems, there is generally no malicious intention. This phenomenon can mostly be tracked back to the technology itself, meaning that AI hallucination occurs mainly due to certain errors in the model's processing.

AI hallucination has three main sources. The first one is the inaccuracy of the training dataset. When an AI model is trained on a dataset which includes biases or unrepresentative (impaired) data, it may result in that it hallucinates patterns reflecting these biases and inaccuracies (giving false output based on false data).

The second source of AI hallucination is the model's complexity. The technological basis of LLMs is a specific neural network, whose decision-making processes are difficult to understand (LLMs are *'non-deterministic'*). Hallucination may occur because of the overfitting of the AI model, i.e. when the model becomes too much trained on its training data (including its *'noises'* which are irrelevant elements of data for the given purpose) rather than learning the underlying patterns. In consequence, when faced with novel inputs, the LLM may generate inaccurate outputs because it has learnt the training data and not the underlying patterns.

The third source is the lack of contextual understanding (i.e. the handling of the context), leading to struggles of AI models with context-specific issues. This can lead to the situation where a model generates a grammatically accurate but otherwise meaningless output.

4. Mitigating the AI hallucination

The explanations of AI hallucination in the previous point do not change anything in the fact that the phenomenon of hallucination gives the impression that these systems are unreliable, and the trust of their deployers can be significantly broken. This can be especially problematic in case of professions like the notariat, making important decisions in which the precision of data and information is crucial and the lack of it can lead to seriously negative consequences. For instance, an AI tool for anti-money laundering purposes which hallucinates may give false positives (flagging something as suspicious when in fact it is not) or false negatives (identifying something as non-suspicious when it is).

At the same time, the accurate use of reliable AI systems may bring plenty of benefits to the profession and it would be regrettable to completely discard the use of such systems as a consequence of some negative experience. Therefore, several solutions are present also to mitigate the AI hallucination.

First of all, it is necessary to ensure that applied AI model is trained with quality (complete, relevant, consistent) dataset, and it should be done with sufficient contextual and various data during the training process to avoid the issues of overfitting.

Secondly—especially in the beginning of its deployment—programming the AI model to generate its outputs based on pre-determined templates and setting limits to the possible outcomes, may contribute to the accuracy of the outputs.

Thirdly, the deployed AI models have to be regularly checked against known real-world information reflecting the context and, based on these checks, they have to be adjusted or re-trained, whenever necessary.

In this context, the process of *'AI grounding'* needs to be shortly mentioned, as—among others—the issue of hallucination can be tackled by grounding the AI system (typically the LLMs, especially NLP solutions) in the real world. More precisely, grounding means the process of linking AI outputs to real-world contexts and knowledge. Without grounding, AI models are limited to their initial training data and that data's timeframe, and generate outputs disconnected from reality, leading to false conclusions. Grounding can mostly be achieved by integrating domain-specific data (external data sources) and continuously updating the AI's training dataset (with real-time data reflecting new circumstances). The benefits of grounding are among others the increased accuracy, relevance and reliability of the AI outputs. However, grounding is a complex task from the technological and human (domain experts) side.

Finally, here also, the role of human (notarial) checking of the outputs is crucial. The notary has to carefully verify the precision of the given output, may it be reference to any legal provision, to case law or information deducted from any real-life data (e.g. the combination of data from registries or documents). By the timely detection and flagging of hallucination cases (deployer feedback), notaries can contribute to the amelioration of the given AI system.

Ideally, the combination of these solutions gives the best possible result. This requires the close cooperation between notaries and IT-specialists.

Key takeaways

- AI bias is an anomaly in the output by the AI model with two main sources: the prejudices in the training data and/or the prejudiced assumptions made during the development of the AI algorithm.
- The reason of the AI bias is that AI systems are created by humans and reflect their—mostly unintentional but natural—biases.
- Bias in the AI system possibly results in discrimination and leads to the violation of the principle of fairness.
- Survivorship bias is a special type of bias characterised by ignoring the unsuccessful outcomes in a selection process leading to the incompleteness of data and very often to incorrect outputs.
- Fully removing biases from the AI systems is generally not possible. Only mitigating bias is realistic.
- In order to tackle the issue of bias, the training data and the algorithm should be regularly and accurately monitored and comprehensively audited.
- Notaries should carefully check AI outputs for biases. Biased outputs should be disregarded for the notarial activity.
- The phenomenon of AI hallucination is commonly present, among others, in case of a large language models (LLM), mostly in generative AI solutions.
- The hallucinating AI provides 'with a high-level of confidence' outputs which are non-existent.
- AI hallucination can mostly be tracked back to the underlying technology itself.
- To mitigate hallucination, the training dataset has to be of a high-quality, and must include sufficient contextual and diverse data.
- Human oversight and feedback are crucial to detect and mitigate hallucination.

IX. Transparency and explainability of AI systems

1. General insights

Understanding the functioning of the AI systems, including their capabilities and limitations, is crucial in order to prevent the incorrect use of these systems as well as to avoid or mitigate the risks linked to the deployment of AI. AI providers have the inherent ethical and—inside the EU due to the AI Act—regulatory obligation to ensure the transparency of their systems, which includes among others, information about what the system developed by them is capable of, which uses it is appropriate and inappropriate for, according to which rules and methods the AI comes to an output.

The appropriate level of transparency and explainability efficiently contributes to the correct and efficient use of the AI models by the downstream providers working on AI solutions based on the model provided, as well as to the end-users (deployers) of such systems. Moreover, transparency and explainability increases the level of user and overall societal trust in the AI solutions, which is critical in the current times when this technology is surrounded by scepticism. Last but not least, transparency and explainability help fulfilling the necessary regulatory compliance.

2. AI Transparency and explainability – the main differences

Even if closely related to each other, the terms *'transparency'* and *'explainability'* have significant differences which require different approaches and methods from the providers as well as from the deployers of the given AI system. Both transparency and explainability aim at making AI systems understandable, regulatory compliant and trustworthy, but in different ways.

AI transparency focuses on the 'how'. More precisely, it means the accessibility of information to the persons with competence and rights (e.g. authorities, deployers, affected persons) about how an AI system was developed and how it functions (i.e. *'what's happening behind the scenes'*). It should span over the entire lifecycle of the given AI system. This includes information about the data used to train the system, the algorithms incorporated, and the main details of development and deployment.

AI explainability focuses on giving clear and understandable reasons for specific AI outputs (e.g. predictions, decisions, recommendations), making it understood why those outputs were provided. For instance, in case of recommendations for solving a legal case, the legal practitioner needs to have the relevant data and information on which the specific recommendation was based. This enables the deployer of the AI system to verify the accuracy of the output and to guarantee that the final human decision will be based on well-founded AI-assisted information. This way, the deployer can have the necessary level of confidence in the reliability of the specific output given by the system.

In summary: explainability focuses on making individual outputs understandable, transparency ensures clarity of the functioning of the AI system.

Besides, science makes the difference among the following three levels of transparency: algorithmic transparency, interaction transparency and social transparency. Without getting deeply into the content of these terms, algorithmic transparency focuses on the internal functioning of the algorithm and covers what is described above under *'AI transparency'*. Interaction transparency encompasses the interactions between human and machine, i.e. deployers and AI systems, is more related to the *'AI explainability'* above, and focuses on the comprehensibility of such interactions, and the understandability of what deployers can expect from their interactions with the AI. Finally, social transparency focuses on the broader impact of AI systems on the society, including ethics, fairness and equity, bias, as well as privacy.

3. Methods for achieving transparency and explainability

Transparency may be reached by the accurate and comprehensive documentation and disclosure of the main aspects of the given AI system. For instance, for high-risk AI systems qualified as such by the AI Act, there is a list of documents and information which should accompany the

AI system. However, in cases where further or different information about the system is mandatory for reasons of special compliance obligations or simply because of the individual requirements of the given deployer, other kind of information and documentation has to be added to the provided AI system. The documentation shall include, among others, the data sources and the main processing operations carried out on the training data, the description of the algorithms applied and their processes. In order to be transparent, the documentation should disclose the purpose and the limitations of the AI system, as well as the potential biases. The latter can be effectively mitigated by using the relevant documentation, more precisely by finding the data and/or the feature of the algorithm causing the bias.

AI explainability may be obtained by various techniques to make the outputs of AI systems understandable to deployers. Some technological methods were elaborated which break down complex models and identify how different data and algorithm features contribute to a specific output.

4. Transparency obligations in the AI Act

In Rectal 27 of AI Act, the legislator does not make the sharp distinction above between transparency and explainability, rather merges them: *"transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights"*.

The AI Act introduces 3 levels of transparency obligations: general rules apply to all relevant AI systems, high-risk AI systems are under stricter transparency duties and the providers of general-purpose AI models have the strictest and most extended obligations.

Article 50 of the AI Act introduces a general transparency regime to any AI system if it falls under one of the listed cases. For instance, providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, if it is not readily apparent to the given individuals. This obligation applies among others to chatbots and it must be fulfilled at the latest at the initial interaction with or exposure to the AI system by individuals.

In Article 13, the AI Act stipulates for transparency obligations of high-risk system providers in a general way. This includes that the relevant providers must design and develop their systems in a way that ensures sufficient transparency for deployers to reasonably understand the system's functioning and output. Furthermore, they should provide *'instructions for use'* to deployers, which give clear and complete information on the characteristics, functioning and other key features of the high-risk AI system.

Finally, according to Article 53 of the AI Act, providers of general-purpose AI models have to fulfil specific transparency obligations because of the complex features and capabilities of such models, making it even more difficult to understand their functioning. Such providers shall create relevant technical documentation covering their training, testing, and evaluation processes supply information and documentation to AI system providers who seek to use the model in their products, in order to understand the model's capabilities and limitations, and provide a detailed summary of the training content and data.

5. Black box AI vs. white box AI

Especially in case of large language models, the so-called *'black box issue'* remains a significant obstacle of both the AI transparency and explainability.

The society's need for transparent and explainable AI is shown by a recent development of the OpenAI company (developer of the ChatGPT) which launched an AI model officially called o1. This is an AI solution with reasoning capabilities, visibly 'thinking out loud' about why it is doing what it is doing, with the intention of making human deployers understand the steps the AI model takes to come to a conclusion. However, the details of what the AI is really doing remain under the hood for the sake of safeguarding trade secrets, and this situation is likely to remain unchanged.

In the classical situation when the deployer is facing the black box issue—due to the opacity of the AI algorithm—he/she knows the input and the output but cannot understand why the given AI system came to a certain conclusion (what happened between the input and the output of the system). Moreover, with self-learning algorithms, very often, even the developers of the given AI solution—despite their high-level IT knowledge—are unable to understand and explain how the given output has been reached. The black box phenomenon does not necessarily mean that the outputs of such systems are incorrect. On the contrary—thanks to their complexity—they can provide extremely precise outputs. The issue is the lack of inherent trust in such AI solutions because of the absence of transparency and explainability.

In contrast, the *'so-called white box AI'* is transparent about how it comes to its conclusions: the functioning of the algorithm and the factors influencing its outputs can be tracked and understood by the deployers. This results in higher level of confidence from the side of deployers, even if these models might have more limited capabilities.

Black box AI may be inappropriate for highly regulated sectors, such as the notariat, but may still be incredibly useful for other industries or sectors.

6. The importance of AI transparency and explainability in the notariat

In several sectors, the relevant professions have the duty not only to understand how the deployed technological solutions function, but also to explain their functioning to the clients. Within their procedures, notaries generally provide clients with legal advice, draw up acts, make binding non-contentious decisions, and have the duty to explain, in an easy-to-understand manner, the legal basis of these activities as well as their legal consequences. The general duty to inform the clients about the technological solutions applied, about their functioning and their depth highly depends on the provisions of the national law regulating the given notariat.

However, in accordance with Article 26 (11) of the AI Act: '*deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system*'. This obligation to inform clients only occurs when the given notary is using a specific high-risk AI system (the high-risk AI systems possibly used by the notarial profession are analysed in a separate chapter of this Handbook) which assists the notary in making a decision. This might occur mostly in the case of non-contentious notarial procedures. However, other decisions of the notary, for instance the refusal to proceed based on an emotion recognition high-risk AI system, can also trigger the notary's obligation to inform the clients. According to Recital 93, '*his information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation.*' Therefore, this is not an obligation to explain the functioning of the given system.

The previously mentioned right to explanation can be found under Article 86 of the AI Act: '*Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.*'

Therefore, if the notary applies certain high-risk AI systems listed in Annex III and has to make a decision and his/her decision producing one of the aforementioned effects is based on the AI output, then the affected person has the right to obtain an explanation from the notary about the AI system deployed. For this article to be applied, several conditions have to be simultaneously fulfilled: a specific high-risk system has to be deployed and the basis of the notary's decision should be its output. These decisions inevitably have legal or other significant effects on a natural person. In notarial procedures, with the exception of some notarial non-contentious proceedings, the probability that the given decision adversely affects the fundamental rights of a natural person is low. Nevertheless, it is important to keep in mind that Article 86 of the AI Act emphasises the need for notaries applying high-risk AI systems to understand the functioning of such solutions and to be prepared any time for such requests from their clients and to disclose their use.

Moreover, for the preservation of the positive image of the profession, in case of a request from their clients about the functioning of the AI solution used, notaries should be able to provide them with the necessary information, even if under a given jurisdiction, there is no express obligation to proactively inform the clients on the technology used or if Article 86 of the AI Act is not applicable in the given situation.

In cases when it is feasible, it could be practical for notaries who decide to use high-risk AI systems to have a document with a declaration at the end that the notary has informed the clients that he/she is using a high-risk AI system. This declaration would be signed by the clients as proof that the notary fulfilled his obligation. This document might also include a simple and understandable explanation on how the system works.

As already mentioned, the use of AI by notaries is not an aim itself but the AI is an assistance tool to streamline and facilitate their work and to increase their efficiency. In order to make full use of the AI's capabilities, notaries need to have a certain level of confidence in these solutions when making decisions about their use, especially when the stakes are high. Therefore, AI transparency and explainability play a crucial role for notaries as well. It is important to emphasize also here, that the notary should in each and every case be the final decision-maker, therefore, he/she must be in the position to overrule or discard any decision, recommendation or other output of the AI system when the grounds on which such output is based are not fully understandable to him/her. This should also cover situations which are present due to the absence of transparency and/or explainability.

In case the developer of the given AI solution is the notarial organisation (chamber) the notary is a member of, the organisation should guarantee the transparency and explainability by providing all necessary information about the AI system and permanently assist the notary whenever questions related to the topic arise. At the same time, notaries should provide the developer with feedback and insightful information from their practice and experience in order to—among others—increase the transparency and explainability of the system. Moreover, depending on the classification of the internally developed AI system or model based on the AI Act (high-risk, low-risk, no risk or general purpose model), the provider organisation shall observe and fulfil the applicable transparency and explainability obligations.

If the AI system is developed and provided by external service providers on the basis of individual agreement, this document shall contain strict duties for the provider for enabling the deployer notary to understand and explain the functioning of the system used. If the notary uses *'off-the-shelf'* AI solutions, the notary shall proceed with the utmost care and give up using the specific AI if he/she has concerns about understanding because of the lack of/limited transparency and/or explainability.

Key takeaways

- Transparency and explainability of AI systems contribute to their understandability, the enhancement of general trust in AI as well as to the regulatory compliance (e.g. AI Act).
- AI transparency and explainability are interrelated but different: explainability focuses on making individual outputs understandable, transparency ensures clarity of the functioning of the AI system.
- Transparency may be reached by accurate and comprehensive documentation and disclosure of the main aspects of the given AI system.
- One of the methods to obtain AI explainability is to break down complex models to identify how data and algorithm features contribute to a specific output.
- The AI Act introduces 3 levels of transparency obligations: general rules to all relevant AI systems, duty of transparency for high-risk AI systems and to the providers of general-purpose AI models.
- The black-box phenomenon is an obstacle of AI transparency and explainability. This means that, because of the opacity of the AI algorithm not only the deployer, but also the developers of the system cannot understand why it came to a certain conclusion. However, the outputs of the black-box AI are not necessarily incorrect, but the phenomenon has a negative influence on the necessary trust in these systems.
- Notaries have to inform their clients about the applied technological solutions only if the relevant national provisions prescribe it. However, on the basis of the AI Act, notaries deploying certain high-risk systems have to inform the affected persons thereof and these persons have in determined cases the right to obtain information about the functioning of the given system.
- However, notaries should always understand the functioning of the applied AI system and the reasons of its outputs in order to be confident about the use of the specific AI solution, to make a reliable and compliant final decision in the process in which the AI is used and to the preserve the positive image of the profession.
- In case of lack of transparency and/or explainability, notaries shall discard the output of the AI system used and provide timely feedback to the relevant provider.

X. Human-in-the-loop—the role of the notaries in the AI-driven world

1. Capabilities and limitations of AI

Although called *'artificial intelligence'* in everyday language, AI systems are not intelligent in the human sense of the word. According to the definition of the Oxford Advanced Learners' Dictionary, intelligence is *'the ability to learn, understand and think in a logical way about things'*. AI systems are able to 'learn' data and apply this data in the way in which and for the purposes for which they have been programmed by human developers. However, AI does not have the capability to understand things and to think the way we humans do. Therefore, despite its conventional naming, AI cannot be considered intelligent and intelligence remains, for the time being, the exclusive realm of humans.

Current AI systems can excel in specific tasks which they are trained for. In principle, they are able to provide correct and reliable outputs related to those tasks. However, this ability of AI is very much investment dependent: the systems which gain more financial, human and time investment (e.g. self-driving cars, medical AI solutions) and systems with high stakes, are generally much more reliable than those which relate to more 'marginal' areas. In our days—despite the hype around ChatGPT and similar solutions of big companies—no general AI exists which has the capability of providing appropriate outputs in all domains. For instance, AI solutions developed for medical purposes, cannot be used in the legal field. Besides, focusing on the field of law, an AI system trained for helping legal research is most probably not the best choice to assist legal practitioners in drawing up legal actions to be filed with courts.

AI has other important limitations which must be taken into consideration when using such systems. First of all, current AI systems are not able to put situations into a context the way humans do. For instance, in case of lawsuits, an AI system can provide the relevant provisions of the applicable acts and the related jurisprudence, but is not capable of understanding the features of the given situation and to take into consideration all necessary factors to give or recommend a correct and trustworthy decision.

Besides, AI is unable to show any human-type creativity which is necessary in the legal field, especially in case of devising legal counsel. AI is able to *'hallucinate'* which could be confused with being creative. As with humans, hallucination is a negative phenomenon, contrary to the positively qualified *'creativity'*. Behind human creativity is a human's decision to create something and such decision does not necessarily stem out of pure necessity. In contrast, AI hallucination is the direct—even if negative—result of the algorithm's programming.

Despite this and despite the broad recognition of the risks of AI systems, the phenomenon of automation bias, the over-reliance on suggestions made by digital systems is very much present and can occur also in the legal field. As already mentioned in this document, the best example of this is the case of an attorney-at-law in the United States of America filing documents at court, with case law only made up by ChatGPT. This sole case in itself demonstrates that the outputs of AI, however correct and convincing they might seem to appear, cannot be trusted blindly. Critical approach, high-level of diligence and stringent control need to be exercised to avoid situations which could lead to harmful consequences. This emphasises the central role of humans within the AI ecosystem, the human-in-the-loop.

2. The role of notaries in the presence of AI

Civil-law notaries are without exception fully qualified legal professionals who become entitled to practice their profession after numerous years of legal practice and stringent examinations. Already for several decades, various technological solutions have been important and necessary part of the notarial work. Without their deployment, notarial proceedings would be slower and less efficient. Therefore, despite the reasonable initial scepticism, embracing and adopting technological innovations is crucial also for the notarial profession, and AI cannot constitute an exception to this.

It should be emphasised that, based on the deficiencies of the AI systems mentioned in this Handbook, AI is currently not able to replace notaries (nor similar legal professions) or jeopardise the profession as a whole. Society is generally sceptical of exclusively machine-made decisions.

The central presence and activity of humans is required (*'humans want advice from and decisions by humans'*). Obviously, this does not mean that society objects to the appropriate and circumspect deployment of cutting-edge technological solutions in the human decision-making processes. However, AI systems do not possess the skills a human trusted third party has (e.g. emotional intelligence, putting oneself in the clients' shoes) and which, besides their professional knowledge and experience, highly contribute to the confidence clients vest in notaries.

Therefore, even in notarial activities and proceedings, AI can serve as an assistance tool whose capabilities and limitations should be well-known by notaries, the deployment of which has to be under their strict human supervision and whose outputs (decisions, recommendations, etc.) should be thoroughly checked and verified before applying or discarding them.

This does not result in the fact that in an AI-driven world, the role of the notaries will be reduced to simple *'checkers'* of AI outputs. AI can accelerate the work of notaries by completing routine tasks (e.g. collecting basic information about the real estate subject to a notarial sale and purchase contract) or administrative tasks (e.g. billing or arrangement of an appointment) which do not require deep legal knowledge. Moreover, it can effectively assist notaries in spotting the relevant legal provisions and jurisprudence, saving significant amount of time for the notary. However, judging the appropriate nature of the output for the given context as well as its application exclusively depends, and should continue to depend, on the knowledge, experience and expertise of the notary.

Within the field of notarial activities, current AI solutions are not able to fulfil any task which cannot be carried out by the notary himself/herself. The main positive difference can be the pace of arriving to a conclusion, just like in the case of a simple calculator: humans are able to calculate very complex mathematical exercises, the calculator only accelerates the process of counting. Differently from counting, however, in notarial cases, there is almost always not only one solution to a matter, but several ones. Therefore the output of the applied AI has a different weight than the one made by a calculator. This means that like any other tech solution, AI complements the work of the notary. Just as in cases of products with embedded AI, notaries have to be able to *'push the stop button'* and fully disregard the output of the AI systems.

3. How to work with AI?

Both in case of internally (by notarial organisations, chambers) developed or externally purchased AI solutions, the involvement of notaries is important from the outset. Notaries can identify their needs and the purpose for which they intend to use an AI system and subsequently actively participate in the testing process of the given solution (e.g. in sandboxes).

Notarial organisations (chambers) have the task to increase the AI literacy of notaries by training them on how and in which situations AI systems may be used. For instance, in the case of generative AI models, where the quality (e.g. relevance, completeness) of the user prompts is crucial to get the correct output, notaries need to be trained on appropriately formulating their prompts since this would have a huge bearing on the output.

Finally, notarial feedback is crucial in spotting, in real-world circumstances, the unexpected limitations and deficiencies of the AI system used. Therefore, notaries should be given an easy-to-use way to speedily report such information to the notarial organisations (chambers) they are members of and to the competent service providers.

Notaries should strive to make use only of the best possible AI solutions which are transparent and explainable and should refrain from deploying systems whose reliability cannot be checked and where the slightest risk of infringing any important notarial obligation (e.g. breach of professional secrecy) can be present.

Key takeaways

- AI is not intelligence in the human sense of the word. AI is unable to understand and to think.
- Current AI systems are not capable of putting things into context and of being creative.
- AI systems can excel in tasks which they are trained for but currently no general AI exists which has the capacity to provide precise and reliable outputs in every field of life.
- The automation bias, i.e. the over-reliance on the suggestion given by technological solutions needs to be avoided. The reliability of AI outputs always has to be verified. Despite this, embracing and adopting technological innovations (including AI) is crucial also for the notarial profession.
- Currently, no AI solution can replace notaries. Clients require human interactions and decision-making, as well as the presence and application of skills (e.g. empathy) only humans possess.
- Current AI solutions are not able to fulfil any task which cannot be carried out by the notary himself/herself.
- AI can serve as an assistance tool for notaries. The deployment of AI systems has to be under strict human supervision, their outputs should be thoroughly checked and verified before applying or discarding them.
- Notaries should take an active role in determining the purpose of the AI solutions to be used by them and in the testing such systems. Notaries should regularly give feedback on such AI systems.
- The AI literacy of the notaries has to be increased for the efficient and safe use of AI systems.

XI. Intellectual property and artificial intelligence

1. General insights – Identification of the relevant IP rights in notary-AI context

There are several types of intellectual property (IP) the most widespread being the copyright and related (neighbouring) rights, the *'sui generis'* database right, the trademark and the patent. All these types of IP have different subjects of protection and occur in different situations. AI has specific connections and issues with each one of these IP rights which require specific examination.

In the notary-AI context, the copyright and the 'sui generis' database right have the highest importance, as copyright-protected works and databases are used and can be produced every day in the notarial practice. Therefore, the present chapter exclusively focuses on these two IP rights.

2. Copyright protection for notarial acts and legal instruments, protection of databases in AI training

a) Copyright and notarial acts

Copyright is a widely harmonised field within the European Union. Despite the co-existence of the national copyright systems, the criteria of protection and the key terms related to the field constitute autonomous European concepts which have to be applied uniformly across the 27 Member States. However, the field of copyright is characterised by the principle of territoriality, which means that together with the EU legislation, the national rules have to be thoroughly observed because of the differences in matters which are not harmonised at EU level. Because of this, in this chapter, the relevant EU legislation is presented, and some points are raised which can be used for verifying the legal situation in the different Member States.

The main criterion of copyright protection all over the EU is the originality of the work. In order to enjoy the benefits of copyright, the specific work has to be *'original'*. This simple term has been interpreted in the Infopaq I decision of the European Court of Justice. The Infopaq I decision defined *'originality'* as the *'author's own intellectual creation'*. This constitutes a relatively low threshold of protection, and as the pecuniary value, the aesthetic characteristics of the work as well as the amount of time, effort and energy invested into its creation cannot play a role in the qualification as copyright-protected, plenty of works fall in the realm of copyright. Furthermore, it is a basic principle that pure ideas cannot enjoy copyright protection, they must be expressed in some form (e.g. in writing) to achieve this.

The criterion of originality results in—in principle—that notarial authentic acts might be copyright protected as soon as they are the *'author's (i.e. the notary's) own intellectual creations'*. In contrast, certain templates and forms used in the notarial practice (e.g. the European certificate of successions) cannot be copyright-protected, as they do not fulfil the criterion of originality (and often they are part of official legal acts which usually fall outside the scope of copyright).

However, copyright remains—despite its EU-level harmonisation—a national field, and the relevant legislation of the notary's country has to be checked to verify whether or not notarial acts are excluded from the copyright protection (e.g. in some countries, official documents by public authorities are excluded from copyright.) Also, depending on the national applicable law to the notarial acts, it can be possible that—if the protection applies—the economic rights of copyright on these acts (e.g. the right of reproduction) are transferred to the respective clients of the notary upon payment of the notarial fees.

In the case that in a national legal system the copyright protection of notarial acts is not excluded, it may have an impact on their use in AI context. More precisely and in principle, their reproduction for the training of (notarial) AI systems would be subject to authorisation (licensing). Moreover, as indicated in the relevant chapters of the present Handbook, personal data, professional and client's trade secrets can also constitute hurdles in the use of notarial acts as AI training material, and it would have to be checked whether even the notarial organisations (chambers) the notary is member of can have access to the content and/or metadata of the acts archived in paper-based or electronic format.

b) Protection of legal texts and case law

Besides, on the *'input'* side of the notarial practice, legal texts and jurisprudence are permanently used. For practical reasons and because of their public importance to society, official legal texts and jurisprudence, in most of the countries, fall out of copyright protection. These legal sources have to be freely accessible and their reproduction has to be allowed without restrictions in order to enable citizens and legal persons to enjoy their rights and observe their duties. This means that these texts can be freely used (e.g. reproduced) also for AI training, in our case for the training of notarial AI systems. However, also in this respect, the relevant national legislation on copyright always has to be thoroughly examined.

c) Database protection

Legal and non-legal databases—regularly used by notaries—can be protected in two different ways: *'general'* copyright protects the database if it is original in its selection, coordination and arrangement. This protects the structure of the database, not its content (which can be works without copyright protection). This results in—among others—that the mere alphabetic arrangement of data is not original enough for protection of the database by *'general'* copyright law.

However, for databases which do not reach the required level of originality, the European legislator introduced the so-called sui generis database right. This *'sui generis'* protection is granted to honour the substantial investment (financial, material and/or human) in either obtaining, the verification or the presentation of the database content. Contrary to the *'general'* copyright, the *'sui generis'* right protects the content of the database and gives a protection of 15 years which begins on the date of creation or of the first making available to the public. Both types of protection might in principle result in that reproducing the same database, extracting or reusing the whole or a substantial part of the database's content for (notarial) AI training infringe the copyright or the *'sui generis'* database right.

3. Text and data mining exception and limitation for AI training

Based on the general rules of copyright (Article 2 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, briefly: the InfoSoc Directive), the author of the respective work has the exclusive right of reproduction regarding the entirety or part of his/her work. Reproducing the given work can be authorised to third parties mainly through licensing. As mentioned under the previous point, in case of the *'sui generis'* database right, the maker of the database has the exclusive right to prevent the extraction and/or reuse of the whole or a substantial part of the database's content.

Taking into consideration the extremely large amount of data (including copyright-protected works) required for AI training purposes, requiring and providing a license every time and for each work would be excessively burdensome for the AI developers and providers, as well as for the rightsholders. However, as the use of works could be considered unauthorised reproduction and reuse, the exclusive rights of the rightsholders—without specific legislative intervention—would constitute legal obstacles to the training of AI models. This could not only hamper the development of AI models, but also can jeopardise the AI innovation and ecosystem as a whole.

In order to give a solution to this issue, the EU legislator introduced in 2019 the so-called text and data mining (TDM) exceptions and limitations in the Directive on the Copyright in the Digital Single Market. In accordance with Article 4, Member States shall provide for an exception or limitation among others to the exclusive rights of reproduction and extraction of copyright-protected works and data from the databases protected by the *'sui generis'* right for the purpose of TDM. The aim of this provision is to free the AI developers and providers from the above license requesting.

This TDM rule does not make any limitation in respect of the entity making use of it, which results in that AI models developed by the notariat can fall under its scope and the profession can make use of it. Besides, the purpose and character (commercial or non-commercial) of the TDM is not limited and the provision only sets as a requirement the lawful access to the given work/database. However, the scope of this exception or limitation is reduced by the opt-out possibility that can be exercised by the given rightsholder (author of the work, maker of the database, including the notary whose acts may be under copyright protection based on the applicable law), re-making it necessary to ask for authorisation for uses of TDM purposes.

In case of content that has been made publicly available online, the rights above can be reserved by the use of machine-readable means which includes metadata and terms and conditions of a website or a service. In other cases, reservation can be carried out for instance by contractual agreements or a unilateral declaration. Therefore, in case of notarial AI development—besides the lawful access to the given material—the opt-out exercised by the given rightsholder has to be checked and respected. In case the opt-out is expressed, the material has to be discarded for TDM and AI training or the notariat developing the system needs to obtain license for such uses. If no opt-out was exercised, the developer is free to use the given work for AI training.

Moreover, Article 53 of the AI Act contains 'mirror' copyright provisions in case the (notarial) AI development is a general-purpose AI model. In this case, the provider has the obligation to put in place a policy to comply with Union law on copyright and in particular to identify and comply with the opt-out right of the Directive on the Copyright in the Digital Single Market, as well as to draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, using templates provided by the AI Office. The aim of this provision is to enable the rightsholders the identification of the use of their works for AI training purposes.

4. Copyright protection of the AI output

Within the EU, the copyright protection applies exclusively to human-made works, which implies that works generated by AI fall outside the copyright realm. However, the works produced with the assistance of AI can be copyright-protected if they fulfil the criteria of originality, i.e. they are *'the author's own intellectual creations'*.

As mentioned in various chapters of this Handbook, the notarial (human) checking and correction of the outputs created by AI solutions is indispensable, and taking into consideration the role and capabilities of the AI (assistance tool for facilitating and streamlining the work, lack of understanding of the context, etc.) it is quite unrealistic that notaries take over one by one—without corrections, additions, amendments—the outputs provided by the AI. The more complex the intended result is, the higher is the probability of deep human intervention. Therefore, the AI serves as a mere assistance tool in these cases, subject to the provisions of national copyright law. Documents produced by the notary with AI assistance (authentic act, legal advice, research, etc.) can fall under copyright protection.

At the same time, in case the AI output is exactly the same or substantially similar to a previously created work and the independent, double creation (production of the same or substantially similar work without any connection between the two works and authors) cannot be proved, there might be a risk of copyright infringement. Therefore, (partial) re-formulation of the given AI output by the notary according to his/her professional methods, own style and vocabulary is highly recommended.

Key takeaways

- In the notary–AI context, the most relevant intellectual property rights are the copyright and the *'sui generis'* database right.
- Copyright is a partially harmonised field, but the principle of territoriality applies, which results in that together with the EU legislation, national rules of the respective countries have to be checked.
- The main criterion of the copyright protection is that the given work has to be original, i.e. has to be *'the author's own intellectual creation'*. The author has exclusive rights of reproduction of part or the entirety of the given work.
- Depending on the national legislation, notarial acts fulfilling the criterion of originality may enjoy copyright protection which can hinder their use for (notarial) AI training purposes.
- In general—but also depending on the national legislation—official legal acts and jurisprudence fall out of the scope of copyright, meaning that these texts can be used without authorisation for AI training purposes also within the notariat.
- The IP protection of databases is twofold in the EU. The *'general'* copyright provisions apply (criterion of originality) to the selection, coordination and arrangement of the data. On the other hand, the *'sui generis'* database right is granted to honour the substantial investment (financial, material and/or human) in either, obtaining, the verification or the presentation of the database content. Both protection rights might result in infringement in case of (notarial) AI training.
- Extremely large amount of data is required for AI training purposes, therefore, asking and providing license for each of them would be excessively burdensome for the AI developers and providers as well as for the rightsholders.
- In order to prevent the infringement of relevant rights and facilitate the AI developments, Member States had to introduce a text and data mining exception or limitation with the opt-out possibility for the rightsholder.
- AI generated works are not copyright-protected in the EU but the AI-assisted ones may be.
- It is recommended for notaries to (partially) re-formulate the AI-assisted output to avoid any risk of copyright infringement.

XII. Off-the-shelf, internally developed and externally provided AI systems

1. 'Off-the-shelf' AI systems

The legal sector, especially the notariat, has numerous specificities which influence the choice of the applied technological tools to be used. *'Off-the-shelf'* software tools, websites and other applications (including AI systems, like for instance ChatGPT, DeepL or Microsoft Copilot) offered to the public online free of charge or in exchange of payment might be used for some specific tasks by notaries. They are generally extremely cost-effective compared to custom ones. Furthermore, the time of development of such solutions is spared because they are usually immediately accessible and applicable. Also, the possible failures of development and the need for algorithm corrections are at the charge of the service provider.

However, the risks of using such AI solutions by default within the notariat are extremely high and usually exceed the potential benefits. The providers of these solutions apply their general terms and conditions which are unilaterally drawn up by them and in which their costumers do not have space for manoeuvre. Moreover, usually there is no guarantee that the *'off-the-shelf'* tools ensure the protection of personal data or the professional and clients' trade secrets, which is crucial for professions like the notariat. Besides, data generated by notaries (e.g. contractual clauses formulated by them) not falling into the previous categories and used as input (e.g. in machine translation solutions) may also be under risk of being further used for training such systems. Furthermore, the sources, the legality and the quality of the data used by such systems often cannot be verified and this may cause issues of copyright infringement, as well as bias. Even if several of these solutions are open source, their providers have their related trade secrets which, on top of the *'black box issue'*, makes it extremely difficult to oversee the functioning of the underlying algorithm as well as to explain why the system came to a certain conclusion (issue of transparency and explainability).

Notaries are not strictly discouraged from using *'off-the-shelf'* AI systems, but are strongly recommended to deploy them with the utmost caution. Various chapters of this Handbook identify the risks (e.g. protection of personal data) one needs to consider when using AI solutions. These risks may be exponentially present when *'off-the-shelf'* AI is used. In case the given risk cannot be avoided or mitigated to the very minimum, it is suggested that the notary avoids the use of the specific system.

2. Advantages and difficulties of internally developed notarial AI solutions

There are specific notarial fields and matters with regards to which *'off-the-shelf'* AI systems cannot provide appropriate and efficient assistance. These systems are most of the time generic ones which are not calibrated to the legal sector and definitely not to the notarial profession (i.e. ChatGPT has extremely limited abilities in correctly drafting notarial deeds). Therefore, in certain cases, only custom, tailor-made, internally developed notarial AI systems can provide the necessary solution. Internal AI development in this context means the development of AI systems exclusively by the given notarial organisation (chamber). This point exclusively addresses notarial organisations, as it is not realistic—mostly due to the costs it triggers (see below)—that individual notaries develop their own AI solutions. Notarial AI systems internally developed by and for the profession have the inherent advantage of efficiently avoiding or mitigating the issues mentioned under point 1 of this Chapter.

Notaries accumulate extensive amount of data every day. These data are profession-specific, therefore always relevant and accurate. Notarial AI solutions must be trained mostly on data coming from the profession and from data sources which provide quality data and to which the profession has lawful access. This guarantees that the intellectual property rights and various rights on data are not infringed, the quality of data is appropriate and the output by the system based on data is not false. Moreover, the protection of the clients' personal data and trade secrets as well as the notaries' professional secrecy can be efficiently guaranteed by establishing technical solutions in the specific AI system.

The difficulty which can arise in this case is the access to individual notaries' data by the competent notarial organisation (chamber) developing the AI system. Different countries have different regulations in this respect, therefore, it might be possible that notarial organisations (chambers) do not have or have limited access to such data or can have access to them only after pre-processing (e.g. masking) them adequately. Therefore, the relevant national restrictions always have to be taken into consideration. If there exist limitations in this respect, the use of templates, excerpts, and similar anonymous documentation prepared by the profession or synthetic data may offer a solution for the training of the given system. Furthermore, in countries where notarial organisations (chambers) can have access to the relevant data—in order to respect the intellectual autonomy (e.g. individually formulated contractual clauses) of notaries—they should be given the opportunity to require the respective organisation (chamber) to leave out their acts, certain acts or parts thereof from the training of AI systems. This opportunity should be made available also in cases where the given country does not qualify the notarial acts as copyright-protected works for which TDM opt-out can be exercised.

As mentioned under the relevant chapter, the AI bias cannot be fully removed from the systems—due to the fact that it is an inherent biological characteristic of humans—but the mitigation of the bias and possible hallucination can be more efficiently and speedily carried out in case of internally developed notarial systems. By introducing built-in feedback mechanisms, notaries can give direct and immediate feedback and inform the developer about their practical experience with the given solution, rendering the AI system more efficient and more precise.

As the control of the development and updating of these systems are in the hands of the profession, the transparency and explainability of such systems can be guaranteed from the first step of the development, resulting in the avoidance of the *'black box issue'*.

The internally developed AI solutions can also be incorporated in the already used notarial digital administration tools, thereby ensuring the interoperability of such systems with the already applied digital solutions. The notarial organisation (chamber) providing its AI solution should ensure the necessary training for notaries and the employees of notaries using such systems and remain available to correct technical issues when necessary.

At the same time, it must be taken into consideration that the development of AI systems is costly, especially when it comes to sophisticated solutions like LLMs and generative AI systems. Developing AI solutions from scratch generally requires long time (development, training, validation, testing, etc.). Besides, such developments require IT specialists and expertise. Furthermore, in case a developed AI system falls under the high-risk category of the AI Act, the notarial organisation (chamber) as provider has to fulfil a wide range of compliance requirements (see the relevant chapter). Currently, not all the notarial organisations might possess the necessary financial/technological/human means to be able to set up such systems, which can lead to having recourse to external service providers.

3. Notarial AI systems provided by external service providers (AI as a Service)

In case a notarial organisation or the individual notary (the two further mentioned under this point as: 'deployer') turns to an external service provider in order to develop and provide a specific AI system, the two main steps taken should be the circumspect choice of the provider and the negotiation of individual contractual terms (AI as a Service – *AIaaS*–contracts).

Very often—especially when the service provider is not a well-known company—conducting due diligence on the service provider is extremely useful in order to assess the risks the recourse to the given provider implies. In the eventuality that the results of the due diligence do not indicate sufficient reliability and expertise on the part of the provider, it is strongly recommended to continue looking for another provider to fully satisfy the needs of the deployer.

In the AIaaS contract, the deployer has to clearly determine and communicate in details the exact purpose of the system to be developed by the provider and the characteristics, as well as the regulation of the activity in which the AI system will assist the deployer.

Besides the usual terms in contracts, clauses on the following matters must be included into the AIaaS contract (the list is not exhaustive, depending on the circumstances, the needs of the deployer, the national regulation, and other matters, other or different clauses might be necessary):

- Requirements of data quality in order to ensure that the data used for the training and operation of the system is appropriate for its purpose;
- Criteria on the sources of training data to guarantee that the data comes from legal and lawfully accessed sources;
- Rights (including IP rights) on the training data, input and output data, in order to ensure that the provider does not get rights on the data provided by the deployer and on the data in prompts as well as on the output data of the system. Moreover, it is strongly recommended to state in the contract that none of the data can be used by the provider for training other AI systems;
- Intellectual property rights (including copyright, patent, trademarks) related to the system and the components of the system provided;
- Personal data protection, in order to guarantee that the relevant rules of the GDPR are appropriately complied with when personal data of the notaries' clients are inserted in the AI system;
- Protection of the professional secrets, trade secrets and other confidential data, to ensure that the secrecy of such data of clients and of the deployers is kept;
- Duty of transparency of the AI system and the explainability of the output, to ensure that the functioning of the system and the production of the output is clear and understandable to the deployers;
- Obligation of regular updating and maintenance of the system, which should cover the updating of the training dataset, and the technological updating of the algorithm used with additional duty of information before the planned update and after its completion;
- Ensuring the compatibility and interoperability with other digital systems used by the given deployer, in order to be able to smoothly incorporate the AI solution into such systems;
- Timely intervention in case of defects and malfunctioning of the system, which should also include the de-biasing and the mitigation of AI hallucinations;
- Obligation of training the deployers about the proper use and specificities of the system;
- Setting up measures to guarantee the appropriate level of cybersecurity;
- Determination of liability and full indemnification in case damages are caused because of the deficiencies and/or malfunctioning of the system;
- Dispositions in respect of third-party offerings (i.e. when the service provider's system will be used in combination with a different provider's system, as a service built on it), in order to avoid the occurrence of any underlying issues related to the previous points because of the terms with third parties;
- Compliance with other provisions required by the relevant legislation (e.g. the AI Act's registration obligation of the high-risk AI system into the EU Database by providers of such systems is fulfilled).

Finally, taking into consideration the definitions of *'provider'* and *'deployer'* in the AI Act, it has to be determined whether in case a notarial organisation (chamber) orders from an external provider for the notaries who are its members, the development of an AI system falling under the material scope of the AI Act, it will be considered as a provider or deployer. This is a significant difference in respect of the more extensive compliance obligations of the providers than of the deployers regarding high-risk AI systems.

In accordance with Article 3 (3) of the AI Act, *'provider'* means also an entity that has an AI system developed which it puts into service under its own name or trademark, whether for payment or free of charge. Putting into service means, according to paragraph 11 of the same Article, the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose. In this situation, the deployers of the AI system will definitely be the notaries, and the action of putting into service could also occur, as the notarial organisation (chamber) would supply the AI system for first use directly to the notary deployers. However, in case the given notarial organisation (chamber) would not put the system into service under its own name or trademark (it is likely that the 'real' and original provider's name or trade mark will be indicated in the product), the qualification as provider will not apply. Therefore, in this situation, the relevant disposition of the AIaaS contract (on the indication of the name and/or trade mark of the developer/original provider) has to be formulated carefully, indicating the name and/or trade mark of the external service provider.

Key takeaways

- *'Off-the-shelf'* software tools, websites and other applications offered online to the public free of charge or in exchange of payment might be used for some specific tasks by notaries.
- The risks of such systems (e.g. protection of personal data, bad quality of data, etc.) usually exceed their potential benefits for the notariat.
- Notaries are not strictly discouraged from using *'off-the-shelf'* AI systems, but it is strongly recommended to deploy them with the utmost care. If the given risk cannot be avoided or mitigated to the very minimum, it is suggested that the notary avoids the use of the specific system.
- In certain cases, only tailor-made, internally developed notarial AI systems can provide the appropriate assistance to notaries.
- The internally developed notarial AI systems can guarantee the quality of the data used, the protection of personal data, clients' trade secrets and professional secrecy, the speedy reaction to bias and hallucination, the transparency and explainability, as well as the compatibility and interoperability with other digital notarial systems.
- The internally developed notarial AI systems have also certain downsides, which are—among others—the high-costs, the long time and the required IT staff for development.
- If a notarial organisation or an individual notary turns to an external service provider in order to develop and provide a specific AI system, the circumspect choice of the provider (due diligence is recommended) and the negotiation of individual AI as a Service contractual terms are crucial.
- The deployer has to clearly determine the exact purpose of the system to be developed and the characteristics, as well as the regulation of the activity in which the AI system will assist the deployer.
- Several key contractual clauses should be individually negotiated in respect of—among others—the data sources used, the liability of the provider, the rights on different kinds of data, as well as on personal data protection, regular updating and maintenance of the system.
- In case the notarial organisation (chamber) orders externally provided AI solutions (falling under the material scope of the AI Act) to its member notaries—in order to avoid the qualification as provider—the external service provider's name and/or trade mark should be indicated instead of the name of the notarial chamber.

XIII. Basics of AI cybersecurity

1. General insights

AI technology is more and more often used to support the cybersecurity protection of various entities (‘*cybersecurity with AI*’). At the same time, AI systems are themselves exposed to cyberattacks, the protection against which is crucial in several respects (‘*cybersecurity of AI*’). Cyberattacks against AI systems can compromise not only the functioning of the given system, but can cause further harm to the organisation deploying them which can extend from negative reputational damage, to data protection breaches and to severe financial consequences.

Cyberthreats and attacks are intentional and most often exploit the vulnerabilities of the AI systems, targeting mainly the training data and the integrity of the applied algorithm. Through these potentially compromised components, attacked systems can be used for malicious purposes. The main purpose of AI cybersecurity is to prevent the unauthorised access to, the manipulation and misuse of AI systems, with the security of data and the protection of models in its focus. As AI systems become more powerful and widely used, maintaining their robustness and security becomes even more crucial.

Under the following points, the possibilities of cybersecurity with AI will not be discussed, only the possible cyberthreats and attacks as well as the possible measures to tackle such threats/attacks ensuring the safe operation of such systems will be presented. The aim of this Chapter is to give a basic understanding of the cybersecurity of AI for notaries, therefore, deep technical aspects will not be discussed.

2. Security risks AI systems face and possible counter-measures

For the purpose of illustration of their various nature and without being exhaustive, under the following sub-points, some cyberthreats and attacks against AI systems are presented. They can impact both the stages of development (training, testing) and deployment (entering prompts, providing outputs). They can be related to the integrity [sub-points a)-d)], to the confidentiality [sub-point e)] or to the availability of the AI system [sub-point f)].

a) Evasion attacks

In case of evasion attacks—by exploiting the model’s vulnerabilities—the attackers subtly manipulate the input data in a way that results in incorrect outputs.

For instance, in case of image (facial) recognition, the input picture can be slightly altered in a way imperceptible to the human eye, causing it to lead to a false output (e.g. false positive for the recognition of the client’s face through videoconferencing). From the technological side, tackling evasion attacks is possible, for instance by using adversarial training, in which case, the AI model is exposed to and trained on a variety of manipulated inputs. Besides, continuous checking and analysis of the inputs and outputs can help in countering such attacks.

b) Training data poisoning

In case of training data poisoning, malicious data (e.g. false information, like outdated legal texts instead of the ones currently in force) is introduced into the training dataset of the AI model. Furthermore, data poisoning can also be achieved by altering or deleting (part of) the dataset. The consequence of data poisoning is a compromised AI model with unpredictable functioning as well as unreliable and inaccurate output. This attack is particularly dangerous, because the poisoned data is often not quickly identifiable amidst the extensive quantities of training data. When such breach is detected, it must be traced back and the dataset immediately restored. In some cases, the model needs to be completely re-trained.

c) Model poisoning

In case of model poisoning, the attackers modify the model parameters or architecture with malicious intent. Model poisoning modifies the behaviour of the model in an unexpected way. The detection of model poisoning is difficult because it is often unnoticeable and its effects come to the surface only under specific conditions.

In order to tackle such attacks, model inspection and sanitisation is applied where the trained model is checked for anomalies. Subsequently, the model can be fixed by fine-tuning, re-training or removing some parameters (pruning).

d) Prompt injection

Prompt injection is specific to LLMs, especially to natural language processing (NLP) solutions. Prompt injection attacks consist in crafting prompts to manipulate the behaviour of the AI system resulting in the production of harmful (e.g. biased or inaccurate) or unintended (revealing confidential data) outputs based on the system's reliance on those prompts. These attacks exploit the fact that an AI model's output can be significantly affected by the phrasing and structure of the prompt it receives.

For instance, in case of a chatbot, the attacker could intercept interactions of other users with the system and inject well-crafted malicious prompts asking for all the queries of such users (possibly including confidential data).

In order to counter prompt injection attacks, several methods are available. For example, input sanitisation can be carried out which involves the cleaning and validation of prompts that AI systems receive to ensure that they do not contain malicious content (i.e. using regular expressions to identify and block inputs that match known malicious patterns). Besides, the adversarial training (mentioned above) can also prove useful to counter prompt injection attacks.

e) Model theft (model extraction)

Model theft (or model extraction) means the unauthorised (e.g. without the permission of the developer) copying of an AI model. This can be considered a violation of intellectual property with significant financial impact (due to the value and cost of the training of AI models). Beside these negative impacts, model theft poses security risks when the given model is used to identify vulnerabilities for preparing further attacks.

Securing AI models against theft involves—among others—the introduction of access controls (only authorised users can interact with the model based on verification of user identities), encryption of model data and invisible watermarking of outputs (to trace and identify unauthorised use).

f) Denial-of-service (DoS)

Denial-of-service (DoS) attacks are malicious attempts with the aim of disrupting or shutting down the functioning of an AI system by overwhelming it (by providing an excessive volume of prompts or complex data inputs), rendering it unresponsive or significantly slower. By disrupting the functioning of the AI system in such a way, legitimate users are unable to access it.

Countering such attacks is possible by increasing the robustness of the system, for instance by monitoring unusual traffic patterns and by developing systems which block the sudden increase of prompts.

3. European regulation of AI cybersecurity

a) Regulatory landscape

Despite the obvious importance of the cybersecurity of AI systems, and the existence of general cybersecurity legislation (e.g NIS2 Directive) at EU level, the current EU legislation does not contain special legal acts in respect of AI cybersecurity, and other acts (e.g. the AI Act) barely include rules specific to this topic. However, national legislation and soft law sources on (AI) cybersecurity always have to be taken into consideration (e.g. the Netherlands has already started to lay down a plan—The Netherlands Strategy Action Plan for AI—which includes relevant statements).

b) AI Act

The AI Act includes specific obligations on cybersecurity and robustness for providers only in respect of high-risk AI systems (and general-purpose AI models with systemic risk). The relevant articles (Article 15) and recitals (66, 74 and 75) do not provide detailed guidance on how to fulfil these obligations.

In accordance with Article 15 (1) of the AI Act, '*high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.*'

Moreover, paragraph (2) of the same Article declares that '*high-risk AI systems shall be as resilient as possible* *regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard.'*

Finally, paragraph (5) of Article 15 states that '*high-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.'*

Paragraph (4) can be understood to mean that the requirement of robustness also covers the resilience of AI systems to cyberattacks and ensures that an AI system is capable of functioning appropriately under difficult circumstances (e.g. when exposed to cyberattacks).

Even if Article 15 and the connecting recitals only apply to high-risk AI systems, in order to preserve the positive image and trust of the notarial profession, as well as to ascertain the legal security and to guarantee the compliance with general (EU and possibly national) cybersecurity obligations, high-level of cybersecurity must be guaranteed also in case of development and use of notarial AI systems not falling under the high-risk category.

c) GDPR

Besides the AI Act, the GDPR includes provisions which can be applicable also in the AI cybersecurity context, even if the GDPR does not include explicit rules for AI systems. These rules are related to (personal) data security obligations. Article 32 of the GDPR includes provisions on the security of processing personal data for controllers and processors by implementing appropriate technical and organisational measures to assure an appropriate level of security. These measures shall provide protection against loss, alteration, disclosure and access. The same article contains a non-exclusive list of these measures (e.g. ensuring the security of processing) without providing further details. Since the GDPR is a technology-neutral regulation, in respect of AI, these measures shall be determined by taking into consideration—among others—the potential risks, characteristics, purposes and significance of the given AI solution on a case-by-case basis.

In respect of the technical and organisational measures, Article 25 (1) of the GDPR shall be taken into account, because within the framework of the requirement of '*data protection by design*', the secure processing of personal data shall be guaranteed. This rule only concerns the data controllers.

Therefore, if a notariat develops AI systems processing personal data and/or the notaries use AI systems processing such data, the above rules of the GDPR need to be taken into consideration.

Finally, the role of standards related to AI systems shall be mentioned. The ISO (International Organisation for Standardisation) published together with the IEC (International Electrotechnical Commission) several AI-specific standards (e.g. ISO/IEC TR 27563 on the use cases for the impact of security and privacy to AI). Most of these standards have been transposed by the CEN (European Committee for Standardisation) and CLC (European Committee for Electrotechnical Standardization). The consultation of these standards is strongly recommended.

4. AI cybersecurity and the notariat

In the notarial profession, both notarial organisations (chambers) and individual notaries have to actively participate in ensuring the cybersecurity of AI systems developed/used by them.

The main task of the former is to develop such systems which can withstand attacks and to provide instructions and guidance to their notaries for the appropriate and safe use of such systems. Subsequently, they shall permanently monitor, audit and update such systems to be resilient enough. Furthermore, notarial organisations (chambers) should establish strict access control to guarantee that only the competent persons get the necessary permissions.

Notaries should follow the instructions and guidance provided, and if they detect cyberthreats or attacks, promptly notify the notarial organisation (chamber) they belong to in order to make speedy steps to prevent/counter these threats/attacks or to fix the negative impacts caused by them.

In case of use of AI systems developed by external service providers, besides the obligations indicated above, the relevant contractual terms have to include detailed provisions for ensuring appropriate cybersecurity protection. The involvement of notarial IT-experts in the establishment of such contractual terms is crucial. Moreover, in every case, consultation with external cybersecurity specialists is highly recommended.

Key takeaways

- AI systems are themselves exposed to cyberattacks, the protection against which is crucial.
- Cyberthreats and attacks are intentional and most often exploit the vulnerabilities of the AI systems, targeting mainly the training data and the integrity of the applied algorithm.
- Cyberthreats and attacks can impact both the stages of development (training, testing) and deployment (entering prompts, providing outputs). They can be targeted and may affect the integrity, the confidentiality, or the availability of the AI system.
- Within this Chapter, the evasion attacks, the training data poisoning, the model poisoning, the prompt injection, the model theft (model extraction) and the denial-of-service attacks are briefly presented, together with possible solution measures.
- Currently, there are no specific legal acts at EU level on AI cybersecurity, and other existing legal acts (e.g. the AI Act) barely include provisions in this respect. However, national legislation and soft law instruments always need to be checked.
- The AI Act includes specific obligations on cybersecurity and robustness for providers only in respect of high-risk AI systems and general-purpose AI models with systemic risk, without providing detailed guidance on how to fulfil these obligations.
- In case of notarial AI solutions not falling under the high-risk category, ensuring the high-level of cybersecurity is also recommended.
- Article 32 of the GDPR (security of processing personal data for controllers and processors by implementing appropriate technical and organisational measures) and Article 25 of the same act (*'data protection by design'*) shall be also applied in the context of AI cybersecurity.
- Consulting the relevant international and European standards is strongly recommended.
- Both notarial organisations (chambers) and individual notaries have to actively participate in ensuring the cybersecurity of AI systems developed/used by them.
- In case of use of AI systems developed by external service providers, the relevant contractual terms have to include detailed provisions for ensuring the appropriate cybersecurity protection.
- In every case, consultation with external cybersecurity specialists is highly recommended.

Publisher:

Council of the Notariats of the European Union (CNUE)
B-1000 Bruxelles
Avenue de Cortenbergh, 120
T. +32 2 513 95 29
info@cnue.be
www.notariesofeurope.eu

Author:

Tamás Sajben

Contributors:

Members of the CNUE Futurology Forum, New Technologies Working Group and Data Protection Task Force

Year of publication:

2025

Cover picture: AI chatbot is the process of artificial intelligence between systems and human beings. In other words, AI chatbot is a virtual customer service that can actively interact with the users. Picture by KhunkornStudio
Background picture: Concept art of digital data cloud storage. Picture by Keopaserth