ARTIFICIAL INTELLIGENCE AND THE LEGAL PROFESSION: CHALLENGES AND RISKS IN THE AREA OF PERSONAL DATA PROTECTION AND LAWYERS' DUTY OF CONFIDENTIALITY[1]

Peter Lukáčka[2], Giang Nguyen[3]

Abstract: Artificial intelligence tools are gradually entering the practical and fairly ordinary life of our entire society. Many tools and applications that use this new technology can be identified almost "at every step," which reinforces the feeling among individuals that without adopting these innovations, it is impossible to remain competitive compared to other individuals or entrepreneurs who do use these tools. In our view, similar attitudes exist within the practice of various legal professions (lawyers, judges, notaries, etc.), and it will depend on future developments whether these expectations are fulfilled. Specifically in the field of law practice, elements of flexibility, speed, and efficiency in providing legal services to clients come to the forefront. This creates pressure to introduce innovations into everyday practice—otherwise, a solicitor may lose competitiveness compared to others. With this in mind, the authors of this paper examined both the technical and legal challenges and risks that can be identified in the use of artificial intelligence tools in the provision of legal services on an on- . In particular, they focused on whether working with selected AI tools ensures adequate protection of personal data under applicable legislation, and whether the use of AI tools leads, or could lead, to a violation of a solicitor's duty of confidentiality.

Key words: Artificial intelligence, legal practice, personal data protection, duty of confidentiality

Introduction

The world has recently been influenced by a new approach to the use of technological progress, which is reflected in the gradual penetration of artificial intelligence (hereinafter "AI") tools into virtually all areas of life. We dare to predict that where

[1] This contribution is funded by the EU NextGenerationEU through the Slovak Republic's Recovery and Resilience Plan as part of the Artificial Intelligence for Legal Professions (AILE) project No. 09I05-03-V02-00038

[2] Comenius University in Bratislava, Faculty of Law

[3] Slovak University of Technology in Bratislava, Faculty of Informatics and Information Technologies

doi: 10.46282/bpf.2025.23

this is not yet the case, it will happen in the near future. However, it should be noted that these attempts to introduce AI into individual human activities do not always fall on fertile ground, and in some areas these tools have not caught on at all or are waiting for an effective and meaningful way to be found to use them. In our opinion, this group of cases can also include, in part, the performance of certain specific activities within the legal profession that cannot be replaced by AI (building trust between client and lawyer, reflecting the client's personal specifics when providing legal assistance, representation before courts and other authorities, etc.). On the other hand, it should be noted that the use of AI is penetrating many activities of lawyers and law firms, mainly with the aim of finding an effective tool to speed up the processes of obtaining information and preparing materials for individual outputs. This is also confirmed by several studies at national and international level carried out by various chambers of lawyers. One of the most extensive studies in this area is the research carried out by the International Bar Association (IBA) and the Centre for Artificial Intelligence and Digital Policy (CAIDP), which was conducted among lawyers from around the world and found that 210 of 333 respondents (law firms) use artificial intelligence in their work. Most of the law firms using artificial intelligence are located in Europe (including the United Kingdom), the United States and other countries that operate in multiple jurisdictions through subsidiaries in different countries. In the case of firms with more than 500 lawyers, 100% said they had implemented artificial intelligence into their work processes. Conversely, in the case of smaller firms, specifically those with 1 to 100 lawyers, the results show that 68% do not yet use artificial intelligence.[4] Similar research was conducted in January and February 2025 by the Slovak Bar Association, which was carried out on a sample of 250 respondents (lawyers, trainees), which showed that 47% of participants use AI tools in practice.[5] These exact data show that, both globally and nationally within the Slovak Republic, there is significant use of artificial intelligence tools in legal practice, which creates an increased need to answer questions related to this. This mainly concerns the area of personal data protection (compliance with the GDPR[6]) as well as the duty of confidentiality, which is formulated very strictly in the legal profession and compliance with which is one of the fundamental duties of lawyers worldwide.

[4] INTERNATIONAL BAR ASSOCIATION CENTER FOR AI AND DIGITAL POLICY: THE FUTURE IS NOW: ARTIFICIAL INTELLIGENCE AND THE LEGAL PROFESSION, SEPTEMBER 2024, London, 2024, pp. 11-12, available on 28 September 2025 at: https://www.ibanet.org/document?id=The-future-is-now-artificial-intelligence-legal-profession

[5] Slovak Bar Association: Peer review of the use of AI in legal practice. Available on 28 September 2025 at: https://info.sak.sk/wp-content/uploads/2025/02/2025_0225_SAK_prieskum_AI-3.pdf

[6] 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 (General Data Protection Regulation)

doi: 10.46282/bpf.2025.23

Legal regulation of personal data protection and confidentiality obligations

Personal data protection is currently one of the important elements of the functioning of society as such, since this data is important to those to whom it belongs, but it can also pose certain challenges in the areas of commerce and marketing, as well as illegal activities. This is all the more true as the current functioning of society is increasingly shifting from personal contact to the digital sphere, where this type of data is exchanged through various types of electronic communication. This is particularly true in the legal profession, which is typically and to a certain extent based on working with personal data or data that must be protected from disclosure or access by other persons. This therefore places special requirements on the legal profession, the fulfilment of which determines whether or not a lawyer fulfils their basic obligations. In this article, we set out to assess whether the use of certain AI tools meets the requirements for personal data protection, or whether working with these tools can be said to preserve the duty of confidentiality or not. Although personal data protection and the duty of confidentiality are, in principle, two somewhat different areas, we believe that they also have certain unifying elements that lead us to assess and analyse them together within the framework of this topic. In this regard, we agree with the view that lawyers are subject to specific legal regulations arising in particular from the Act on Advocacy[7] and the professional regulations of the Slovak Bar Association, which justify a special approach by lawyers to the protection of personal data under the GDPR. The protection of personal data by lawyers is a fundamental prerequisite for compliance with the obligation of lawyers to maintain confidentiality. A breach of personal data protection could compromise the obligation to maintain confidentiality.[8] In view of the above, we therefore consider it appropriate to assess and analyse the obligation to protect personal data and the obligation of confidentiality of lawyers in conjunction with each other, as ultimately, strictly separating them may not be appropriate in every case.

Lawyers have multiple responsibilities – to the individuals and organisations they provide services to, to their colleagues in the law firm, and to the legal profession.

[7] Act No. 586/2003 Coll. on Advocacy and on Amendments to Act No. 455/1991 Coll. on Small Business (Small Business Act), as amended

[8] Slovak Bar Association: CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA BY LAWYERS under the General Data Protection Regulation (GDPR). Approved by the Office for Personal Data Protection of the Slovak Republic by Decision No. 00676/2018-Os-9 of 4 December 2018, which entered into force on 10 December 2018, p. 3, available on 28 September 2025 at: https://www.sak.sk/web/sk/cms/sak

doi: 10.46282/bpf.2025.23

Lawyers fulfil their obligations primarily to the extent that they represent their clients and respect the deontological rules of the legal profession.[9]

The area of personal data protection[10] and the lawyer's duty of confidentiality[11] (not only in connection with the use of artificial intelligence tools) are regulated at several levels of legislation:

- European Union legislation (in particular the GDPR, AI Act[12]),
- Slovak legislation (in particular the Constitution of the Slovak Republic, the Act on Advocacy, the Act on Personal Data Protection[13] , the AML Act[14] , the Criminal Procedure Code[15] , the Civil Procedure Code[16]),
- ethical and internal regulations of the Slovak Bar Association (Resolution of the Presidium of the Slovak Bar Association No. 12/4/2025 of 31 March 2025, Position Paper of the SBA, 6 June 2025),
- ethical and internal regulations of the Council of Bars and Law Societies (Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers, CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE[17] , Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU[18])

[9] Position paper of the Slovak Bar Association approved by the conference of lawyers on 6 June 2025, p. 2, available on 28 September 2025 at: https://www.sak.sk/web/sk/cms/sak

[10] Herath, H.M.S.S., Herath, H.M.K.K.M.B., Madhusanka, B.G.D.A. and Guruge, L.G.P.K., 2024. Data protection challenges in the processing of sensitive data. In Data Protection: The Wake of AI and Machine Learning (pp. 155-179). DOI 10.1007/978-3-031-76473-8_8. Cham: Springer Nature Switzerland.

[11] Richmond, D.R., 2021. Lawyers' duty of confidentiality and clients' crimes and frauds. Ga. St. UL Rev., 38, p.493. https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=3128&context=gsulr

[12] REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules in the field of 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 (Artificial Intelligence Act))

[13] Act No. 18/2018 Coll. on the protection of personal data and on amendments to certain acts, as amended

[14] Act No. 297/2008 Coll. on the prevention of legalisation of proceeds from criminal activity and on the prevention of terrorist financing and amending certain acts

[15] Act No. 301/2005 Coll. Criminal Procedure Code, as amended

[16] Act No. 160/2015 Coll. Civil Procedure Code, as amended

[17] Council of Bars and Law Societies of Europe The voice of European Lawyers: CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE, available on 28 September 2025 at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf

[18] Council of Bars and Law Societies of Europe The voice of European Lawyers: Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU. Council of Bars and Law Societies of Europe: Brussels, 2022, available on 28 September 2025 at:

doi: 10.46282/bpf.2025.23

These regulations create a comprehensive system of obligations that must be strictly adhered to in legal practice. The obligation to protect personal data arises primarily from the GDPR and the Personal Data Protection Act, while attorney-client privilege is specifically regulated in the Act on Advocacy and ethical regulations. Internal documents of the Slovak Bar Association also play an important role, such as the Rules for the Use of Artificial Intelligence Tools in Legal Practice[19] , which set out principles for the safe use of AI tools with an emphasis on the protection of confidentiality, professional secrecy and personal data, and the Position Paper of the Slovak Bar Association approved by the conference of lawyers on 6 June 2025, which emphasises the importance of protecting confidentiality, professional secrecy, independence and adaptation to technological developments, including digitisation and cyber security in legal practice. Exceptions to confidentiality and specific obligations in data processing are contained in specific laws, particularly in the area of anti-money laundering and procedural rules, but also in the Act on Advocacy itself. The EDPB Opinion on Artificial Intelligence Models: the principles of the General Data Protection Regulation support responsible artificial intelligence[20] (hereinafter referred to as "EDPB Opinion 28/2024"), which formulates a number of principles and requirements in relation to the use of AI tools and the protection of personal data (the impossibility of assuming the anonymity of AI models trained on personal data; strict application of the three-step test of legitimate interest; the importance of mitigating measures and documentation, etc.).

The obligation to protect personal data in legal practice

Personal data protection is currently a highly topical issue, as data and information are becoming an important commodity and often enable entities to gain a competitive advantage. However, this is not an obligation that is specifically addressed only to lawyers; many entities that come into contact with this category of data have an obligation to protect personal data and handle it in accordance with the relevant regulations. According to Article 19(3) of the Constitution of the Slovak Republic, everyone has the right to protection against unauthorised collection, disclosure or other misuse of data concerning their person. This right is matched by the obligation of entities that process such data to protect it and handle it in accordance with applicable legislation. However, the legal profession is even more

https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Reports_studies/EN_ITL_20220331_Guide-AI4L.pdf

[19] Resolution of the SAK Presidium No. 12/4/2025 of 31 March 2025

[20] European Data Protection Board: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024, available on 28 September 2025 at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

doi: 10.46282/bpf.2025.23

exposed in this regard, as it is common for this type of data to be processed in the course of practising law. In the context of personal data processing, we identify several principles that must be observed in this process. These are:

- **Lawfulness, fairness and transparency**: Personal data must be processed lawfully, fairly and transparently in relation to the data subject.
- **Purpose limitation**: Data may only be collected for specific, explicitly stated and legitimate purposes and may not be further processed in a manner incompatible with those purposes.
- **Data minimisation**[21] : The data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy**: Data must be accurate and kept up to date as necessary.
- **Storage limitation**: Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
- **Integrity and confidentiality**: Data must be processed in a manner that ensures appropriate security[22] , including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.[23] These principles are also reflected in the Personal Data Protection Act, in particular in Sections 13 and 39.

Lawyers and law firms generally act as personal data controllers when processing the data of clients, counterparties, witnesses, employees and other persons in the course of providing legal services. Their main obligations include:

- **Identifying the legal basis for processing** (e.g. compliance with a legal obligation, performance of a contract, etc.).
- **Information obligation:** (obligation to inform data subjects about the processing of their data, to the extent specified in Articles 13 and 14 of the GDPR).
- **Data security** (obligation to take appropriate technical and organisational measures to protect data - Article 32 of the GDPR and Section 29 of the Personal Data Protection Act). In this context, it is possible to mention, in particular, the encryption of data on disks, servers, in backups and during

[21] Ganesh, P., Tran, C., Shokri, R. and Fioretto, F., 2025, June. The data minimisation principle in machine learning. In Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (pp. 3075-3093). DOI 10.1145/3715275.37321.

[22] Torre, D., Alferez, M., Soltana, G., Sabetzadeh, M. and Briand, L., 2021. Modelling data protection and privacy: application and experience with GDPR. Software and Systems Modelling, 20(6), pp. 2071–2087. DOI 10.1007/s10270-021-00935-5.

[23] Article 5 GDPR

doi: 10.46282/bpf.2025.23

transmission (e-mail communication, cloud storage)[24] , the use of strong passwords, two-factor authentication, regular changes to access data, regular employee training[25] , etc.

- **Minimising access[26]** (only persons who absolutely need it for their work should have access to personal data). Examples of such measures include locked archives, office access control, and physical protection of documents.
- **Contractual security of processing** (if a law firm uses intermediaries, it must have a contract with them for the processing of personal data).
- **Keeping records of processing activities** (obligation to keep records of personal data processing in accordance with Article 30 of the GDPR).
- **Notification of data breaches:** Obligation to notify the Office for Personal Data Protection of personal data breaches.

Compliance with personal data protection obligations must also be viewed in the context of the possible negative consequences not only for the subjects whose personal data has been leaked, but also for the lawyers themselves. In this regard, there is a risk of fines being imposed by the Office for Personal Data Protection, disciplinary liability under the regulations of the Slovak Bar Association, as well as a possible investigation into the conditions for imposing an obligation to compensate the persons concerned.

Lawyer's duty of confidentiality

The duty of confidentiality is one of the most fundamental elements of the legal profession and is a basic prerequisite for trust between a lawyer and their client. For a lawyer to do their job, it is essential that their client confides in them things they would not tell anyone else. A lawyer should be a recipient of information based on trust. A client cannot trust a lawyer without feeling certain that the lawyer will maintain confidentiality about the facts they have learned. The duty of confidentiality is therefore a primary and fundamental right and, at the same time, a primary and fundamental duty of a lawyer.[27] This duty is enshrined in the legislation

[24] Easttom, C., 2022. Virtual private networks, authentication, and wireless security. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 309-327). Cham: Springer International Publishing. DOI 10.1007/978-3-031-12304-7_14.

[25] Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In Data ethics and challenges (pp. 41-59). Singapore: Springer Singapore. DOI 10.1007/978-981-19-0752-4_3.

[26] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), pp. 4682-4696. DOI 10.1109/JIOT.2020.2969326

[27] The Council of Bars and Law Societies of Europe: CHARTER OF KEY PRINCIPLES OF THE EUROPEAN LEGAL PROFESSION AND CODE OF CONDUCT FOR EUROPEAN LAWYERS. Brussels, Éditeur responsable: Jonathan Goldmsith, 2013, p. 15

of the Slovak Republic, in European standards, as well as in the ethical and internal regulations of the Slovak Bar Association. It can even be said that the essence of the practice of law is the fact that a client can confide in their lawyer with matters that they would not tell anyone else. A lawyer should treat client information as confidential. Without the assurance of confidentiality, the client cannot trust them. Maintaining confidentiality is not only a lawyer's duty, but also a fundamental right of the client. [28]The basic legal regulation is the Act on Advocacy, which stipulates in § 23: *"A lawyer is obliged to maintain confidentiality regarding all facts that he or she has learned in connection with the practice of law. The duty of confidentiality also applies to trainee lawyers and employees of lawyers."* This duty is absolute and continues even after the provision of legal services has ended. This Act also regulates exceptions to the duty of confidentiality. According to Section 24, a solicitor may be released from the duty of confidentiality only with the written consent of the client (only the client or their legal successor - however, the solicitor may not respect this release if they consider that the release from the duty of confidentiality is to the detriment of the client) or on the basis of the law (e.g.: a lawyer is not obliged to maintain confidentiality towards a person whom he or she entrusts with the performance of individual legal services if that person is himself or herself bound by a duty of confidentiality; in proceedings before a court or other authority if the subject matter of the proceedings is a dispute between him or her and the client; a statutory obligation to prevent the commission of a criminal offence). Legal exceptions to the duty of confidentiality also include the obligation to report unusual transactions under the AML Act[29] . The duty of confidentiality is also regulated by procedural rules. For example, according to Section 129(2) of the Criminal Procedure Code, a witness may not be heard as a witness on matters covered by the duty of confidentiality unless he or she has been released from this duty. Similarly, Section 203 of the Civil Procedure Code stipulates that a witness is obliged to maintain confidentiality regarding information protected under special regulations and other confidentiality obligations established by law or recognised by the state when giving testimony. The above procedural rules therefore also reflect the lawyer's statutory duty of confidentiality.

Two basic conclusions can be drawn from the above:

1. The duty of confidentiality is formulated in very general terms and applies to a relatively wide range of cases. The duty of confidentiality covers all information about facts that a lawyer has learned from a client and about a client in the course of providing legal services. This duty does not apply to

[28] Position paper of the Slovak Bar Association approved by the conference of lawyers on 6 June 2025, p. 3, available on 28 September 2025 at: https://www.sak.sk/web/sk/cms/sak

[29] Section 4(2) of the AML Act

doi: 10.46282/bpf.2025.23

publicly known, notorious or trivial facts. Thus, the scope and content of the duty of confidentiality includes not only information directly related to the performance of the mandate, but also other private, personal, business, tax or political matters relating to the client. The duty of confidentiality arises at the moment of first contact with a potential client, i.e. the moment when the solicitor learns of the circumstances relating to the future provision or provision of legal services. This duty exists throughout the duration of the lawyer's relationship with the client and continues until the client releases the lawyer from the duty of confidentiality or a situation arises in which the law allows for a breach of the duty of confidentiality. The duty of confidentiality is never time-barred and continues even after the provision of legal services to the client has ended, or after the client's death (natural person) or dissolution (legal entity). The lawyer's duty of confidentiality continues even if the lawyer's licence to practise law has been suspended or they have ceased to practise.[30]

2. A solicitor may only breach their duty of confidentiality in specific and explicitly defined exceptions governed by the relevant legislation. Other cases must be considered a breach of duty and result in liability claims.

Personal data protection and the lawyer's duty of confidentiality in the age of artificial intelligence

The use of artificial intelligence tools by lawyers is gradually becoming a common or usual way of working around the world, as confirmed by the research mentioned above. It can even be noted that the effective use of these tools can represent a significant competitive advantage over lawyers who do not use these tools effectively. On the other hand, this situation raises a number of questions that need to be addressed because the development and use of new technologies must be incorporated into a specific legal framework to prevent a legal vacuum, i.e. a situation where a particular activity is not properly regulated. In the case of the use of artificial intelligence tools, this consequence should be prevented in particular through the adoption and consistent implementation of basic legislation, which at European level is primarily the AI Act. However, the fact remains that, particularly at the national level in the Slovak Republic , we currently do not have legal regulations in the area of personal data protection or confidentiality obligations that would respond to the existence and use of artificial intelligence tools. In view of this fact, it is necessary to apply the "old" but valid legal regulation to new phenomena and facts that did not

[30] Olej, J., Kerecman, P., Kalata, P. et al. Act **on** Advocacy. Commentary. 1st edition. Bratislava: C. H. Beck, 2013, commentary on § 23

doi: 10.46282/bpf.2025.23

exist at the time of its creation, which will test its functionality in relation to these new facts.

In view of the above, we have attempted to examine and subsequently verify the current situation with regard to selected artificial intelligence tools[31] nd Co-pilot, ChatGPT, and Gemini, as we were interested in how the use of these applications fulfils or fails to fulfil the conditions and obligations of personal data protection arising in particular from the GDPR and the Personal Data Protection Act, as well as whether whether, when these applications are used properly, it is possible to speak of compliance with the duty of confidentiality as stipulated for lawyers in the Slovak Republic by the Act on Advocacy[32] . With this in mind, we have prepared three separate tables that provide information on whether, in our opinion, the application and its use meet the legal requirements for personal data protection and the proper fulfilment of the duty of confidentiality of lawyers. Each table is prepared separately for each application assessed. The tables contain an evaluation of the assessed data for both paid and unpaid versions.

Table No. 1

Name of AI tool	**Version**	**Compliance with GDPR**	**Technical data protection measures**	**Personal data processing policies**	**Restrictions/exceptions in personal data processing**
Microsoft Copilot	Free	Partial, no contractual guarantees; not intended for corporate GDPR compliance	Encryption during transmission; limited data management options; data may be used to improve services	Data may be stored, analysed, used to improve services; Microsoft has access to data, third-party access possible	No option to select data region; no DPA; data may be used for training

[31] We narrowed down our selection of artificial intelligence tools (applications) to three, namely Co-pilot, ChatGPT and Gemini, which, according to the Collegial Survey on the Use of AI in Legal Practice (see reference no. 5), are the most widely used artificial intelligence tools in the Slovak Republic.

[32] For more information on the legal regulation of the "duty of confidentiality", see the explanation above.

doi: 10.46282/bpf.2025.23

Microsoft Copilot	Paid (Copilot for Microsoft 365, Azure OpenAI Service)	Possible compliance with GDPR; DPA included in Microsoft Product Terms; SCC for transfer outside the EU	Encryption in transit and at rest; option to select data region (EU/EEA); compliance with ISO 27001, ISO 27018, SOC 1/2/3; auditability	Data is not used to train basic models; data ownership on the customer's side; access only by authorised employees in necessary cases	Contractual guarantees not to use data for training; choice of region; auditable access

Processed Co-pilot and own processing

Table 2

AI tool name	Version	Legal requirements for personal data protection – compliance with GDPR	Technical data protection measures	Personal data processing policies	Restrictions/exceptions in personal data processing
Google Gemini	Free	Partial, no contractual guarantees; not intended for corporate GDPR compliance	Encryption during transmission; limited data management options; data may be used for model training	Data may be stored, analysed, used to improve services; Google has access to data, third-party access possible	No option to select data region; no DPA; data may be used for training
Google Gemini	Paid (Gemini for Workspace, Vertex AI)	Possible compliance with GDPR; DPA according to GDPR; SCC for transfer outside the EU	Encryption in transit and at rest; option to select data region (EU/EEA); compliance with ISO 27001, ISO 27018, SOC 2/3; auditability	Data is not used for model training; data ownership remains with the customer; access only by authorised employees in necessary cases	Contractual guarantees not to use data for training; option to select region; auditable access

Processed Co-pilot and own processing

AI tool name	Version	Legal requirements for personal data protection – compliance with GDPR	Technical measures for data protection	Personal data processing policies	Restrictions/exceptions in personal data processing
ChatGPT (OpenAI)	Free	Partial, no contractual guarantees; not intended for corporate GDPR compliance	Encryption in transit, limited at rest; data may be used to train models	Data may be stored, analysed, used to improve services; OpenAI has access to data, third-party access possible	No option to select data region; no DPA; data may be used for training
ChatGPT (OpenAI)	Paid (Enterprise, Team)	Possible compliance with GDPR; DPA according to Art. 28 GDPR; SCC for transfer outside the EU	Encryption in transit and at rest; auditability; option to select data region (EU/EEA); SOC 2 Type 2 compliance	Data is not used for model training; data ownership remains with the customer; access only by authorised employees in necessary cases	Contractual guarantees not to use data for training; choice of region; auditability of access

Processed Co-pilot and own processing

It follows from the above that the unpaid versions do not meet the requirements of the GDPR, mainly because no *Data Protection Agreement (*DPA) within the meaning of Article 28 of the GDPR, which can be considered a problem in this regard, and therefore any personal data uploaded to the system in this way does not have the required level of protection guaranteed, and at the same time it cannot be ruled out that in some versions this data will be used to train AI models. On the other hand, paid versions are better in this respect, as such an agreement may be concluded and intermediaries, namely Google, Open AI and Microsoft, undertake to comply with the GDPR in relation to personal data if such an agreement is concluded.

However, neither the tables nor the systems in question address the obligation of confidentiality, i.e. they do not contain any regulation that would expressly ensure access to information subject to confidentiality only to persons who meet the conditions set out in the Advocacy Act, since the circle of persons, despite the conclusion of a DPA (data protection agreement) and the use of paid versions, is significantly broader than that provided for by the Act on Advocacy. In general, it can be stated that when concluding a DPA, only the following persons may, in principle, have access to data uploaded to individual AI tools (Co-pilot, Gemini, ChatGPT):

Service provider: Access is limited to authorised employees who need access for maintenance, support or security purposes.

Subcontractors (sub-processors): Open AI, Google, and Microsoft may use subcontractors to provide part of the services (e.g., cloud hosting, infrastructure), who are bound by the same obligations.

Customer employees: Only authorised persons on the customer's side (data controller) have access to the data.

Public authorities: Access is only possible on the basis of legal requirements (e.g. court order, investigation), and OpenAI, Google, Microsoft are required to inform the customer unless prohibited by law.

To summarise the above findings, we can conclude that some paid versions of the AI tools examined may comply with the personal data protection obligations set out in the GDPR, particularly if a DPA is concluded to ensure and guarantee this. On the other hand, we can state that, under certain conditions, persons who do not fall under the legal exceptions to the attorney-client privilege set out in Section 23 of the Act on Advocacy may also have access to the data.

With regard to the use of artificial intelligence tools, we note the opinion of the Slovak Bar Association[33] , according to which:

Article 3

1. When providing legal services, a lawyer shall use AI tools in a manner that does not compromise their independence, duty of confidentiality, protection of professional secrecy, and prevents conflicts of interest.

2. Lawyers shall retain full responsibility for outputs generated using AI tools.

3. The use of AI tools does not replace professional judgement, legal argumentation or an individual approach to a case.

Article 4

A lawyer must not enter any information into AI tools that could lead to a breach of confidentiality or compromise personal data unless there is a guaranteed mechanism for their protection and a contractual assurance from the AI provider that the data will be secured in accordance with the GDPR and the Act on Advocacy.

[33] Resolution of the Presidium of the Slovak Bar Association No. 12/4/2025 of 31 March 2025 approving the rules for the use of artificial intelligence tools in legal practice

doi: 10.46282/bpf.2025.23

We have also recorded a similar opinion within the Czech Bar Association, which was adopted by its board at a meeting held on 11 and 12 September 2023.[34]

In our opinion, it follows from the above that in both Slovakia and the Czech Republic, it is possible to use artificial intelligence tools in accordance with the regulations of the professional chambers, but in a manner that guarantees compliance with all obligations that a lawyer has in relation to the protection of personal data and the obligation of confidentiality. It is therefore up to the lawyer or law firm themselves to ensure these requirements are met at their own risk. With regard to personal data protection and the fulfilment of the individual obligations associated with it, it can be assumed that the specified requirements are met, especially in the case of paid versions of individual AI tools. However, it is necessary to recommend verifying the compliance of the licence terms of the service provider at a specific time and for a specific case. Otherwise, such a user (lawyer) exposes themselves to the risk of breaching their obligations in this area. In this regard, in our opinion and in accordance with EDPB Opinion 28/2024, it is therefore necessary to emphasise in particular the strict application of the three-step test of legitimate interest, if this is the reason for the processing of personal data; the importance of mitigating measures and documentation (e.g., working with pseudonymised files; not using full identifiers in prompts; agreeing on "no training/no data sharing" and "zero/limited retention"; Data Protection Impact Assessment, where necessary, etc.).

With regard to compliance with the obligation of confidentiality, we believe that the systems examined do not provide sufficient guarantees in this regard to ensure that the data provided by lawyers to the AI tool will only be accessed by persons and in situations that allow for exceptions to the confidentiality obligation under the relevant legislation of the Slovak Republic. In this regard, we think it's worth noting that a breach of confidentiality can happen under certain circumstances, even if the document is anonymised. This would mainly concern cases where, on the basis of partial data supplemented, for example, by data from publicly available sources, it would be possible to identify a specific legal matter that is subject to the duty of confidentiality. This could be the case if we uploaded an anonymised real estate purchase agreement to the system, which we could then link (its specific terms and conditions) to the contracting parties, as the real estate cadastre in the Slovak Republic is public in terms of basic data on the owner of the real estate. For this reason, we recommend approaching artificial intelligence tools with caution, taking into account the risks we have tried to identify above.

[34] Czech Bar Association: OPINION ON THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE PROVISION OF LEGAL SERVICES, available on 28 September 2025 at: https://advokatnidenik.cz/2023/09/15/stanovisko-cak-k-vyuzivani-ai-pri-poskytovani-pravnich-sluzeb/

Conclusion

The protection of personal data and the duty of confidentiality of lawyers currently face a number of challenges, mainly related to artificial intelligence tools, which are gradually becoming a common working tool for lawyers in their work. This situation has a number of practical implications for the fulfilment of these obligations by lawyers, since, unlike in the past, data is now processed online, i.e. it is not locked away in a safe at the lawyer's office, but is stored in a location that is essentially unknown, and access to this data does not usually depend solely on the will of the entity (lawyer) that uploaded it to the system. In our opinion, it is therefore important that lawyers take these facts into account when working with these tools and handle the data with the utmost caution in this regard, or take the necessary steps to ensure compliance with the conditions required by the relevant legislation for working with personal data. In this article, we analysed the conditions for fulfilling the obligation to protect personal data and the obligation of confidentiality of lawyers when working with selected artificial intelligence tools from the perspective of lawyers' work, and we identified the risks involved in working with these tools. In our research, we concluded that, within the framework of selected AI tools (paid versions), after fulfilling specific conditions (conclusion of a DPA, required security, encryption of communication, etc.), it is possible to say that the conditions for personal data protection under the GDPR are being met. Of course, it is necessary to always verify these facts at a specific time and for a specific AI tool and to reflect on the recommendations formulated in EDPB Opinion 28/2024. As for whether the artificial intelligence systems examined can also meet the requirements for compliance with the obligation of confidentiality, we are rather sceptical in this regard, as in our opinion there is no sufficient guarantee that only those persons who are authorised to access the data under the Advocacy Act will have access to the data recorded in the individual systems.

List of references

1. Council of Bars and Law Societies of Europe The voice of European Lawyers: CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE, 2020 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf
2. Council of Bars and Law Societies of Europe The voice of European Lawyers: Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU. Council of Bars and Law Societies of Europe: Brussels, 2022, available on 28 September 2025 at:

doi: 10.46282/bpf.2025.23

https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Reports_studies/EN_ITL_20220331_Guide-AI4L.pdf

3. Czech Bar Association: OPINION ON THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE PROVISION OF LEGAL SERVICES, available on 28 September 2025 at: https://advokatnidenik.cz/2023/09/15/stanovisko-cak-k-vyuzivani-ai-pri-poskytovani-pravnich-sluzeb/
4. Easttom, C., 2022. Virtual private networks, authentication, and wireless security. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 309-327). Cham: Springer International Publishing. DOI 10.1007/978-3-031-12304-7_14.
5. European Data Protection Board: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en
6. Ganesh, P., Tran, C., Shokri, R. and Fioretto, F., 2025, June. The data minimisation principle in machine learning. In Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (pp. 3075-3093). DOI 10.1145/3715275.37321.
7. Herath, H.M.S.S., Herath, H.M.K.K.M.B., Madhusanka, B.G.D.A. and Guruge, L.G.P.K., 2024. Data protection challenges in the processing of sensitive data. In Data Protection: The Wake of AI and Machine Learning (pp. 155-179). DOI 10.1007/978-3-031-76473-8_8. Cham: Springer Nature Switzerland.
8. INTERNATIONAL BAR ASSOCIATION CENTER FOR AI AND DIGITAL POLICY: THE FUTURE IS NOW: ARTIFICIAL INTELLIGENCE AND THE LEGAL PROFESSION, SEPTEMBER 2024, London, 2024, https://www.ibanet.org/document?id=The-future-is-now-artificial-intelligence-legal-profession
9. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), pp.4682-4696. DOI 10.1109/JIOT.2020.2969326
10. Olej, J., Kerecman, P., Kalata, P. et al. Law on Advocacy. Commentary. 1st edition. Bratislava: C. H. Beck, 2013, Ean: 9788089603114
11. Position paper of the Slovak Bar Association approved by the conference of lawyers on 6 June 2025 https://www.sak.sk/web/sk/cms/sak
12. Richmond, D.R., 2021. Lawyers' duty of confidentiality and clients' crimes and frauds. Ga. St. UL Rev., 38, p.493. https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=3128&context=gsulr

13. Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In Data ethics and challenges (pp. 41-59). Singapore: Springer Singapore. DOI 10.1007/978-981-19-0752-4_3.
14. Slovak Bar Association: Collegial survey on the use of AI in legal practice. https://info.sak.sk/wp-content/uploads/2025/02/2025_0225_SAK_prieskum_AI-3.pdf
15. Slovak Bar Association: CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA BY LAWYERS under the General Data Protection Regulation (GDPR). Approved by the Office for Personal Data Protection of the Slovak Republic by Decision No. 00676/2018-Os-9 of 4 December 2018, https://www.sak.sk/web/sk/cms/sak
16. The Council of Bars and Law Societies of Europe: CHARTER OF KEY PRINCIPLES OF THE EUROPEAN LEGAL PROFESSION AND CODE OF CONDUCT FOR EUROPEAN LAWYERS. Brussels, Éditeur responsable: Jonathan Goldmsith, 2013
17. Torre, D., Alferez, M., Soltana, G., Sabetzadeh, M. and Briand, L., 2021. Modelling data protection and privacy: application and experience with GDPR. Software and Systems Modelling, 20(6), pp.2071-2087. DOI 10.1007/s10270-021-00935-5.
18. Resolution of the SAK Presidium No. 12/4/2025 of 31 March 2025

In preparing this work, LLM artificial intelligence tools were used ***only*** *for grammar correction, natural language improvement, and table creation. Content edited and grammatically checked by artificial intelligence was thoroughly reviewed and edited as necessary. The authors take full responsibility for the final content of this work.*

Contact details

doc. JUDr. Peter Lukáčka, PhD.
peter.lukacka@flaw.uniba.sk
Comenius University in Bratislava, Faculty of Law

doc. Ing. Giang Nguyen, PhD.
giang.nguyen@stuba.sk
Slovak University of Technology in Bratislava, Faculty of Informatics and Information Technologies

doi: 10.46282/bpf.2025.23